UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

CRISTINA MELCHIORS

Gerenciamento de Redes Fortemente Distribuído Utilizando a Tecnologia P2P

Tese apresentada como requisito parcial para a obtenção do grau de Doutor em Ciência da Computação

Prof. Dr. Lisandro Zambenedetti Granville
Orientador

Profa. Dra. Liane Margarida Rockenbach Tarouco
Co-orientadora

Porto Alegre, janeiro de 2011.

CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Melchiors, Cristina

Gerenciamento de Redes Fortemente Distribuído Utilizando a Tecnologia P2P/ Cristina Melchiors – Porto Alegre: Programa de Pós-Graduação em Computação, 2011.

222 f.:il.

Tese (doutorado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação. Porto Alegre, BR – RS, 2011. Orientador: Lisandro Zambenedetti Granville; Co-orientador: Liane Margarida Rockenbach Tarouco.

1.Gerenciamento de redes distribuído. 2.Taxonomias e paradigmas de gerenciamento de redes. 3.Peer-to-peer. I. Granville, Lisandro Zambenedetti. II. Tarouco, Liane Margarida Rockenbach. III. Gerenciamento de Redes Fortemente Distribuído Utilizando a Tecnologia P2P.

AGRADECIMENTOS

Inicialmente, gostaria de agradecer ao Prof. Lisandro Granville, pelo seu constante apoio, por sua inesgotável paciência, por seus valiosos conselhos, idéias e sugestões, por sempre ter uma palavra de incentivo e uma visão otimista, pela confiança, pelas intermináveis discussões travadas, pela firme e segura orientação ao longo de todos os anos deste trabalho.

Gostaria, também, de agradecer à Profa. Liane Tarouco, pelos enormes e preciosos ensinamentos, conselhos e sugestões recebidos, pela constante motivação, pela confiança depositada ao longo destes vários anos de jornada acadêmica (ainda me lembro dos meus tempos de bolsista de IC).

Aos professores do grupo de redes, pelas idéias, pelo apoio na realização deste trabalho, pelo incentivo recebido. Aos colegas da pós-graduação, por suas contribuições com discussões e trabalhos conjuntos. Aos funcionários do PPGC e do Instituto de Informática, que tanto me auxiliaram, sempre solícitos e atenciosos.

Ao meu querido Mauro, a quem dedico este trabalho, pelo enorme encorajamento, estímulo, compreensão, carinho e amor ao longo de todos estes anos. Pela sua paciência com minha ausência ao longo desta jornada. Pelo seu auxílio e paciência na revisão deste trabalho, nas longas discussões, nas sugestões.

Um enorme agradecimento aos meus pais, Djalmar e Leila, pelo inesgotável e constante incentivo e carinho, pelo apoio incondicional, pelo estímulo e pelas valiosas lições recebidas sobre o valor intrínseco do estudo e do conhecimento. Agradeço, também, às minhas irmãs, Lúcia e Paula, e ao meu cunhado, Marcelo, pelo companheirismo, motivação, incentivo e carinho. À Clarinha e ao Luquinhas, por serem tão especiais e me lembrarem do lado mágico da vida. Aos meus sogros, Mauro e Lígia, e aos meus cunhados, pelo carinho e apoio. Aos meus amigos, pelo constante encorajamento ao longo destes anos.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

CIM	Common Information Model
CMIP	Common Management Information Protocol
COD	Code-on-Demand
CORBA	Common Object Request Broker Architecture
DARPA	Defence Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DHT	Distributed Hash Table
DMTF	Distributed Management Task Force
FCAPS	Fault, Configuration, Accounting, Performance, Security
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
IAD	Inteligência Artificial Distribuída
IDL	Interface Definition Language
IETF	Internet Engineering Task Force
ISO	International Standards Organization
ITU	International Telecommunication Union
JMAPI	Java Management Application Programming Interface
JMX	Java Management Extensions
JSR	Java Specification Request
MA	Mobile Agent
MbD	Management by Delegation
MIB	Management Information Base
OMA	Object Management Architecture
OMG	Object Management Group
ORB	Object Request Broker
OSI-SM	OSI Systems Management
PEP	Policy Enforcement Point

PDP	Policy Decision Point
QoS	Quality of Service
RBC	Raciocínio Baseado em Casos
REV	Remote Evaluation
RMON	Remote Monitoring MIB
SLP	Service Location Protocol
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SNMPv2c	Community-based Simple Network Management Protocol version 2
SOAP	Simple Object Access Protocol
TMN	Telecommunications Management Network
UDDI	Universal Description, Discovery, and Integration
UDP	User Datagram Protocol
UML	Unified Modeling Language
URI	Universal Resource Identifier
W3C	World Wide Web Consortium
WBEM	Web-Based Enterprise Management
VM	Virtual Machine
WS	Web Services
WSDL	Web Services Description Language
XML	eXtensible Markup Language

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

O gerenciamento de redes é realizado seguindo diversos modelos, baseados em diferentes paradigmas. Os paradigmas tradicionais de gerenciamento compreendem o paradigma centralizado e o paradigma hierárquico fracamente distribuído. Tais paradigmas, contudo, apresentam limitações para o gerenciamento de diversas redes atuais, em virtude de fatores como o aumento em tamanho, em complexidade e em heterogeneidade destas redes. Em adição a estes fatores, existem atualmente contextos de rede que, por apresentarem certas peculiaridades, não podem ser gerenciados de modo apropriado por tais modelos.

Estas limitações e requisitos diferenciados encontrados nas redes atuais trazem a necessidade do emprego de modelos de gerenciamento inovadores, baseados nos paradigmas fortemente distribuídos. Neste contexto, uma tecnologia que se mostra promissora para o desenvolvimento de um modelo de gerenciamento com tais características é a tecnologia *peer-to-peer* (P2P).

Esta Tese versa sobre estes tópicos. Discute, como primeiro objetivo, as limitações dos modelos tradicionais para o gerenciamento de *contextos modernos* de rede, isto é, contextos de redes atuais que possuem particularidades distintas e, com isto, demandam requisitos de gerenciamento específicos, não identificados nas redes tradicionais. Define e investiga, então, como segundo objetivo, um modelo de gerenciamento fortemente distribuído baseado na tecnologia P2P. Este modelo visualiza a rede P2P como uma infra-estrutura que provê suporte para que as operações de gerenciamento sejam desempenhadas com forte distribuição. Por fim, como terceiro objetivo, analisa como as soluções de gerenciamento para redes atuais baseadas neste modelo podem ser classificadas segundo os paradigmas de gerenciamento das principais taxonomias propostas na literatura. Tal análise proporciona a identificação das limitações destas taxonomias para a classificação das soluções de gerenciamento requeridas para os contextos de redes atuais e deu origem à definição de uma taxonomia para soluções de gerenciamento que destaca as características e os requisitos demandados dos modelos de gerenciamento modernos.

Palavras-Chave: gerenciamento de redes distribuído, paradigmas de gerenciamento de redes, *peer-to-peer*.

Strongly Distributed Network Management Using P2P Technology

ABSTRACT

Network management is carried out following several models, based on different paradigms. Traditional management paradigms consist of centralized and weakly distributed hierarchical ones. However, such paradigms present limitations to be applied to the management of several today networks. This occurs because of some issues such as the grown in size, complexity and heterogeneity of such networks. Additionally, nowadays, there are network contexts that can not be appropriately managed by such models because of some context peculiarities.

Those today's networks drawbacks and requirements demand the employment of innovative models, based on strongly distributed paradigms. A technology that seems promising in addressing such needs is peer-to-peer (P2P).

This Thesis discusses about those topics. As its first objective, the Thesis discusses traditional models drawbacks to the management of modern network contexts, this is, current network contexts that have some different peculiarities and, because of them, demand specific management requirements not existent in traditional networks. As its second objective, the Thesis defines and investigates a strongly distributed management model based on P2P technology. Such model looks at P2P network as an infrastructure that can be used as support to management operations be accomplished in a strongly distributed way. Finally, as its third objective, the Thesis analyses how the management solutions based on such model can be classified according the management paradigms of the main literature taxonomies. Such analysis provides the identification of taxonomies limitations to the classification of management solutions required by today's network contexts. It has originated the definition of a management solution taxonomy that emphasizes the features and requirements demanded of modern management models.

Keywords: distributed network management, network management paradigms, peer-to-peer.

1 INTRODUÇÃO

Nos dias de hoje, as redes de computadores são essenciais para o correto funcionamento das organizações. Tais redes compreendem um enorme volume de recursos, com grande heterogeneidade nos equipamentos envolvidos. O gerenciamento de redes (CLEMM, 2007) (COMER, 2006) (HEGERING; ABECK; NEUMAIR, 1999) (UDUPA, 1996) é a disciplina que visa garantir a correta operação, manutenção e administração das redes.

As atividades de gerenciamento são realizadas seguindo diversos modelos, baseados em diferentes paradigmas. Vários critérios têm sido utilizados para definir os paradigmas de gerenciamento (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000) (MARTIN-FLATIN; ZNATY; HUBAUX, 1999) (MARTIN-FLATIN, 2003): tais definições e classificações serão abordadas em detalhes posteriormente neste documento. Entretanto, numa visão geral, estes paradigmas podem ser definidos como listado a seguir.

O **paradigma de gerenciamento centralizado** é o mais antigo, sendo ainda utilizado em algumas organizações, tipicamente aquelas que possuem redes de pequeno porte. Neste paradigma, todo o processamento e a inteligência de gerenciamento são concentrados em uma única entidade, denominada estação de gerenciamento. Esta estação é responsável por interagir com o software de gerenciamento dos equipamentos gerenciados (agentes), que assumem o papel de meros fornecedores de dados. A estação concentra todas as informações de gerenciamento obtidas dos equipamentos e fornece um ponto de acesso unificado para todas as aplicações.

O paradigma centralizado possui como vantagens a baixa complexidade e a acessibilidade facilitada, já que fornece um ponto único para interagir com todas as aplicações de gerenciamento, executar as atividades requeridas, etc. Tal paradigma, contudo, apresenta severas limitações de escalabilidade, já que, com o crescimento das redes, a estação de gerenciamento se torna sobrecarregada e um alto tráfego de gerenciamento é concentrado nos enlaces próximos a ela. Este paradigma sofre também de graves limitações de tolerância a falhas, uma vez que todas as funções de gerenciamento são concentradas em um único ponto. Adicionalmente, se a rede é particionada por uma falha em um enlace, toda a porção da rede que não possui a estação fica sem gerenciamento.

A fim de tentar solucionar estas limitações, paradigmas alternativos ao gerenciamento centralizado foram propostos. Estes paradigmas visam distribuir as ações de gerenciamento por vários pontos da rede, reduzindo a concentração do gerenciamento em um único ponto.

O paradigma de gerenciamento denominado **hierárquico fracamente distribuído** (MARTIN-FLATIN, 2003) é um destes. Nele, o sistema de gerenciamento é espalhado por algumas máquinas da rede, eliminando a concentração do processamento do gerenciamento em um único ponto. Neste paradigma, existe uma pequena proporção de máquinas da rede envolvidas no processamento de gerenciamento, que concentram a inteligência do gerenciamento, e um grande número de agentes que assumem o papel de meros fornecedores de dados. Este paradigma é encontrado no gerenciamento de inúmeras organizações dos dias atuais, sendo seguido por plataformas comerciais tradicionais largamente utilizadas (*e.g.*, HP OpenView Network Node Manager) e por tecnologias como RMON. Contudo, embora este paradigma distribua o processamento de gerenciamento em algumas entidades, este ainda é concentrado em poucas estações, gerando limitações de escalabilidade. Além disto, em caso de falha na comunicação entre as estações de gerenciamento e os agentes, estes últimos ainda não possuem meios de tomar ações corretivas, já que a inteligência do gerenciamento é concentrada apenas nas estações.

Os paradigmas de gerenciamento fortemente distribuídos visam lidar com tais limitações. O paradigma denominado **hierárquico fortemente distribuído** (MARTIN-FLATIN, 2003) é um destes. Neste paradigma, o processamento e a inteligência de gerenciamento são descentralizados para gerentes e também para agentes, passando, deste modo, a envolver um grande número de elementos da rede como entidades de gerenciamento. Tais entidades são organizadas hierarquicamente, com a presença de uma entidade principal num nível superior, e entidades adicionais em um ou mais níveis inferiores.

Por fim, o paradigma denominado **cooperativo fortemente distribuído** (MARTIN-FLATIN, 2003) também descentraliza o processamento e a inteligência de gerenciamento para um grande número de elementos da rede. Neste paradigma, contudo, não há hierarquia entre as entidades de gerenciamento.

Por serem amplamente utilizados atualmente, o paradigma centralizado e o paradigma hierárquico fracamente distribuído serão referidos neste documento como **paradigmas tradicionais**.

1.1 Definição do Problema e Motivação

Nos dias de hoje, com o aumento em tamanho e complexidade das redes atuais, as limitações dos modelos de gerenciamento baseados nos *paradigmas centralizado e fracamente distribuído* se tornam ainda mais acentuadas. Em adição a estas limitações, existem atualmente contextos de rede (denominados ***contextos modernos*** neste documento) que, por apresentarem certas peculiaridades, impossibilitam o gerenciamento apropriado de suas redes por tais modelos de gerenciamento. Tais contextos, como será analisado posteriormente neste documento, exigem o atendimento a requisitos tais como a necessidade das atividades de gerenciamento serem executadas em múltiplos pontos simultaneamente ou a presença de múltiplos domínios administrativos demandando a cooperação entre estes para a execução de suas operações.

Estas limitações e requisitos diferenciados encontrados em redes atuais trazem a necessidade do emprego de modelos de gerenciamento baseados nos paradigmas fortemente distribuídos. Contudo, como se discutirá adiante, embora modelos de gerenciamento seguindo tais paradigmas tenham sido propostos e discutidos há diversos

anos (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000) (MARTIN-FLATIN; ZNATY; HUBAUX, 1999) (MARTIN-FLATIN, 2003), tais modelos raramente foram aplicados no gerenciamento de redes reais e poucos exemplos concretos de sua utilização em ambientes de produção são encontrados nos dias de hoje. Afigura-se, deste modo, importante investigar modelos alternativos de gerenciamento fortemente distribuídos que atendam aos requisitos de gerenciamento das redes atuais.

Uma tecnologia que desponta como uma promissora alternativa para o desenvolvimento de um modelo de gerenciamento com tais características é a tecnologia *peer-to-peer* (P2P) (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004) (LUA et al, 2005) (MILOJICIC et al, 2003). Esta tecnologia possui como características relevantes, entre outras, a descentralização, a auto-organização, a transparência e o suporte a facilidades para compartilhamento de recursos e colaboração, sendo empregada em diferentes contextos, tais como sistemas de compartilhamento de arquivos, sistemas de armazenamento distribuído, sistemas de colaboração, etc. A tecnologia P2P tem sido largamente utilizada em diversas áreas de aplicação nas redes reais, de produção, o que reforça sua relevância de ser investigada para o desenvolvimento de tal modelo.

A presente Tese versa sobre estes tópicos. Como será detalhado na seção a seguir, aborda, como seu primeiro objetivo, as limitações dos modelos tradicionais para o gerenciamento de contextos de redes atuais com características modernas. Discute, a seguir, como seu segundo objetivo, a investigação do uso da tecnologia P2P como infra-estrutura para o gerenciamento de redes, com vistas a analisar se um modelo de gerenciamento distribuído baseado nesta tecnologia se apresenta como uma alternativa adequada para o gerenciamento das redes atuais. Na perspectiva enfocada neste trabalho, a rede P2P é vista como uma infra-estrutura que pode ser utilizada para prover suporte para a realização das operações de gerenciamento, permitindo a realização destas de um modo fortemente distribuído. Deste modo, as características inovadoras introduzidas pela utilização de redes P2P podem ser empregadas para aperfeiçoar a forma pela qual as operações de gerenciamento são realizadas, agregando a este modelo de gerenciamento os serviços já encontrados em tais redes P2P. Por fim, aborda, como seu terceiro objetivo, a classificação deste modelo segundo os paradigmas de gerenciamento propostos na literatura.

1.2 Objetivos da Tese

Esta Tese possui três objetivos principais:

I. Identificar e analisar porque os modelos de gerenciamento baseados nos paradigmas tradicionais possuem limitações para o gerenciamento de contextos de redes modernos.

Tal objetivo investigou a existência de *contextos modernos do ponto de vista de gerenciamento* nas redes atuais, isto é, contextos de rede que possuem particularidades distintas das encontradas em contextos tradicionais e que, em virtude disto, possuem requisitos de gerenciamento específicos, não atendidos de modo apropriado pelos modelos de gerenciamento utilizados tradicionalmente. Os contextos modernos representam limitações adicionais ao emprego de modelos tradicionais para o gerenciamento das redes atuais,

em adição às limitações de escalabilidade e tolerância a falhas discutidas anteriormente.

Os itens que foram endereçados para alcançar este objetivo compreenderam:

a. Realização de um levantamento do estado da arte em gerenciamento de redes distribuído. Estudo da terminologia empregada na área e das principais taxonomias propostas na literatura.

b. Estudo e análise de redes atuais para identificação de contextos modernos de rede do ponto de vista de gerenciamento. Identificação e revisão de três contextos modernos selecionados como estudos de caso.

c. Definição de uma metodologia para análise dos contextos modernos de redes do ponto de vista de gerenciamento. Tal metodologia auxilia a identificação dos paradigmas e dos modelos adequados para o gerenciamento do contexto em análise, com enfoque em particularidades distintas das encontradas nos contextos de redes tradicionais e que demandam requisitos de gerenciamento não atendidos de modo apropriado pelos modelos tradicionais.

d. Análise, seguindo esta metodologia, dos três contextos modernos selecionados como estudos de caso, com o objetivo de identificar as limitações dos modelos tradicionais para o gerenciamento de cada contexto e os modelos apropriados para este gerenciamento.

II. Investigar o uso de um modelo de gerenciamento distribuído baseado em P2P para o gerenciamento das redes atuais.

Tal objetivo investigou o emprego da tecnologia P2P como infra-estrutura para prover suporte para a realização das operações de gerenciamento, analisando ainda como estas são realizadas com forte distribuição valendo-se desta infra-estrutura. O modelo investigado abordou o gerenciamento das redes atuais de modo amplo, enfocando não apenas o gerenciamento das redes atuais com *contextos modernos*, mas também o gerenciamento das redes atuais tradicionais, cujo gerenciamento por modelos baseados nos paradigmas centralizado e fracamente distribuído possui limitações de escalabilidade e tolerância a falhas.

Os itens que foram endereçados para alcançar este objetivo compreenderam, além de alguns itens já referidos, tais como os *itens I.a e I.d*:

a. Realização de um levantamento do estado da arte da tecnologia P2P, identificando as principais características da tecnologia e as arquiteturas de rede utilizadas.

b. Definição do modelo de gerenciamento distribuído baseado em P2P.

c. Definição da arquitetura para um ambiente de gerenciamento que materialize este modelo de gerenciamento em redes reais. Esta arquitetura enfocou como as operações de gerenciamento são realizadas no ambiente de modo fortemente distribuído, e como as

funcionalidades de gerenciamento são estruturadas em um ambiente baseado em P2P.

d. Realização de um levantamento das principais funcionalidades de gerenciamento pertinentes a tal ambiente e discussão sobre como a infra-estrutura P2P e a arquitetura fortemente distribuída suportada pelo ambiente podem ser empregadas para aperfeiçoá-las.

e. Identificação dos principais serviços estruturais que o ambiente de gerenciamento distribuído baseado em P2P deve oferecer. Análise das principais características de um destes serviços como exemplo.

f. Análise, como estudo de caso, de uma atividade de gerenciamento no ambiente distribuído baseado em P2P, empregada para a realização de duas funcionalidades de gerenciamento, propondo uma arquitetura para a realização destas.

g. Análise do modelo e da arquitetura baseados em P2P. Comparação destes com duas outras importantes abordagens de gerenciamento. Discussão do emprego da abordagem baseada em P2P para o gerenciamento de diferentes redes atuais.

III. Analisar como o modelo de gerenciamento distribuído baseado em P2P pode ser classificado segundo os paradigmas de gerenciamento.

Tal objetivo discutiu como o modelo proposto pode ser classificado e se as taxonomias existentes identificam as características do modelo de modo apropriado. Tal objetivo resultou ainda em uma importante contribuição desta Tese, como discutido na seção a seguir.

Os itens que foram endereçados para alcançar este objetivo compreenderam, além de alguns itens já referidos nos objetivos anteriores:

a. Análise da classificação taxonômica das soluções de gerenciamento requeridas para redes atuais considerando as principais taxonomias para paradigmas de gerenciamento de redes propostas na literatura. Identificação de limitações destas taxonomias para tal classificação.

b. Proposição de uma taxonomia para soluções de gerenciamento atuais.

c. Análise da taxonomia proposta, com classificação das soluções de gerenciamento para os três contextos modernos analisados como estudos de caso segundo esta taxonomia.

d. Classificação das soluções de gerenciamento baseadas no modelo de gerenciamento distribuído P2P segundo a taxonomia proposta.

Em virtude de limitações de escopo, não é objetivo deste trabalho:

- Definir a arquitetura do ambiente com outros enfoques que não o modo pelo qual as operações de gerenciamento são realizadas no ambiente, isto é, o modo como as funcionalidades são estruturadas e como suas atividades podem ser realizadas no ambiente baseado em P2P.

- Definir a arquitetura de um ou mais serviços estruturais que um ambiente de gerenciamento distribuído baseado em P2P deve oferecer: o escopo deste documento enfoca a análise das principais características de um serviço estrutural como exemplo (a saber, o serviço para envio de notificações, selecionado como exemplo a ser analisado entre os serviços estruturais), sem, porém, definir sua arquitetura para projeto e implementação.
- Definir a arquitetura das funcionalidades de gerenciamento de tal ambiente: o escopo deste documento enfoca a discussão de como a infra-estrutura P2P e a arquitetura fortemente distribuída suportada pelo ambiente podem ser utilizadas para aperfeiçoar estas funcionalidades. Como estudo de caso do ambiente, entretanto, uma atividade de gerenciamento, responsável por duas funcionalidades, será detalhada.

1.3 Principais Contribuições

As principais contribuições resultantes da presente Tese incluem:

- **Análise de fatores que tornam os modelos de gerenciamento baseados nos paradigmas tradicionais não apropriados para o gerenciamento de contextos modernos de rede**. Relacionadas a esta contribuição, algumas contribuições secundárias foram também obtidas, incluindo:
    - Definição de uma metodologia para análise de contextos modernos que auxilia a identificação dos paradigmas e dos modelos adequados para o gerenciamento de tais contextos.
    - Análise detalhada das características e dos requisitos de gerenciamento dos contextos modernos selecionados como estudos de caso.
    - Identificação dos fatores que tornam os modelos baseados nos paradigmas tradicionais não apropriados para o gerenciamento de cada um dos contextos modernos analisados. Análise das características dos modelos de gerenciamento apropriados para os contextos.

- **Definição e investigação de um modelo de gerenciamento distribuído baseado em P2P.**
- **Definição e investigação de uma arquitetura para um ambiente de gerenciamento distribuído baseado em P2P.** Esta arquitetura tem como enfoque o modo como as operações de gerenciamento são realizadas no ambiente, considerando como as funcionalidades são estruturadas e realizadas no ambiente baseado em P2P. Relacionadas a estas duas últimas contribuições principais, algumas contribuições secundárias foram também obtidas, incluindo:
    - Levantamento e discussão das principais funcionalidades de gerenciamento pertinentes a tal ambiente de gerenciamento.

- Identificação dos principais serviços estruturais que um ambiente de gerenciamento distribuído baseado em P2P deve oferecer. Análise das principais características de um destes serviços como exemplo.
- Análise, como estudo de caso, de uma atividade de gerenciamento no ambiente proposto, empregada para a realização de duas importantes funcionalidades de gerenciamento.
- Análise do modelo e da arquitetura baseados em P2P, incluindo a análise comparativa destes com outras duas importantes abordagens de gerenciamento distribuídas e a discussão do emprego destes para o gerenciamento de diferentes redes atuais.

- **Definição de uma taxonomia para soluções de gerenciamento que destaca as características e os requisitos requeridos nos modelos de gerenciamento atuais.** Relacionadas a esta contribuição, algumas contribuições secundárias foram também obtidas, incluindo:
  - Identificação de limitações das principais taxonomias propostas na literatura para a classificação das soluções de gerenciamento requeridas por redes atuais.
  - Classificação das soluções de gerenciamento para os três estudos de caso de contextos modernos segundo a taxonomia proposta.
  - Classificação das soluções de gerenciamento que seguem o modelo distribuído baseado em P2P segundo a taxonomia proposta.

Outras contribuições secundárias resultantes da presente Tese, relacionadas às quatro contribuições principais, incluem:

- Análise da terminologia empregada na área de gerenciamento de redes e definição de uma terminologia a ser empregada.
- Discussão acerca do emprego de modelos e de tecnologias propostos na literatura para o desenvolvimento de sistemas de gerenciamento fortemente distribuídos.
- Análise crítica das principais taxonomias de paradigmas de gerenciamento de redes propostas na literatura.

1.4 Organização deste Documento

Este documento está organizado do seguinte modo.

A **primeira parte deste documento** contém os princípios e fundamentos para a Tese proposta, apresentando o estado da arte e os conceitos necessários para a elaboração desta pesquisa, assim como uma análise crítica dos tópicos quando necessária. Esta parte compreende os capítulos 2 e 3.

O capítulo 2 apresenta a tecnologia P2P, discutindo sua definição, suas principais características e suas áreas de aplicações. Aborda, ainda, trabalhos relacionados que fizeram uso desta tecnologia para o gerenciamento de redes. O capítulo 3, por sua vez, discute os principais conceitos de gerenciamento de redes distribuído relevantes para a

realização dos objetivos desta tese. Este capítulo analisa a terminologia da área de gerenciamento de redes distribuído, apresenta as principais taxonomias de paradigmas de gerenciamento distribuídos propostas na área, realiza uma análise crítica destas taxonomias e apresenta uma discussão acerca do emprego e das limitações de modelos e de tecnologias propostos na literatura para o gerenciamento de redes baseado em paradigmas fortemente distribuídos.

A **segunda parte deste documento** compreende o **objetivo I da presente Tese**, fornecendo uma análise das principais limitações dos modelos de gerenciamento baseados nos paradigmas tradicionais para o gerenciamento de contextos modernos de rede, utilizando como estudo de caso alguns contextos modernos de rede. Esta parte inclui o capítulo 4. Tal capítulo introduz a existência de contextos modernos do ponto de vista de gerenciamento, identifica e revisa três destes contextos como estudos de caso, define uma metodologia para análise destes contextos e analisa tais contextos segundo tal metodologia.

A **terceira parte deste documento** compreende o **objetivo II da Tese**, investigando o uso de um modelo de gerenciamento distribuído baseado em P2P para o gerenciamento das redes atuais. Esta parte inclui os capítulos 5, 6, 7 e 8 deste documento.

O capítulo 5 aborda o modelo e a arquitetura de gerenciamento distribuído baseado em P2P. O capítulo propõe este modelo de gerenciamento, propõe a arquitetura de um ambiente de gerenciamento que materializa este modelo para redes reais, discute as principais funcionalidades estruturais e de gerenciamento em tal ambiente e analisa outros aspectos que poderiam ter sido enfocados na arquitetura.

O capítulo 6, por sua vez, analisa um dos principais serviços estruturais do ambiente de gerenciamento proposto: o serviço de envio de notificações. Tal capítulo apresenta o paradigma *publish-subscribe*, discute as principais características necessárias e desejáveis em tal serviço num ambiente como o proposto e apresenta algumas abordagens *publish-subscribe* baseadas em P2P existentes na literatura que podem ser investigadas para serem integradas ao ambiente.

O capítulo 7 aborda um estudo de caso para uma atividade de gerenciamento no ambiente de gerenciamento proposto, a saber, a atividade de *polling*, empregada para as funcionalidades de monitoração do estado dos recursos da rede e de coleta periódica de dados de desempenho. O capítulo apresenta a arquitetura para a realização de *polling* distribuído, discorre sobre as características desta, discute um protótipo desenvolvido e os experimentos realizados.

Por fim, o capítulo 8 analisa o modelo e a arquitetura baseados em P2P. Este capítulo apresenta uma análise comparativa da abordagem com duas outras importantes abordagens de gerenciamento, seguida por considerações sobre esta análise. Discute, por fim, o emprego da abordagem baseada em P2P para o gerenciamento de diferentes redes atuais, incluindo redes tradicionais e redes com características modernas.

A **quarta parte deste documento** compreende o **objetivo III da presente Tese**. Esta parte inclui a discussão acerca da classificação do modelo de gerenciamento baseado em P2P segundo os paradigmas de gerenciamento das taxonomias propostas na literatura. Inclui, também, contribuições adicionais decorrentes da análise desenvolvida, que resultaram na proposição de uma **nova taxonomia para paradigmas de gerenciamento de redes, que tem por propósito destacar as características e os**

requisitos requeridos nos modelos de gerenciamento atuais. Esta parte inclui o capítulo 9. Tal capítulo analisa as limitações das taxonomias propostas na literatura para a classificação das soluções de gerenciamento requeridas nos contextos de redes atuais, propõe uma taxonomia e a analisa, e discute a classificação das soluções baseadas no modelo de gerenciamento P2P segundo a taxonomia proposta.

Por fim, a **parte final deste documento** compreende sua conclusão, representada pelo capítulo 10. Este capítulo apresenta as conclusões obtidas com a presente Tese, discutindo ainda as suas contribuições e considerações finais.

2 TECNOLOGIA *PEER-TO-PEER*

Popularizada nos primeiros anos pela sua utilização em sistemas de compartilhamento de arquivos como Napster e Kazaa, a tecnologia *peer-to-peer* (P2P) (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004) (LUA et al, 2005) (MILOJICIC et al, 2003) (MELCHIORS, 2005) (ROCHA et al, 2004) tem sido empregada atualmente como base de operação para sistemas descentralizados com diversos enfoques de aplicação, incluindo comunicação e colaboração entre humanos, computação distribuída e armazenamento distribuído. Este capítulo apresenta uma revisão do estado da arte da tecnologia P2P, abordando os principais tópicos da tecnologia que serão relevantes para a compreensão do restante deste documento. A seção 2.1 discute os conceitos e as principais características da tecnologia. A seção 2.2 apresenta os tipos de abordagens P2P existentes e as principais categorias de aplicação para as quais a tecnologia P2P tem sido empregada. Por fim, a seção 2.3 aborda as principais pesquisas que fazem uso da tecnologia P2P para gerenciamento de redes.

2.1 Conceitos e Características da Tecnologia P2P

Sistemas P2P operam sobre uma rede *overlay* criada sobre a rede física de computadores, denominada **rede P2P**. As redes P2P compreendem uma rede virtual de computadores formada por nodos (ou nós) de software denominado ***peers***, que podem agir tipicamente como consumidores de recursos (clientes) e fornecedores de recursos (servidores) simultaneamente, emitindo requisições para outros *peers* e respondendo a requisições recebidas. Tais sistemas são caracterizados pelo compartilhamento de recursos computacionais (incluindo conteúdo, armazenamento, ciclos de CPU, etc.) sem requererem a intermediação de um servidor centralizado. A abordagem utilizada em sistemas P2P contrasta com a adotada em sistemas cliente-servidor, onde um pequeno número de servidores, usualmente com grande capacidade computacional, atende um grande número de clientes. A figura 2.1 esquematiza um exemplo de uma rede P2P executando sobre uma infra-estrutura de rede física.

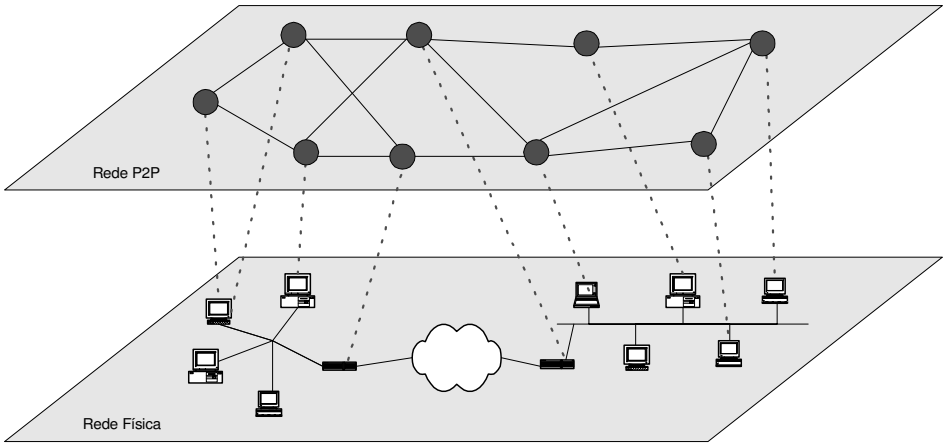


Figura 2.1: Esquema de uma rede P2P

Diferentes definições têm sido apresentadas para sistemas P2P na literatura. Tais definições variam de acordo com as características e as arquiteturas adotadas em tais sistemas, sem existir um consenso sobre um exato conceito a ser utilizado. Com enfoque apenas na arquitetura, as definições de sistemas P2P denominados "puros" incluem apenas sistemas totalmente distribuídos, em que todos os nodos são completamente equivalentes em termos de funcionalidade e tarefas que apresentam. Tais definições, contudo, podem ser consideradas excessivamente restritas, excluindo sistemas tipicamente considerados como sistemas P2P. Neste contexto, uma definição mais ampla, que considera a arquitetura e as características dos sistemas, é proposta em (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004) [traduzido]:

> Sistemas *peer-to-peer* são sistemas distribuídos que consistem em nodos interconectados aptos a se auto-organizarem em topologias de rede com o propósito de compartilharem recursos tais como conteúdo, ciclos de CPU, armazenamento e largura de banda, capazes de se adaptarem para falhas e acomodarem uma população transiente de nodos enquanto mantém conectividade e desempenho aceitáveis, sem requerem a intermediação ou suporte de um servidor ou autoridade global centralizada.

Para tais autores, assim, a definição de sistemas P2P inclui desde sistemas P2P puros, com arquitetura totalmente descentralizada (tal como as primeiras versões do Gnutella), até sistemas com arquitetura híbrida (tais como o Kazaa e a infra-estrutura JXTA), excluindo sistemas que dependem de um ou mais servidores globais centralizados para sua operação básica (tal como o Napster, que utiliza um índice global e realiza buscas neste índice).

Uma definição distinta e menos restrita segundo as arquiteturas englobadas, que enfoca as características e funcionalidades providas pela tecnologia, é adotada por Milojicic et al (MILOJICIC et al, 2003). Tais autores apontam que a tecnologia P2P envolve *compartilhamento*, oferecendo e recebendo recursos da comunidade de *peers*, onde um *peer* oferece alguns recursos e obtém em troca outros recursos. Apontam também que P2P compreende um modo de implementar sistemas baseado na noção da descentralização de sistemas, aplicações ou algoritmos. P2P representa um modo de utilizar a vasta quantidade de força computacional, armazenamento e conectividade de computadores distribuídos ao longo do mundo.

A apresentação da tecnologia P2P abordando a utilização e o compartilhamento de recursos descentralizados ao longo dos vários nodos da rede é também empregada por outros autores (GONG, 2001)(CHAN et al, 2007). Além disto, outros destacam de

modo mais específico a colaboração de todas as entidades da rede P2P para o fornecimento dos serviços básicos de rede, tais como compartilhamento de conteúdo, processamento ou armazenamento, destacando ainda que nestas redes todos os *peers* possuem capacidades equivalentes e um servidor central com maior poder de processamento não é mais necessário (ARNEDO-MORENO; HERRERA-JOANCOMARTI, 2009).

Neste capítulo, a fim de prover uma visão mais ampla da tecnologia P2P, serão discutidas as arquiteturas e as características dos sistemas P2P segundo as definições menos restritas, tal como a apresentada acima proposta por Milojicic et al, abrangendo inclusive os sistemas que necessitam de servidores globais centralizados para sua operação básica.

Diversas características são atribuídas para sistemas P2P. Tais características são, muitas vezes, relacionadas e influenciam-se umas às outras. Nem todas as características, contudo, estão presentes em todos os sistemas, assim como a relevância destas para o sistema varia de acordo com a arquitetura e os requisitos de cada sistema em particular. Entre as principais características, podem ser citadas (MILOJICIC et al, 2003) (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004):

- **Descentralização**. Representa uma das principais características de sistemas P2P. Diferentes graus de descentralização podem ser identificados em tais sistemas, estando relacionados com a arquitetura adotada. Em sua forma totalmente descentralizada, todos os participantes executam exatamente as mesmas tarefas, sem coordenação central de suas atividades. Tais sistemas são referenciados usualmente, com visto, como *sistemas P2P puros***.** Em outros sistemas, alguns nodos assumem funções mais importantes, agindo como coordenadores: é o caso, por exemplo, de arquiteturas que utilizam o conceito de *super-peers*, como será visto a seguir.

- **Escalabilidade**. Tipicamente, arquiteturas P2P possuem como característica inerente a escalabilidade (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004). Contudo, a descentralização empregada, assim como a topologia, a estrutura de rede e os mecanismos de roteamento e localização adotados influenciam a escalabilidade de tais sistemas. Além disto, a escalabilidade é influenciada pelo nível de comunicação requerido para o processamento computacional entre os *peers* do sistema: aplicações com nível de comunicação próximo de zero são extremamente escaláveis. Já em aplicações que exigem maior nível de comunicação, a escalabilidade é influenciada pela transferência de dados requerida para o processamento do sistema.

- **Tolerância a falhas**. A tolerância a falhas de sistemas P2P varia, assim como a escalabilidade, em função da topologia, da estrutura de rede e dos mecanismos adotados. Sistemas P2P puros não possuem um ponto central de falhas. Estão, porém, ainda sujeitos às desconexões de *peers* ou às falhas dos nodos, como ocorre nos demais sistemas distribuídos. Além disto, uma das características de redes P2P é a conexão intermitente de *peers*. Em virtude disto, sistemas P2P devem possuir mecanismos para tratar a desconexão dos nodos e se manterem operacionais enquanto existir um número suficiente de nodos no sistema. Os mecanismos de tolerância a falhas utilizados nos

diversos sistemas P2P variam conforme as funcionalidades e garantias requeridas por eles.

- **Suporte à conectividade intermitente de nodos e auto-organização.** Redes P2P possuem um conjunto variável de nodos, que se conectam e desconectam da rede a qualquer momento. Não permitem, assim, que se assegure se um determinado nodo estará ou não conectado em dado instante, o que requer mecanismos de tratamento nos sistemas P2P. Em sistemas de compartilhamento de arquivos, por exemplo, o acesso aos arquivos compartilhados será intermitente, sujeito à conectividade dos nodos provedores daquele conteúdo. Quando os sistemas precisam fornecer garantia de acesso ao conteúdo, uma técnica usual é a utilização de redundância. Sistemas P2P requerem ainda a capacidade de auto-organização em virtude da conexão intermitente dos nodos e dos requisitos de tolerância a falhas demandados.
- **Transparência**. Um dos objetivos dos sistemas distribuídos é fornecer transparência para aplicações, tal como a habilidade de conectar sistemas distribuídos de modo transparente, como se fosse um sistema local. A maior parte dos sistemas P2P fornece transparência utilizando funcionalidades do sistema de comunicação, do *middleware*, da infra-estrutura e dos protocolos.
- **Propriedade compartilhada dos recursos**. Sistemas P2P possuem a propriedade compartilhada dos recursos, o que reduz o custo de propriedade e a manutenção dos recursos empregados no sistema, já que este se divide entre todos os participantes da rede.
- **Anonimato**. A organização de sistemas P2P permite que estes ofereçam condições de anonimato para seus usuários, que pode ser utilizado para esconder a identidade do remetente da comunicação, a identidade do destinatário da conexão ou a identidade de ambos. A necessidade ou não de tal característica depende do sistema P2P sendo desenvolvido.

As redes P2P podem ser baseadas em diferentes arquiteturas de rede e roteamento, existindo diversas classificações para organizá-las (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004) (LUA et al, 2005) (MESHKOVA et al, 2008). Neste documento, foi adotada uma classificação que considera o grau de centralização e os algoritmos e os mecanismos utilizados para a estrutura da rede P2P, proposta com base nas apresentadas em (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004) e em (MESHKOVA et al, 2008). Esta classificação organiza as arquiteturas de rede P2P em quatro categorias:

- **Arquitetura de rede estruturada descentralizada**: redes onde a topologia é controlada e os arquivos (assim como ponteiros para os arquivos, quando existentes) são armazenados em localizações específicas, a fim de manter um mapeamento entre o conteúdo do arquivo e sua localização real na rede, com o objetivo de manter um mecanismo de busca eficiente. Exemplos incluem a *Content Addressable Network* (CAN) (RATNASAMY et al, 2001) e a Chord (STOICA et al, 2003).
- **Arquitetura de rede não-estruturada descentralizada**: redes onde todos os nodos executam exatamente as mesmas tarefas. Não há coordenação central para as atividades dos nodos, e não há a presença de nodos com

função de controle. Exemplos de redes P2P com tal arquitetura incluem as primeiras versões da rede Gnutella (DING; NUTANONG; BUYYA, 2005).

- **Arquitetura de rede centralizada**: redes que possuem um ou mais servidores de diretórios centralizados, responsáveis por funções tais como manter informações sobre os usuários conectados e manter a relação de arquivos que cada usuário está compartilhando na rede, juntamente com os meta-dados sobre tais arquivos. Um exemplo de sistema com tal arquitetura é o sistema Napster (DING; NUTANONG; BUYYA, 2005).
- **Arquitetura de rede híbrida**: redes que combinam características das demais arquiteturas. Diferentes abordagens podem ser utilizadas, sendo a utilização da técnica de *clustering* a mais popular (MESHKOVA et al, 2008), onde se destaca a arquitetura que faz uso de ***super-peers***. Os *super-peers* representam nodos escolhidos dinamicamente que assumem funções específicas, tais como indexação ou *cache*, e atendem a uma pequena parcela da rede. A topologia destas redes é, usualmente, formada por dois níveis, sendo o primeiro nível formado por *peers* ordinários que se conectam a um *super-peer*, com topologia centralizada, e o segundo nível formado por *super-peers*, com topologia descentralizada. Exemplos de redes com esta arquitetura incluem as utilizadas pelo sistema Kazaa (KAZAA, 2010) e pela plataforma JXTA (GONG, 2001).

2.2 Enfoques Adotados por Abordagens P2P

As abordagens P2P podem ser enquadradas em dois grupos principais: infra-estruturas e aplicações. Tais grupos, baseados nos propostos por alguns autores para sistemas de distribuição de conteúdo (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004), compreendem:

- **Aplicações**: abordagens P2P que provém aplicações, **desenvolvidas com um propósito específico**, tais como as aplicações para compartilhamento de arquivos (incluindo os sistemas Napster, Kazaa, Gnutella, eDonkey e BitTorrent) ou as aplicações para comunicação (incluindo as aplicações para mensagem instantânea) (MILOJICIC et al, 2003) (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004). Como discutem Paller e Kokkinen, as aplicações P2P possuem muitas vezes o protocolo P2P e o *middleware* associado suportando as necessidades de apenas um tipo específico de aplicação, sendo muito difícil executar um tipo diferente de aplicação no topo deste protocolo e *middleware*. Os protocolos P2P específicos para aplicações (sendo estes designados principalmente para compartilhamento de arquivos) representam os protocolos P2P mais amplamente difundidos (PALLER; KOKKINEN, 2008).
- **Infra-estruturas**: abordagens P2P desenvolvidas para prover serviços e aplicações básicas que habilitam a execução de outras aplicações sobre a rede P2P. Tais infra-estruturas podem **enfocar áreas e propósitos específicos de aplicação** (tais como infra-estruturas com enfoque apenas em colaboração ou em distribuição de conteúdo) (MILOJICIC et al, 2003) (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004), ou podem **possuir um propósito geral**, tal como seguido pelo JXTA (GONG, 2001) e pelo

CAESAR (CHAN et al, 2007). Alguns autores denominam as abordagens P2P de infra-estrutura através do termo *plataforma* (MILOJICIC et al, 2003) (MAUTHE; HUTCHISON, 2003), enquanto outros a indicam através do termo *framework* (MESHKOVA et al, 2008) ou pelo termo *middleware* (CHAN et al, 2007). Além de abordagens P2P que implementam a infra-estrutura propriamente dita, abordagens P2P de propósito geral para abstrair a infra-estrutura na camada base são também propostas (PALLER; KOKKINEN, 2008) (BROGI et al, 2008). Tais abordagens visam prover uma camada de abstração que pode se adequar em uma ou mais infra-estruturas P2P, sendo denominadas e propostas de diferentes modos, incluindo como *middleware* (BROGI et al, 2008) e como uma *API* (PALLER; KOKKINEN, 2008).

Os grupos acima não representam categorias mutuamente excludentes: algumas abordagens P2P possuem características que atendem ambos os grupos, representando infra-estruturas P2P em um nível e, simultaneamente, provendo aplicações finais.

Abordagens P2P têm sido empregadas para diversos objetivos, podendo abranger uma única ou múltiplas categorias de utilização simultaneamente. Diferentes categorias são indicadas na literatura para apresentar as abordagens P2P, não existindo consenso sobre como as abordagens devem ser agrupadas. Entre as categorias apresentadas (MAUTHE; HUTCHISON, 2003) (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004) (MILOJICIC et al, 2003) (GASPARY et al, 2007) (ROCHA et al, 2004), podem ser citadas:

- **Compartilhamento de arquivos:** compreende as abordagens P2P designadas para a troca de conteúdo entre usuários, também referenciada por alguns autores como parte das abordagens para *distribuição de conteúdo* (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004). Esta categoria inclui algumas das aplicações P2P mais conhecidas, tais como os sistemas Napster, Kazaa, Gnutella, eDonkey e BitTorrent. Um estudo detalhado sobre sistemas P2P de distribuição de conteúdo pode ser obtido em (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004).
- **Comunicação e colaboração:** inclui as abordagens P2P que fornecem a infra-estrutura para a comunicação e a colaboração entre *peers*, usualmente em tempo real. As aplicações desta categoria abrangem desde os sistemas para envio de mensagens instantâneas até as aplicações para colaboração em ambientes educacionais e corporativos, tal como o Groove.
- **Computação distribuída:** abrange as abordagens P2P que fazem uso do poder de processamento disponível nos *peers* para a execução de tarefas computacionais. Exemplos de aplicações P2P desta categoria incluem o SETI@home e o genome@home.
- **Armazenamento distribuído:** inclui as abordagens P2P que proporcionam o armazenamento de dados de modo seguro e persistente. Restrições e mecanismos de controle de acesso são usualmente empregados para prover a segurança das informações, assim como técnicas de replicação (WILLIAMS et al, 2007) são freqüentemente utilizadas para proporcionar maior disponibilidade dos dados. Exemplos de abordagens P2P desta categoria incluem o OceanStore e o PAST.

- **Serviços para Internet**: compreendem as abordagens que fazem uso da tecnologia P2P para oferecer suporte para serviços de Internet, tais como as aplicações e as infra-estruturas de segurança para detecção de ataques de negação de serviço (ZHANG; PARASHAR, 2006). Sistemas *multicast* P2P são também enquadrados nesta categoria por alguns autores (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004), enquanto outros enquadram tais sistemas na categoria de comunicação (MAUTHE; HUTCHISON, 2003) ou como uma categoria isolada (GASPARY et al, 2007).

2.3 Tecnologia P2P Aplicada ao Gerenciamento de Redes

O uso da tecnologia P2P para a área de gerenciamento de redes tem sido investigado em algumas pesquisas, sendo empregado com diferentes enfoques.

State e Festor (STATE; FESTOR, 2003) propõem um *framework* de gerenciamento de redes que se baseia na infra-estrutura P2P JXTA (GONG, 2001) para a integração da arquitetura de gerenciamento distribuído, enfocando a dependência de serviços oferecidos e consumidos entre os *peers* da abordagem. A tecnologia *Java Management Extensions* (JMX) (SUN MICROSYSTEMS, 2002) é utilizada sobre a infra-estrutura JXTA como um *framework* de agentes, e cada agente para um equipamento ou serviço gerenciado é estruturado empregando esta tecnologia. A infra-estrutura JXTA é utilizada para o anúncio e o consumo de serviços entre *peers*. Os autores propõem mecanismos para o emprego de dependências entre serviços, descrevendo uma extensão para o anúncio de serviços do JXTA de modo a incluir tais dependências. Descrevem ainda a API para as operações de gerenciamento das entidades de software agente e gerente baseadas em JMX, incluindo as classes da abordagem para o projeto de software destas entidades.

Um *framework* para testes e monitoração de Qualidade de Serviço é apresentado por **Binzenhölfer et al (BINZENHÖLFER et al, 2006) (BINZENHÖLFER et al, 2005)**. A arquitetura do *framework* é composta por agentes homogêneos que formam uma rede *overlay* de gerenciamento baseada no Kademlia, abordagem P2P que utiliza uma *Distributed Hash Table* (DHT) para organizar a rede *overlay*. O *framework* é concebido para prover funcionalidades para uma estação de gerenciamento central. Cada nodo contém módulos de teste que representam as funcionalidades do nodo. Um módulo pode conter testes locais, tais como testes para o hardware e a conectividade da rede TCP/IP, e testes distribuídos, realizados em conjunto com outro nodo da rede *overlay*, tais como solicitações para o outro nodo executar um comando *ping*, executar um *port scan* no nodo requisitante ou coletar medidas da vazão no envio de tráfego entre eles. O propósito principal do emprego da rede *overlay* é prover a conectividade lógica entre os nodos do *framework*, fazendo uso das propriedades de auto-organização das redes P2P, e permitir que um nodo encontre outro em um período de tempo razoável independente do número IP do nodo ou do provedor a que este faz parte.

Outra pesquisa que aborda o uso de redes P2P para o gerenciamento de redes é apresentada por **Kamienski et al (KAMIENSKI et al, 2006)**. Tais autores propõem um *framework* para *Policy-based Management* (PBM, gerenciamento baseado em políticas) baseado na tecnologia P2P, denominado *Peer-to-Peer Policy Management Infrastructure* (P4MI). A arquitetura do *framework* compreende, entre outros, uma rede de servidores de políticas (denominada PDN) e agentes de políticas. Os servidores de

políticas interagem através de uma rede P2P baseada em uma DHT, enquanto a interação entre os servidores de políticas e os agentes de políticas segue uma abordagem P2P baseada em *super-peers*. O conjunto da rede forma, assim, uma rede P2P com arquitetura híbrida onde os *super-peers* comunicam-se através da rede DHT. A comunicação entre os agentes de políticas, por sua vez, é feita diretamente uns com os outros em uma abordagem P2P.

Alguns autores enfocam ainda o uso de redes *overlay* para a disseminação e a agregação de informações de gerenciamento coletadas nos recursos da rede. Entre estes, **Dam e Stadler (DAM; STADLER, 2005)** propõem um protocolo denominado GAP (*Generic Aggregation Protocol*) que permite que uma estação de gerenciamento receba continuamente o valor agregado de variáveis dos equipamentos da rede. É assumido que cada equipamento da rede executa um processo que suporta este protocolo, internamente ou em um equipamento externo associado. A comunicação entre os processos dos diversos equipamentos é realizada através de uma rede *overlay*. O protocolo é baseado em um algoritmo distribuído que constrói e mantém um gráfico da rede em formato de árvore que se estende ao longo da rede *overlay*, usando esta árvore para propagar e agregar os valores em direção ao nodo raiz. O modelo de execução do protocolo assume um conjunto de serviços de níveis inferiores da rede *overlay* incluindo detecção de falhas em um nodo vizinho, descoberta de nodos vizinhos, entrega de mensagens, assim como serviços para mensagens entre vizinhos para informar a atualização de um valor agregado.

Uma extensão do protocolo GAP é apresentada por **Pietro e Stadler (PIETRO; STADLER, 2007)**, denominada A-GAP. Este protocolo usa um esquema de filtros para propagar as mensagens ao longo da árvore de agregação, enviando mensagens de agregação apenas quando uma diferença mínima entre o valor corrente e o último valor atualizado é atingida. Funcionalidades de criação e manutenção da árvore de agregação, incluindo entrada, saída e falhas em nodos, e funcionalidades para agregação parcial dos valores são herdadas do protocolo GAP.

Outra pesquisa é apresentada por **Yalagandula et al (YALAGANDULA et al 2006)**, que faz uso de um algoritmos baseado em uma DHT para a agregação e a disseminação de informações de gerenciamento coletadas em tempo real. Os autores propõem um serviço para a obtenção de medidas e estimativas para um sistema de gerenciamento e monitoração, concebido para grandes sistemas de rede. A arquitetura proposta engloba três componentes: *Sensor Pods, Sensing Information Management Backplane* e *Scalable Inference Engines*. Um *Sensor Pod* compreende um conjunto de sensores de medida e monitoração que coletam informações na máquina, provendo interfaces Web Services para consulta das informações coletadas pelos diferentes sensores e para configuração das medidas a serem obtidas (tais como sensores a serem invocados, freqüência, período). O *Sensing Information Management Backplane* representa um *middleware* para agregação e gerenciamento de dados que coleta os dados medidos dos sensores individuais e provê um substrato para programação de serviços de aplicações agregarem os dados. Este componente faz uso de um sistema distribuído que emprega algoritmos baseados em DHT para a agregação e disseminação das informações. Por fim, as *Scalable Inference Engines* são componentes que estimam informações completas de uma métrica de rede baseada em medidas parciais obtidas de sensores.

Publicações abordando o uso da tecnologia P2P para gerenciamento de redes têm sido apresentadas pelo grupo de pesquisa em que este presente trabalho faz parte e estão

inseridas no contexto desta pesquisa. Em (GRANVILLE; ROSA; PANISSON; MELCHIORS; ALMEIDA; TAROUCO, 2005), foi apresentado um modelo inicial para o gerenciamento de redes distribuído baseado em P2P, modelo este que foi aprimorado na presente pesquisa, e foram discutidas facilidades proporcionadas pelo gerenciamento baseado em P2P, quais sejam, cooperação entre administradores humanos, conectividade aprimorada para troca de mensagens e balanceamento de carga para as atividades de gerenciamento. O documento proposto em (PANISSON; ROSA; MELCHIORS; GRANVILLE; ALMEIDA; TAROUCO, 2006), por sua vez, apresenta o *framework* ManP2P, que pode ser empregado para a implementação de *peers* que materializam uma entidade de gerenciamento. Este documento discute os componentes de um *peer* concebido no *framework* e os detalhes de projeto de tais componentes, enfocando como desenvolver um *peer* de gerenciamento de redes utilizando o *framework* JXTA (GONG, 2001). O *framework* ManP2P é utilizado para o desenvolvimento do protótipo apresentado no capítulo 7. Por fim, **Panisson (PANISSON, 2007)** detalha em sua dissertação de mestrado a distribuição de carga de tarefas de gerenciamento, assim como aspectos do *framework* ManP2P, enquanto **Rosa (ROSA, 2007)**, também em sua dissertação de mestrado, discute a cooperação entre humanos com o uso de times virtuais.

Além das pesquisas acima, relacionadas ao modelo para gerenciamento de redes distribuído baseado em P2P, outras pesquisas relativas ao uso de P2P para a área de gerenciamento de redes foram também desenvolvidas por pesquisadores do grupo. Entre estes, **Marquezan** aborda em sua tese de doutorado o uso de P2P em gerenciamento autonômico, investigando se a combinação de propriedades *self*-* e abordagens P2P aprimoram a execução de atividades de gerenciamento (MARQUEZAN et al, 2010) (MARQUEZAN et al, 2008). Por fim, **Santos (SANTOS, 2008)** analisa em sua dissertação de mestrado o uso de serviços de presença em conjunto com sistemas P2P.

2.4 Considerações Finais

Este capítulo discorreu sobre a tecnologia P2P, apresentando seu conceito, características, tipos de abordagens e categorias de aplicação. Abordou, ainda, as principais pesquisas que aplicam a tecnologia P2P para o gerenciamento de redes, área onde o presente trabalho está enquadrado.

O capítulo a seguir, por sua vez, aborda a revisão do estado da arte e os principais conceitos da área de gerenciamento de redes distribuídos.

3 GERENCIAMENTO DE REDES DISTRIBUÍDO

Nas últimas duas décadas, o gerenciamento de redes (CLEMM, 2007) (COMER, 2006) (HEGERING; ABECK; NEUMAIR, 1999) (UDUPA, 1996) tem passado por grande evolução. As abordagens iniciais utilizadas para o gerenciamento de redes deram lugar a diversas formas de acessar e controlar os recursos gerenciados de modo distribuído, baseadas em diferentes arquiteturas e tecnologias. Entre estas, algumas se tornaram amplamente utilizadas nas redes reais; outras foram objeto apenas de pesquisas, com poucas aplicações em ambientes de produção.

Este capítulo discute os principais conceitos de gerenciamento de redes distribuído requeridos para a compreensão deste documento, apresentando, quando pertinente, uma análise crítica dos tópicos abordados. A seção 3.1 discute a terminologia definida para o documento. As seções 3.2 e 3.3 abordam as principais taxonomias de gerenciamento de redes propostas na literatura, apresentando ainda uma análise crítica destas taxonomias. A seção 3.4 discute o emprego de modelos e de tecnologias propostos na literatura para o gerenciamento de redes baseado em paradigmas fortemente distribuídos. Por fim, a seção 3.5 apresenta as considerações finais do capítulo. Este capítulo é complementado pelo Apêndice A, que apresenta as principais tecnologias propostas para utilização no gerenciamento de redes.

3.1 Estudo sobre a Terminologia da Área de Gerenciamento Distribuído

Na área de Computação, freqüentemente o mesmo termo é utilizado para expressar diferentes conceitos de acordo com cada contexto específico. Adicionalmente, muitas vezes, diferentes termos são utilizados para expressar o mesmo significado. A fim de aprimorar o entendimento deste documento, esta seção apresenta a definição dos termos utilizados ao longo desta Tese que se enquadram nestas situações.

Há uma grande alternância entre os termos "***paradigma***" e "***modelo***" ao discutir abordagens de gerenciamento de redes. Neste documento, o termo *paradigma* será empregado para definir em alto nível a abordagem utilizada para estruturar conceitualmente as operações de gerenciamento de redes ou a abordagem de comunicação. Será utilizado, assim, para a apresentação dos *paradigmas de gerenciamento de redes*, tais como o *paradigma de gerenciamento de redes centralizado* e o *paradigma de gerenciamento de redes fracamente distribuído hierárquico* (vide seção 3.2). Será utilizado, também, para apresentar o *paradigma gerente-agente* (apresentado a seguir) e os *paradigmas de código móvel* (vide seção A.2.1).

Por outro lado, o termo *modelo* será utilizado ao definir uma visão conceitual de baixo nível das entidades que compõem a estrutura de gerenciamento de redes e como estas entidades são organizadas. Neste contexto, um *modelo* representa um dos possíveis modos de empregar um paradigma em direção ao mundo real utilizando alguma solução existente no domínio, freqüentemente sendo baseado em uma ou mais tecnologias específicas. Neste documento, o termo modelo será utilizado, por exemplo, ao discutir o *modelo de gerenciamento de redes distribuído baseado em P2P* (vide capítulo 5).

Por fim, o termo "***arquitetura***" será empregado para discutir a estrutura que materializa *modelos* no mundo real. Neste documento, será empregado para definir como aplicar o *modelo de gerenciamento distribuído baseado em P2P* no gerenciamento de redes reais.

Relacionado está o termo "***tecnologia***". Tecnologias são utilizadas para implementar no mundo real modelos e arquiteturas definidos. A tecnologia SNMP (vide seção A.1.1), por exemplo, é empregada nos modelos do *framework* de gerenciamento Internet.

Outro termo que necessita ser discutido é o termo "***agente***", utilizado com diferentes propósitos e significados nas diversas áreas da Computação. Na área de gerenciamento de redes, este termo é usualmente empregado com relação ao **paradigma gerente-agente**. Neste paradigma, o gerente é responsável por contatar agentes e obter um conjunto de objetos de gerenciamento. Estes objetos representam as informações dos recursos gerenciados, escondendo do gerente os detalhes de implementação para manipulação destas informações. Além de responder a requisições de gerentes, os agentes podem ainda enviar mensagens assincronamente para gerentes reportando a ocorrência de algum evento. Os exemplos mais significativos deste paradigma são a arquitetura de gerenciamento OSI Systems Management (OSI-SM) e a arquitetura de gerenciamento Internet. Esta última, por exemplo, envolve os agentes que seguem o *Simple Network Management Protocol* (SNMP) (HARRINGTON; PRESUHN; WIJNEN, 2002), referidos como *agentes SNMP*.

A partir do paradigma gerente-agente, o termo agente passou a ser utilizado com dois enfoques em gerenciamento de redes. Por um lado, o agente representa o *papel* que a entidade assume no gerenciamento, sendo responsável por responder a requisições de entidades gerentes sobre os recursos gerenciados e notificar entidades gerentes na ocorrência de eventos imprevistos. Por outro lado, o agente representa um *software que encapsula os recursos gerenciados e oferece uma interface de acesso unificada para estes recursos*.

A utilização do termo *agente* com enfoque no *papel* que a entidade assume é freqüentemente encontrada ao abordar paradigmas de gerenciamento, onde há, em alguns paradigmas, a introdução de entidades que assumem duplo papel (gerente e agente) simultaneamente. Alguns autores (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000) optam por evitar até mesmo definir os termos *gerente* e *agente* se referindo a entidades que desempenham funções de gerenciamento (gerentes) e entidades que executam funções mundanas (agentes), já que atualmente os agentes assumem em muitas arquiteturas de gerenciamento mais responsabilidades que nas arquiteturas tradicionais. Tais autores, assim, definem "gerentes como uma entidade que necessita se comunicar com outras entidades (tipicamente os agentes) para executar suas tarefas" e que um "agente, em contraste, pode executar sozinho as tarefas atribuídas para

ele" [traduzido] (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000). Adicionalmente, observa-se que, mesmo com enfoque no *papel* que a entidade assume, dois significados são evocados para o termo agente: *identificar as entidades que tem como papel executar funções mundanas, sem inteligência de gerenciamento, tipicamente assumindo o papel de meros fornecedores de dados no modelo de gerenciamento*; e *identificar entidades que executam suas funções sem necessitar de outras entidades, podendo, assim, assumir muito mais responsabilidades que meros fornecedores de dados*, tal como adotado pelos autores acima referenciados.

Por outro lado, há também, como apresentado acima, a utilização do termo *agente* com intuito de destacar os *módulos de software que provêem o encapsulamento das informações de gerenciamento, fornecendo um ponto de acesso único para acessá-las*. Alguns autores (PAVLOU, 2007), por exemplo, ao definir uma taxonomia que classifica as tecnologias de gerenciamento de redes, criam uma categoria que abrange as tecnologias que são invocadas remotamente, com duas subcategorias: uma para invocação de objetos gerenciados através de um *agente* e outra para invocação de objetos gerenciados diretamente através de tais objetos (vide seção 3.3.2).

Além dos diferentes contextos e significados para o termo *agente* vistos acima, empregados para a área de gerenciamento de redes, o termo *agente* é também utilizado para definir *agentes móveis*, uma abordagem de código móvel que é caracterizada por uma unidade de execução que migra seu código e alguns resultados intermediários de um nodo para outro (vide seção A.2.4). Por fim, outro uso do termo *agente* está relacionado a *agentes inteligentes*, uma abordagem originada dos domínios Inteligência Artificial Distribuída (IAD) e Sistemas Multiagentes (vide seção A.3).

Neste documento, quando o termo *agente* aparecer de modo isolado e sem explicações complementares, ele será utilizado para *agentes* no contexto de gerenciamento de redes, com enfoque no papel que a entidade assume no gerenciamento.

Por fim, diferentes usos e interpretações são empregados na área de gerenciamento para o conceito de "***hierarquia"*** entre entidades. Muitas vezes, o conceito é empregado para definir o *modo como as entidades são estruturadas de acordo com as funcionalidades desempenhadas por cada entidade*. Este é uso empregado, por exemplo, por (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000) ao definir as entidades pertencentes a um sistema de gerenciamento e seus papéis de gerente, agente e entidade com duplo papel. Como será visto na seção 3.2.2, tais autores explicam que a disposição destes papéis implica em uma estrutura hierárquica do sistema, onde há a presença de gerentes de nível superior, no topo da hierarquia; a presença de agentes, na base da hierarquia; e a presença de entidades de duplo papel, chamadas de gerentes de nível intermediário, nos níveis intermediários da hierarquia.

Com enfoque um pouco distinto e mais restrito, o conceito de *hierarquia* é empregado para expressar não apenas o modo como as entidades são estruturadas e como a comunicação é desempenhada, *mas também as relações de autoridade e subordinação existentes entre as entidades*. Neste caso, a hierarquia supõe a expressa subordinação de uma entidade em relação à outra: a entidade subordinada não possui autonomia para, por exemplo, optar por executar ou não uma atividade solicitada. Cabe destacar que, muitas vezes, os limites para a interpretação do conceito não são claramente determinados. Em certos casos, por exemplo, o conceito de hierarquia é utilizado misturando parcialmente as duas interpretações e sem definir expressamente a

presença ou ausência de autonomia para a realização das atividades em entidades subordinadas.

Um exemplo de utilização do conceito que expressa relações de subordinação pode ser encontrado em (MARTIN-FLATIN, 2003). Tal autor, como será visto na seção 3.2.1, define que paradigmas hierárquicos empregam delegação vertical, onde um gerente de nível superior delega uma tarefa para seu subordinado no nível imediatamente inferior.

Neste documento, a fim de que os diferentes usos do termo sejam diferenciados, quando não explicitado, o conceito de *hierarquia* será empregado no seu enfoque mais geral, isto é, como modo de estruturar as entidades e estruturar como a comunicação é desempenhada. Por outro lado, quando o termo for empregado com enfoque específico de autoridade e subordinação, será definida a existência de uma hierarquia com esta forma de relacionamento. Neste caso, por exemplo, o termo ***hierarquia administrativa*** será empregado para situações em que estiver sendo considerada a relação de autoridade de uma equipe ou domínio administrativo sobre outro.

3.2 Taxonomias para Paradigmas de Gerenciamento de Redes

As primeiras abordagens tradicionais de gerenciamento foram baseadas em uma entidade com papel de gerente e diversas entidades com papel de agente, que seguiam o paradigma gerente-agente. Com o passar dos anos e o aumento da complexidade das necessidades de gerenciamento, este paradigma passou a ser estendido para outras arquiteturas mais elaboradas. Um exemplo é a introdução de entidades que assumem o papel de gerente e agente simultaneamente e podem ser utilizadas como gerentes intermediários, dando origem aos paradigmas de gerenciamento hierárquicos.

Atualmente, diversos paradigmas são seguidos pelos modelos e arquiteturas de gerenciamento de redes. Esta seção apresenta as principais taxonomias propostas para *descrever os paradigmas de gerenciamento* conforme a distribuição empregada por estes, considerando aspectos como *a estrutura, os papéis e os modos de interação das entidades*. Inicialmente, é apresentada a taxonomia simples proposta por Martin-Flatin, Znaty e Hubaux, seguida pela taxonomia proposta por Schönwälder, Quittek e Kappler. A seção 3.3 apresentará outras importantes taxonomias de gerenciamento de redes que enfocam aspectos distintos, tais como a taxonomia aprimorada proposta por Martin-Flatin, Znaty e Hubaux e a taxonomia proposta por Pavlou.

3.2.1 Taxonomia Simples segundo Martin-Flatin, Znaty e Hubaux

Martin-Flatin, Znaty e Hubaux propõem duas diferentes taxonomias, apresentadas em (MARTIN-FLATIN; ZNATY; HUBAUX, 1999) e aperfeiçoadas em (MARTIN-FLATIN, 2003). A primeira taxonomia, denominada pelos autores como *taxonomia simples*, define paradigmas de gerenciamento de redes e é baseada na estrutura organizacional. A segunda taxonomia, denominada *taxonomia aprimorada*, possui enfoque distinto, com uma abordagem mais pragmática que objetiva indicar que paradigmas e tecnologias devem ser usados no contexto de uma dada organização, sendo baseada em quatro critérios. Esta seção abordará a *taxonomia simples*; a seção 3.3.1 abordará a *taxonomia aprimorada*.

A taxonomia baseada no modelo organizacional proposta pelos autores define quatro categorias de paradigmas: centralizado, hierárquico fracamente distribuído, hierárquico fortemente distribuído, e cooperativo fortemente distribuído.

O **paradigma centralizado** é definido pela presença de apenas um gerente, que concentra todo o processamento e a inteligência de gerenciamento, e um conjunto de diversos agentes limitados ao papel de simples coletores de dados. Este paradigma é seguido por tecnologias tais como SNMPv1 e o SNMPv2, apresentados na seção A.1.1.

O **paradigma hierárquico fracamente distribuído** é caracterizado pelo sistema de gerenciamento ser concentrado em poucos nodos da rede, existindo um conjunto numeroso de agentes limitados ao papel de simples coletores de dados. O paradigma segue a **delegação vertical** de tarefas, definida como uma forma de delegação onde um gerente do nível superior delega uma tarefa para um subordinado no nível inferior, descendo a hierarquia. Há, tipicamente, uma ou duas ordens de magnitude entre o número de entidades *espertas* e o número de entidades *coletoras de dados simples* envolvidas no gerenciamento. É seguido por tecnologias como o RMON em suas versões 1 e 2, apresentados na seção A.1.2.

No **paradigma hierárquico fortemente distribuído**, o processamento de gerenciamento é descentralizado para todos os gerentes e agentes, distribuídos hierarquicamente seguindo a delegação vertical de tarefas. Agora, tarefas de gerenciamento são atribuídas também para os agentes, que podem participar ativamente do sistema de gerenciamento. Os autores da taxonomia agrupam as tecnologias utilizadas para o desenvolvimento destes sistemas em dois grandes grupos: tecnologias que seguem o paradigma de código móvel e tecnologias que seguem o paradigma de objetos distribuídos. Exemplos de tecnologias que seguem este paradigma e são baseadas no paradigma de código móvel incluem os agentes móveis, apresentado na seção A.2.4. Exemplos de tecnologias que seguem este paradigma e são baseadas no paradigma de objetos distribuídos incluem CORBA, apresentada na seção A.1.3, e *JMX*, apresentada na seção A.1.4.

Por fim, no **paradigma cooperativo fortemente distribuído**, o processamento é descentralizado para todos os gerentes e agentes, assim como no paradigma hierárquico fortemente distribuído. Contudo, no paradigma cooperativo, utiliza-se **delegação horizontal**, definida como uma forma de delegação entre pares no mesmo nível da hierarquia. Este paradigma é definido como *orientado a objetivos* (MARTIN-FLATIN, 2003): os gerentes enviam aos agentes o objetivo da atividade — isto é, "porquê" devem executar esta atividade —, e os agentes tomam suas próprias decisões para definir "como" chegarão a este objetivo. Esta abordagem difere das utilizadas nas tecnologias de código móvel do paradigma hierárquico fortemente distribuído, nas quais os gerentes enviam programas aos agentes e estes os executam sem conhecer os objetivos desta atividade: gerentes enviam, assim, "como" executar a atividade, e não informam os agentes "porquê" as operações estão sendo feitas. O paradigma é descrito associado a abordagens de agentes inteligentes, originados da Inteligência Artificial Distribuída (MARTIN-FLATIN, 2003), apresentadas na seção A.3.

3.2.2 Taxonomia segundo Schönwälder, Quittek e Kappler

A taxonomia proposta por Schönwälder, Quittek e Kappler objetiva classificar os sistemas de gerenciamento distribuídos (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000). A classificação é baseada em um modelo que contém três papéis que as entidades podem assumir, sendo estes *gerentes* (entidades que necessitam comunicar-se com outras entidades para executar suas tarefas), *agentes* (entidades que podem executar suas tarefas sozinhas) e *entidades com duplo papel de gerentes e agentes*. Tais entidades organizam-se em um modelo com estrutura hierárquica implícita, onde *top-*

level managers (gerentes de nível superior) se encontram no topo da hierarquia e representam entidades gerentes, *mid-level managers* (gerentes de nível intermediário) se encontram nos níveis intermediários da hierarquia e representam entidades com duplo papel, e agentes se encontram no menor nível da hierarquia. Cada sistema de gerenciamento pode possuir todos ou alguns dos tipos de entidades, dando origem aos diferentes paradigmas de gerenciamento.

Esta taxonomia define quatro paradigmas (denominados como *classes* pelos autores): gerenciamento centralizado, gerenciamento fracamente distribuído, gerenciamento fortemente distribuído e gerenciamento cooperativo. O principal critério utilizado na taxonomia é o número relativo de entidades, onde m representa o número total de gerentes (incluindo gerentes de nível superior e gerentes de nível intermediário) e n representa o número total de entidades (resultantes da soma de m e o número de agentes). Os paradigmas são, deste modo, assim definidos: gerenciamento centralizado, com $m = 1$; gerenciamento fracamente distribuído, com $1 < m << n$; gerenciamento fortemente distribuído, com $1 << m < n$; e gerenciamento cooperativo, com $m \approx n$. A figura 3.1, extraída de (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000)[traduzida], esquematiza as estruturas dos diferentes paradigmas (classes) de sistemas de gerenciamento de redes, onde os círculos brancos indicam um gerente de nível superior, a elipse cinza indica um gerente de nível intermediário e o círculo preto indica um agente.

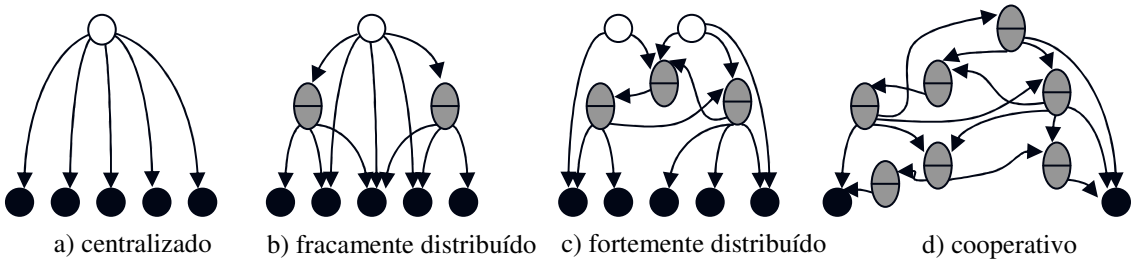


Figura 3.1: Estrutura das classes dos sistemas de gerenciamento (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000)

Além do critério principal, os autores apresentam quatro características secundárias que tipicamente mudam com os diferentes paradigmas de gerenciamento. A primeira característica é a conectividade C, definida como o número de pares de gerentes comunicando-se entre si, dividido pelo número total de gerentes existente. Em sistemas em que a conectividade é alta, gerentes são usualmente considerados cooperativos. A característica é, assim, tipicamente distribuída da seguinte forma entre os paradigmas: gerenciamento centralizado, $C = 0$; gerenciamento fracamente distribuído, $0 < C < 1$; gerenciamento fortemente distribuído, $1 \leq C << m$; gerenciamento cooperativo, $1 << C \leq m$.

A segunda característica secundária é a distribuição da complexidade das tarefas de gerenciamento para as entidades. No gerenciamento fracamente distribuído, tipicamente tarefas complexas são atribuídas para gerentes de nível superior, e tarefas simples são atribuídas para gerentes de nível intermediário. Por sua vez, no gerenciamento cooperativo, tipicamente a complexidade das tarefas de gerenciamento entre as entidades é mais balanceada.

A delegação dinâmica de tarefas de gerenciamento é a terceira característica secundária proposta. Esta característica indica se tarefas de gerenciamento podem ser atribuídas e alteradas dinamicamente, contrastando com os paradigmas tradicionais nos

quais as tarefas de gerenciamento são estáticas e atribuídas uma única vez. Usualmente associada com gerenciamento fortemente distribuído e com gerenciamento cooperativo, a delegação dinâmica de tarefas pode também ser utilizada em gerenciamento fracamente distribuído.

Por fim, a última característica secundária é a mobilidade dos processos de gerenciamento completos, implicando a mobilidade não apenas do código, mas também do estado de execução. A mobilidade dos processos usualmente ocorre no gerenciamento fortemente distribuído e no gerenciamento cooperativo; contudo, até mesmo o gerente de um sistema centralizado poderia mover entre máquinas.

Além da classificação baseada no critério principal e as características secundárias, os autores apresentam ainda propriedades adicionais típicas de cada paradigma de gerenciamento. A escalabilidade é uma destas propriedades, na qual, quanto mais distribuído um sistema de gerenciamento é, mais escalável ele se torna. Outra propriedade é a flexibilidade: se tarefas de gerenciamento podem ser atribuídas dinamicamente ou processos tornam-se móveis, o sistema de gerenciamento torna-se mais flexível, já que tarefas podem ser atribuídas ou alteradas com mais facilidade, assim como novas tarefas podem ser atribuídas em tempo real.

3.2.3 Análise Crítica das Taxonomias Apresentadas

As taxonomias apresentadas acima permitem *identificar os paradigmas de gerenciamento* seguidos por arquiteturas e sistemas de gerenciamento de redes conforme *suas características de distribuição, incluindo sua estrutura, os papéis e modos de interação das entidades de gerenciamento*.

Ambas as taxonomias definem quatro paradigmas de gerenciamento. A taxonomia simples de Martin-Flatin, Znaty e Hubaux define o paradigma centralizado, o paradigma hierárquico fracamente distribuído, o paradigma hierárquico fortemente distribuído e o paradigma cooperativo fortemente distribuído. Esta taxonomia indica expressamente que os paradigmas hierárquicos são baseados na delegação vertical, requerendo, deste modo, a presença de subordinação entre as entidades. Além disto, esta taxonomia apresenta a restrição de que o paradigma cooperativo fortemente distribuído é definido como baseado em objetivos e é sempre associado a agentes inteligentes.

A taxonomia de Schönwälder, Quittek e Kappler, por sua vez, é mais flexível, não abordando a presença de subordinação entre as entidades e enfocando apenas a estrutura hierárquica surgida pelas formas de comunicação entre as entidades. Seu critério principal, quantitativo, baseado no número de entidades com papel de gerente em relação ao número total de entidades, torna a taxonomia bastante abrangente, permitindo enquadrar as diversas arquiteturas e sistemas de gerenciamento.

Além de definir características de distribuição que permitem classificar arquiteturas e sistemas de gerenciamento, na taxonomia de Martin-Flatin, Znaty e Hubaux, os autores apresentam tecnologias relacionadas a cada paradigma, objetivando identificar que paradigma é implementado por dada tecnologia. Assim, sob este contexto, além de permitir classificar as arquiteturas de gerenciamento, tal taxonomia poderia ser utilizada também para classificar tecnologias de gerenciamento, permitindo atribuir uma tecnologia para um paradigma específico. Contudo, uma mesma tecnologia pode ser empregada para desenvolver sistemas que seguem diferentes paradigmas, como discutido em (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000). Assim, a utilização desta taxonomia para classificar tecnologias não se mostra intuitiva, já que uma

tecnologia poderia ser enquadrada em mais de um paradigma, o que não é considerado na taxonomia.

Comparando agora os paradigmas definidos pelas duas taxonomias propriamente ditos, embora apresentem critérios distintos para defini-los, ambas as taxonomias possuem similaridades nas categorias definidas que permitem compará-los através dos quatro paradigmas.

O *paradigma de gerenciamento centralizado* é similar em ambas as taxonomias, ambos indicando a concentração do gerenciamento em um único ponto. Os *paradigmas de gerenciamento fracamente distribuídos* definidos em cada taxonomia, por sua vez, possuem importantes similaridades, ambos representando a distribuição das atividades de gerenciamento ao longo de alguns pontos da rede. Os paradigmas de cada taxonomia, contudo, não são correspondentes em todas as ocorrências uma vez que Martin-Flatin, Znaty e Hubaux determinam expressamente a presença de delegação vertical neste paradigma (denominado paradigma hierárquico fracamente distribuído), enquanto Schönwälder, Quittek e Kappler optam por defini-lo apenas pela presença de um elevado número de entidades com função de gerente de nível intermediário, com duplo papel (denominando-o paradigma fracamente distribuído).

Restrição similar ocorre ao compararmos os *paradigmas fortemente distribuídos* das taxonomias, denominados paradigma hierárquico fortemente distribuído (Martin-Flatin, Znaty e Hubaux) e paradigma fortemente distribuído (Schönwälder, Quittek e Kappler). Embora em ambos os paradigmas o processamento seja descentralizado para um grande número de entidades, também estes paradigmas possuem a diferença em relação a determinação expressa (ou não) de delegação vertical.

Por fim, a comparação dos *paradigmas fortemente distribuídos cooperativos* das taxonomias possui diferenças mais significativas. Embora em ambas as taxonomias o gerenciamento do paradigma seja descentralizado para todos os gerentes e agentes, Martin-Flatin, Znaty e Hubaux determinam de modo específico que a comunicação é baseada em mecanismos de delegação horizontal, com todas as entidades localizando-se no mesmo nível organizacional, e sendo baseado em agentes inteligentes. Schönwälder, Quittek e Kappler, por sua vez, definem o paradigma apenas pela presença de entidades com duplo papel no universo das entidades, apresentando um enfoque distinto para o uso do termo cooperativo.

3.3 Outras Taxonomias de Gerenciamento de Redes

As taxonomias apresentadas na seção anterior definem paradigmas de gerenciamento de redes de acordo com a distribuição utilizada, considerando aspectos como a estrutura, os papéis e os modos de interação entre as entidades, e permitindo classificar arquiteturas e sistemas de gerenciamento. Esta seção apresenta taxonomias de gerenciamento de redes com enfoques distintos. Inicialmente, é apresentada a taxonomia aprimorada proposta Martin-Flatin, Znaty e Hubaux. A seção posterior apresenta a taxonomia proposta por Pavlou.

3.3.1 Taxonomia Aprimorada segundo Martin-Flatin, Znaty e Hubaux

Como apresentado anteriormente, Martin-Flatin, Znaty e Hubaux propuseram duas taxonomias: a taxonomia denominada pelos autores *simples*, abordada na seção 3.2.1, e a taxonomia denominada pelos autores *aprimorada*, que será apresentada nesta seção. Esta taxonomia é proposta em (MARTIN-FLATIN; ZNATY; HUBAUX, 1999) e

posteriormente aperfeiçoada em (MARTIN-FLATIN, 2003), sendo baseada em quatro critérios: granularidade de delegação, riqueza semântica do modelo de informação, grau de automação do gerenciamento e grau de especificação da tarefa.

A **granularidade de delegação** corresponde à granularidade com que o processo de delegação ocorre em sistemas de gerenciamento de redes. No primeiro estágio, há arquiteturas que não suportam delegação, como, por exemplo, com os protocolos SNMPv1 e SNMPv2. Nos estágios seguintes, há dois tipos possíveis de delegação: delegação por domínio e delegação por tarefa (que será subdividida em dois estágios).

A **delegação por domínio** se baseia em tarefas estáticas e o gerente do nível superior assume que todos os gerentes do nível inferior conhecem todas as tarefas que devem ser realizadas dentro daquele domínio. É uma delegação com carta branca, na qual o gerente de nível inferior tem total controle sobre sua rede, e o gerente de nível superior não pode executar políticas de gerenciamento sobre os gerentes de nível inferior. Tipicamente, é utilizado para realizar delegação de acordo com o domínio geográfico, sendo empregado para gerenciar organizações dispersas geograficamente. Um exemplo de tecnologia que pode ser empregada para esta categoria é o SNMPv2p com a MIB M2M.

A **delegação por tarefa** permite que o gerente de nível superior obtenha uma visão mais detalhada do processamento ocorrendo no nível inferior, onde tarefas podem ser alteradas dinamicamente. Tarefas representam unidades de processamento de gerenciamento que, em conjunto, formam o sistema completo. Estas tarefas são distribuídas para gerentes e agentes, e o gerente no nível superior controla as tarefas executadas pelos subordinados. De acordo com a complexidade das tarefas, a delegação por tarefa pode ser dividida em dois estágios: micro-tarefas e macro-tarefas. As **micro-tarefas** correspondem às tarefas que realizam simplesmente o pré-processamento de variáveis estáticas da MIB, tipicamente com o objetivo de calcular estatísticas. Com micro-tarefas, se o contato com o gerente é perdido, as estatísticas ainda podem ser calculadas, mas a entidade subordinada não possui meios para tomar ações corretivas. As **macro-tarefas**, por sua vez, correspondem às tarefas que possuem controle completo sobre a entidade. Deste modo, se o contato com a entidade de nível superior é perdido, a tarefa pode tomar ações corretivas. O RMON é exemplo de tecnologia que suporta a delegação de micro-tarefas. A Script MIB e as tecnologias que seguem os paradigmas de código móvel e objetos distribuídos, por sua vez, são exemplos de tecnologias que suportam a delegação de micro e macro-tarefas.

O segundo critério da taxonomia é a **riqueza semântica do modelo de informação**, que indica os tipos de entidades e ações que podem ser definidos no modelo de informação do sistema de gerenciamento e está relacionada à força expressiva das abstrações utilizadas no modelo. Três tipos de abstrações são definidos: objetos gerenciados, objetos computacionais e objetivos.

Na abordagem de **objetos gerenciados**, a semântica oferecida para desenvolvimento do sistema de gerenciamento é restrita de acordo com as primitivas do protocolo empregado para a comunicação. O protocolo é automaticamente imposto e os objetos gerenciados devem ser localizados em agentes, sendo a comunicação realizada através do paradigma gerente-agente. Exemplo inclui a arquitetura SNMP.

A abordagem de **objetos computacionais**, por sua vez, é baseada no paradigma de objetos distribuídos. Nesta abordagem, os objetos pertencentes ao sistema são definidos pela interface que oferecem para outros objetos e o modelo é independente do protocolo

de comunicação, que é totalmente transparente para a aplicação. O desenvolvimento de sistemas com esta abordagem permite a utilização de bibliotecas de classes que oferecem visões de alto nível dos recursos gerenciados. Exemplos de tecnologias que têm adotado esta abordagem para o gerenciamento de redes incluem as tecnologias de objetos distribuídos. Contudo, os autores destacam que as tecnologias de objetos distribuídos também podem adotar a abordagem de objetos gerenciados para o gerenciamento, citando como exemplo o uso de CORBA na área de telecomunicações, usualmente baseada na abordagem de objetos gerenciados, onde é feita a simples tradução de objetos gerenciados para objetos CORBA.

Por fim, na abordagem através de **objetivos**, as tarefas do sistema são modeladas em abstrações de nível muito alto e parcialmente especificadas com objetivos, cabendo ao agente definir como atingir tais objetivos. Objetivos representam o mais alto nível de abstração disponível para desenvolvimento de sistemas de gerenciamento. Sistemas com esta abordagem são baseados em tecnologias de agentes inteligentes, que geralmente suportam algum tipo de máquina de inferências e aprendizado.

O terceiro critério da taxonomia diz respeito ao **grau de especificação de uma tarefa**. Este critério está relacionado à riqueza semântica do modelo de informação: objetos gerenciados e objetos computacionais se baseiam em **tarefas totalmente especificadas**, enquanto objetivos se baseiam em **tarefas parcialmente especificadas**.

Por fim, o quarto critério da taxonomia é baseado **no grau de automação do gerenciamento** e está relacionado com a granularidade da delegação. Um **baixo grau de automação** é obtido com delegação por domínio ou em sistemas sem delegação; um **grau médio** é obtido com micro-tarefas, e um **alto grau** é obtido com macro-tarefas, já que estas permitem que os agentes tomem ações corretivas de modo independente do gerente.

A figura 3.2, extraída de (MARTIN-FLATIN, 2003) [traduzida], esquematiza a taxonomia.

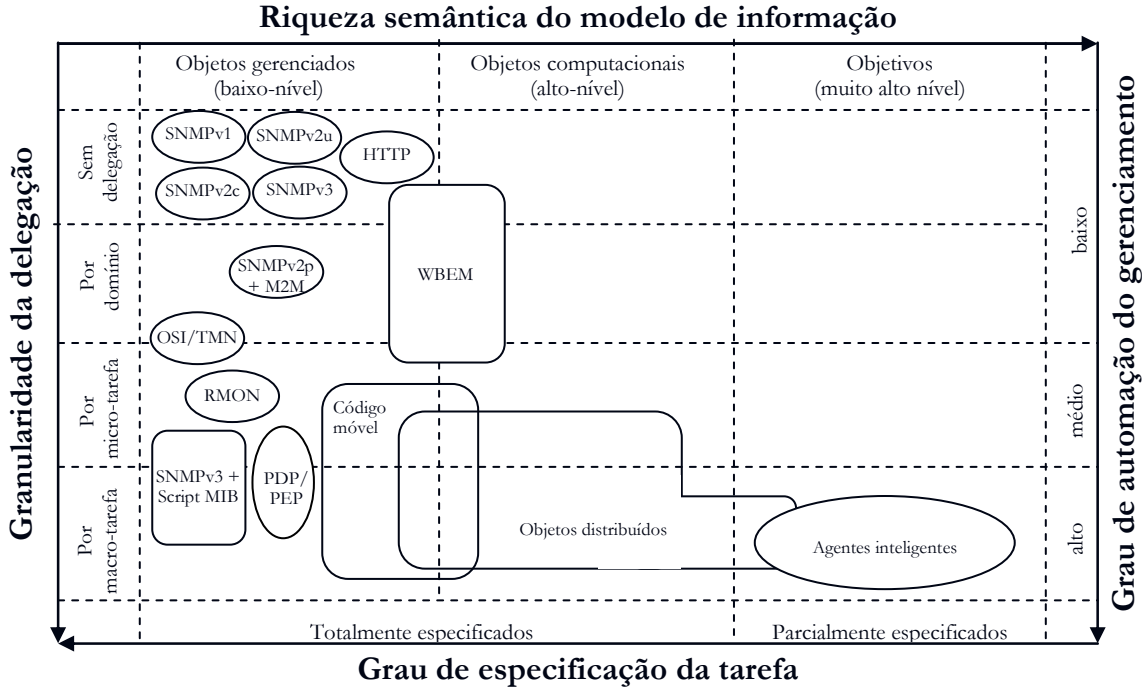


Figura 3.2: Taxonomia aprimorada (MARTIN-FLATIN, 2003)

3.3.2 Taxonomia segundo Pavlou

Pavlou propõe uma taxonomia para abordagens, *frameworks* e protocolos de gerenciamento (PAVLOU, 2007), utilizando como critério os diferentes modos de executar as atividades de gerenciamento. A taxonomia proposta exclui as abordagens de gerenciamento baseadas em procedimentos (PAVLOU, 2007), utilizadas na primeira geração das abordagens de gerenciamento, até o início da década de 1990. Duas categorias são definidas para o primeiro nível da taxonomia: **gerenciamento por invocação remota** e **gerenciamento por delegação**.

A categoria de **gerenciamento por invocação remota** compreende as abordagens em que o gerenciamento se dá "invocando operações remotas em objetos gerenciados"[traduzido](PAVLOU, 2007, p. 435). Duas subcategorias são definidas, de acordo com o modo com a invocação é realizada: "executando invocações em objetos gerenciados através de um agente, *i.e.*, o modelo gerente-agente"[traduzido](PAVLOU, 2007, p. 435), sendo denominada **baseada em gerente-agente**; e "executando invocações diretamente para os objetos gerenciados, *i.e.*, o modelo de objeto distribuído ou interface de serviço" [traduzido](PAVLOU, 2007, p. 435), sendo denominada **baseada em objetos/interface de serviços**. Exemplos de tecnologias que seguem a categoria baseada em gerente-agente incluem o SNMP e o OSI-SM. Exemplos de tecnologias que seguem a categoria baseada em objetos/interface de serviços incluem CORBA e WebServices.

A categoria de **gerenciamento por delegação**, por sua vez, abrange as abordagens em que as atividades são realizadas "enviando a lógica de gerenciamento, *i.e.*, o código, para equipamentos gerenciados de modo que este esteja situado próximo aos objetos que ele requer para executar operações localmente" [traduzido] (PAVLOU, 2007, p. 435). Dois modos são definidos para esta categoria. O primeiro, apresentado como **baseado em gerente-agente**, inclui as abordagens mais simples em que a lógica para a atividade de gerenciamento é carregada no equipamento gerenciado a fim de ser executada mais próxima dos objetos gerenciados. Exemplos incluem a Script MIB e o CMIP *command sequencer*. O segundo modo desta categoria, apresentado como **baseado em código móvel completo,** envolve mover a lógica de um equipamento para outro, ou seguindo um itinerário pré-definido (denominado mobilidade restrita), ou avaliando o ambiente de modo autônomo. Exemplos incluem tecnologias de agentes móveis.

A figura 3.3, extraída de (PAVLOU, 2007)[traduzida], esquematiza a taxonomia.

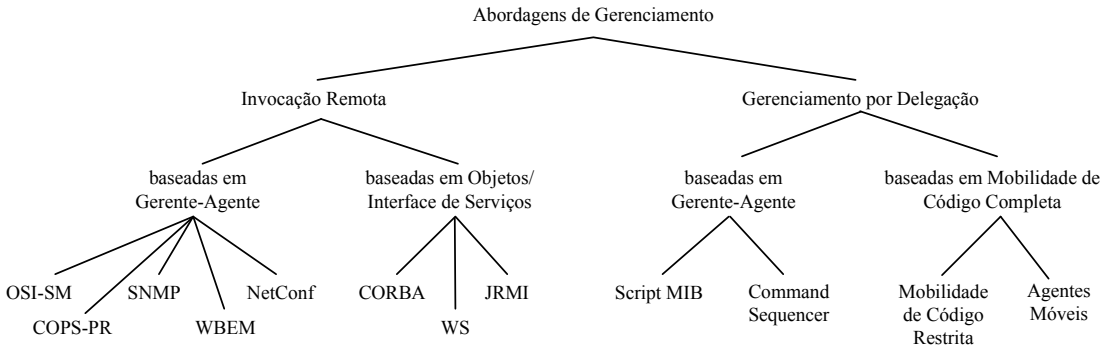


Figura 3.3: Taxonomia das abordagens, *frameworks* e protocolos de gerenciamento (PAVLOU, 2007)

3.3.3 Análise Crítica das Taxonomias Apresentadas

Analisando a taxonomia aprimorada proposta por Martin-Flatin, Znaty e Hubaux, se observa que esta difere bastante da taxonomia simples proposta pelos mesmos autores, permitindo avaliar diferentes aspectos das abordagens de gerenciamento de redes. Esta taxonomia pode ser empregada para analisar o uso de tecnologias para gerenciamento, auxiliando a identificação das tecnologias adequadas para o gerenciamento de uma dada rede. Como pode ser observado na figura 3.2, a taxonomia permite que uma tecnologia suporte mais de uma categoria para um mesmo critério.

A taxonomia proposta por Pavlou, por sua vez, possui enfoque distinto, sendo baseada no modo com as tarefas de gerenciamento são realizadas. Esta taxonomia pode ser empregada para classificar tecnologias de gerenciamento, possuindo um primeiro nível da taxonomia bastante intuitivo para este propósito, que a subdivide na categoria de gerenciamento por invocação remota de operações em objetos gerenciados e na categoria de gerenciamento por delegação. O segundo nível da categoria **gerenciamento por invocação remota em objetos gerenciados**, por sua vez, embora correto, deve ser utilizado cuidadosamente para evitar má interpretação em função da múltipla utilização do termo agente na literatura. As duas subcategorias deste nível compreendem a invocação remota de objetos gerenciados baseando-se ou na invocação de objetos gerenciados através de um agente, ou na execução de invocações diretamente para objetos gerenciados. Contudo, o termo agente é abordado na área de gerenciamento com enfoques distintos (vide seção 3.1): por um lado, o termo agente é empregado para indicar o software que encapsula os objetos gerenciados, como seguido nesta taxonomia; por outro, é empregado para destacar um papel das atividades de gerenciamento, como, por exemplo, em referências que abordam a presença de agentes CORBA (HEGERING; ABECK; NEUMAIR, 1999) e agentes baseados em WebServices (SCHÖNWÄLDER; PRAS; MARTIN-FLATIN, 2003). Esta dupla utilização do termo pode causar ambigüidade na interpretação: nesta taxonomia, por exemplo, há a classificação de CORBA e WebServices dentro da subcategoria baseada em objetos/interface de serviços; em contraste, há a utilização do termo agente CORBA e agente WebServices por outros autores. No entanto, é importante ressaltar que a taxonomia não está incorreta, pois é consistente com a terminologia na qual o termo agente define um software que encapsula os objetos gerenciados e é invocado de modo restrito a partir das primitivas do protocolo de comunicação empregado: apenas tal taxonomia deve ser utilizada com atenção em relação a este aspecto, já que o termo assume outros enfoques na literatura.

3.4 Discussão acerca da Aplicação de Modelos e Tecnologias Propostos na Literatura para Gerenciamento Fortemente Distribuído

Nos dias atuais, diversos sistemas de gerenciamento baseados nos paradigmas tradicionais (paradigmas centralizado e fracamente distribuído) são empregados para o gerenciamento de redes reais. Tais sistemas fazem uso, freqüentemente, do *framework* de gerenciamento Internet através dos protocolos SNMPv1 ou SNMPv2 (vide seção A.1.1), sendo ainda desenvolvidos fazendo uso de outras tecnologias, tais como RMON (vide seção A.1.2).

Por sua vez, o desenvolvimento de sistemas de gerenciamento baseados nos paradigmas fortemente distribuídos requer o emprego de modelos de gerenciamento distintos, baseados em tecnologias que se mostrem apropriadas para o emprego da alta

distribuição das ações de gerenciamento. Na última década, alguns modelos e tecnologias foram propostos por alguns autores para uso em tais sistemas. Entre estes, Martin-Flatin (MARTIN-FLATIN, 2003) apresentou como tecnologias que implementam o paradigma hierárquico fortemente distribuído as seguintes: a Script MIB (fazendo uso do protocolo SNMPv3), outras tecnologias baseadas no paradigma de código móvel e as tecnologias baseadas no paradigma de objetos distribuídos. Para o paradigma denominado cooperativo fortemente distribuído (vide seção 3.2.1), o autor reporta ao emprego de tecnologias de agentes inteligentes.

Schönwälder, Quittek e Kappler (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000), por sua vez, discutiram o desenvolvimento de sistemas de gerenciamento concentrando-se apenas em tecnologias que oferecem delegação dinâmica, discutindo o uso da Script MIB, de agentes móveis e de redes ativas. Neste contexto, os autores defenderam que a aplicação da Script MIB para o desenvolvimento de sistemas depende do suporte que a linguagem do *script* possui para a comunicação no papel de gerente, indicando que um *script* que faça uso da biblioteca SNMP pode ser adequado para sistemas fracamente distribuídos e para alguns sistemas fortemente distribuídos. Com relação aos sistemas com forte distribuição que tais autores classificam como cooperativos (vide seção 3.2.2), defendem que a aplicabilidade da Script MIB é questionável. Tecnologias de agentes móveis, por sua vez, foram indicadas para uso em sistemas denominado cooperativos, nos quais a presença de mobilidade de processos poderia trazer maior flexibilidade, embora os autores tenham ponderado que ainda não estivesse claro se as tarefas de gerenciamento poderiam realmente fazer uso da mobilidade, aspecto que é também discutido por outras pesquisas (QUITTEK; BRUNNER. 2003), que apontam que não havia clara evidência até aquele momento se a capacidade de mobilidade seria de grande significância para aplicações de gerenciamento. Por fim, acerca de redes ativas, os autores defenderam que esta tecnologia, embora suficiente para tal propósito, não parece ser uma boa solução para sistemas cooperativos, já que a força do gerenciamento baseado nesta tecnologia é o isolamento da funcionalidade de gerenciamento, e sistemas cooperativos tipicamente possuem alta conectividade.

Passada quase uma década da publicação de tais estudos (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000) (MARTIN-FLATIN; ZNATY; HUBAUX, 1999) (MARTIN-FLATIN, 2003), percebe-se que, embora modelos seguindo os paradigmas fortemente distribuídos baseados nestas tecnologias tenham sido propostos, poucos exemplos de sua aplicação são encontrados no gerenciamento para redes reais, de produção, especialmente em redes TCP/IP. Uma discussão acerca do emprego destas tecnologias e de aspectos que podem ter motivado esta não utilização são apresentados a seguir.

Com relação às tecnologias de código móvel, a Script MIB destaca-se como uma das tecnologias propostas para o gerenciamento de redes mais discutidas. Tal tecnologia foi abordada em diversas pesquisas (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000) (MARTINEZ et al, 2002) (QUITTEK; BRUNNER, 2003) e tem como aspecto relevante ter sido discutida através de um grupo de trabalho do IETF (grupo de trabalho *Distributed Management*, ou disman) (IETF, 2010) e ter sido padronizada através de uma RFC (LEVI; SCHÖNWÄLDER, 2001), tendo representando um importante avanço no gerenciamento distribuído. Entretanto, esta tecnologia, assim como as demais, não foi muito utilizada em ambientes de gerenciamento de redes reais (PAVLOU, 2007). Discussões acerca dos motivos da não utilização desta tecnologia

não foram encontradas na literatura. Entretanto, algumas considerações acerca de aspectos e limitações da tecnologia que podem ter contribuído para isto podem ser arrazoados. Tais aspectos incluem as restrições na flexibilidade proporcionada, em virtude de fatores tais como os gerentes de nível intermediário (através dos *scripts*) serem invocados necessariamente através de uma MIB, tornando a invocação dos *scripts* e a obtenção de seus resultados restritas aos recursos providos por esta; o limitado suporte para envio de notificações pelo gerente de nível intermediário; o significativo controle requerido do gerente de nível superior para a execução dos *scripts* nos gerentes de nível intermediário, já que este terá que transferir o *script*, controlar sua execução, etc.; e a continuidade de significativas limitações de escalabilidade e de tolerância a falhas, já que há a necessidade de um gerente de nível superior que interaja com os *scripts* e realize diversas operações de controle sobre estes.

Por fim, outra tecnologia de código móvel proposta para o gerenciamento de redes foi a baseada em agentes móveis. Contudo, embora discutida em algumas pesquisas (STEPHAN; RAY; PARAMESH, 2004) (LIOTTA; PAVLOU; KNIGH, 2002) (SATOH, 2003) (QUITTEK; BRUNNER, 2003), também esta tecnologia não foi utilizada em redes reais (PAVLOU, 2007). Discussões acerca dos motivos de sua não utilização não foram igualmente encontradas na literatura, entretanto, algumas dificuldades apontadas para o uso do modelo que podem ter contribuído para sua não utilização podem ser citados. Entre estes, inclui-se a necessidade dos equipamentos da rede suportarem a migração dos agentes móveis, requerendo suporte para a mobilidade de uma unidade de execução completa de um nodo para outro, incluindo seu estado de execução, seus resultados intermediários, o código necessário para sua execução e alguns recursos necessários para a tarefa demandada, assim como para que a execução da unidade seja continuada no nodo receptor. Tal necessidade pode trazer restrições ao emprego do modelo, já que muitos equipamentos gerenciados possuem um software rígido, com limitação para atualizações. Além do suporte à migração, pode também ser citada como dificuldade a necessidade de mecanismos eficientes para definição do itinerário de migração dos agentes (SATOH, 2003), uma vez que o itinerário realizado pelo agente possui grande importância sobre a execução e a eficiência das tarefas no agente. Contudo, é muitas vezes difícil gerar dinamicamente um itinerário eficiente entre múltiplos nodos sem ter conhecimento sobre a rede.

Em relação às tecnologias baseadas em objetos distribuídos propostas para emprego em gerenciamento de redes, a tecnologia CORBA foi bem aceita no gerenciamento de ambientes de telecomunicações e foi utilizada por vários fabricantes de equipamentos para gerenciamento de comutadores e redes telefônicas (MARTIN-FLATIN, 2003). Contudo, apesar de sua utilização em ambientes de telecomunicações e no gerenciamento de serviços, a tecnologia não foi utilizada em escala significativa para o gerenciamento de redes (PAVLOU, 2007). Problemas apontados para sua utilização incluem ser uma tecnologia relativamente pesada e dispendiosa: o gerenciamento de equipamentos de rede pode conter centenas de milhares de objetos para gerenciamento, e transformar cada objeto em um objeto distribuído separado com uma interface individual consome muitos recursos. Soluções para contorno destes problemas são proprietárias e não foram acordadas através de uma solução padronizada. Deste modo, problemas do uso de CORBA para o gerenciamento de redes, assim como de outras tecnologias de objetos distribuídos, incluem a ausência de suporte para transferência de volume de dados e problemas de escalabilidade por modelar vastas quantidades de entidades dinâmicas (*e.g.*, conexões) como objetos individuais. Abordagens baseadas

em Java RMI, por sua vez, foram usadas para o gerenciamento de redes principalmente em pesquisas (PAVLOU, 2007).

O uso de Web Services para o gerenciamento de redes e serviços tem sido também pesquisado. Uma das diferenças entre esta tecnologia e CORBA é que em CORBA, há tipicamente um forte acoplamento cliente-servidor, no qual o cliente possui conhecimento pré-compilado da interface do servidor, com suporte para checagem de tipo em tempo de compilação. Web Services, por sua vez, foram planejados para serem orientados a mensagens, com baixo acoplamento entre clientes e servidores usando *parsing* XML e checagem somente em tempo de execução. Contudo, esta tecnologia também possui alguns dos problemas encontrados em tecnologias de objetos distribuídos, vistos acima, quando utilizados para gerenciamento, relativos à ausência de suporte à recuperação de dados otimizada e por constituírem uma tecnologia relativamente dispendiosa para o gerenciamento de um grande volume de objetos (PAVLOU, 2007).

3.5 Considerações Finais

Este capítulo apresentou os principais conceitos de gerenciamento de redes distribuído relevantes para a compreensão deste documento. Inicialmente, foi introduzida a terminologia seguida pelo documento, a fim de aprimorar seu entendimento, uma vez que diversos termos na área são empregados com múltiplos significados, sem uma terminologia comum. Em seguida, as principais taxonomias propostas para a área de gerenciamento de redes foram abordadas, separadas por dois grupos: as taxonomias que propõe paradigmas de gerenciamento, com enfoque na distribuição das atividades, na estrutura empregada, nos papéis e nos modos de interação entre as entidades; e as taxonomias com outros enfoques. Uma análise crítica de cada grupo de taxonomias foi também apresentada. Por fim, foi abordada uma discussão acerca do emprego dos principais modelos e tecnologias propostos na literatura para o desenvolvimento de sistemas de gerenciamento fortemente distribuídos.

O capítulo a seguir discute a utilização dos paradigmas e modelos de gerenciamento em contextos de redes atuais, enfocando os paradigmas propostos pelo primeiro grupo de taxonomias discutido acima.

4 PARADIGMAS E MODELOS DE GERENCIAMENTO EM CONTEXTOS MODERNOS DE REDE

Como visto, embora ainda utilizados no gerenciamento de organizações, modelos de gerenciamento baseados nos paradigmas tradicionais se tornam cada vez mais inadequados para o gerenciamento de redes atuais, em virtude do aumento em tamanho e complexidade destas redes, que causam maior severidade às limitações destes modelos. Entretanto, em adição a estas limitações, existem atualmente contextos de redes que, por possuírem certas características, demandam requisitos de gerenciamento que não podem ser atendidos de modo apropriado pelos modelos tradicionais. Estes contextos compreendem as redes ou os aspectos de uma rede que possuem particularidades não encontradas usualmente em redes tradicionais, tais como a necessidade de atividades de gerenciamento serem executadas simultaneamente em múltiplos pontos ou a presença de múltiplos domínios administrativos demandando a cooperação entre estes para execução de suas operações.

Neste documento, tais contextos serão denominados **contextos modernos**, onde, por contexto, entende-se uma arquitetura de rede completa (*e.g.*, rede *mesh* sem fio) ou um particular aspecto de uma rede, que pode ser uma aplicação ou serviço, um problema a ser tratado na rede ou uma situação encontrada na rede (*e.g.*, ataques de negação de serviço distribuídos e grades computacionais). Com intuito de simplificar a terminologia deste documento, o primeiro grupo será denominado *contexto do tipo rede* e o segundo grupo será denominado *contexto do tipo aspecto de rede*.

Este capítulo analisa os paradigmas e os modelos adequados para o gerenciamento de contextos modernos de rede, demonstrando as limitações apresentadas pelos modelos baseados nos paradigmas tradicionais. A seção a seguir introduz e revisa brevemente três contextos modernos que serão analisados como estudos de caso, sendo estes uma arquitetura de rede (rede *mesh* sem fio) e dois aspectos de rede (ataques de negação de serviço distribuídos e grades computacionais). A seção 4.2 apresenta a metodologia desenvolvida para auxiliar a identificação e a análise de modelos de gerenciamento adequados para contextos como estes, com enfoque em requisitos de gerenciamento relacionados à distribuição das atividades e à presença de múltiplos domínios administrativos. Cada um dos três contextos modernos introduzido é então analisado segundo esta metodologia na seção 4.3. Por fim, a seção 4.4 apresenta as considerações finais.

4.1 Contextos Modernos: Estudos de Caso

Esta seção introduz e revisa três contextos modernos de rede como estudos de caso. Inicialmente, representando um *contexto do tipo rede*, serão apresentadas as redes *mesh*

sem fio, redes com estrutura em malha dinâmica nas quais o roteamento dos pacotes é realizado de modo colaborativo entre os nodos da rede. A seção a seguir, representando um *contexto do tipo aspecto de rede*, aborda os ataques de negação de serviço distribuídos, selecionados por exigirem mecanismos de detecção e tratamento a ataques baseados em redes intermediárias. Por fim, a seção final, também representando um *contexto do tipo aspecto de rede*, discute as grades computacionais, que consistem em sistemas de computação distribuídos em rede que compartilham recursos computacionais dispersos em múltiplas organizações e possuem requisitos distintos para o gerenciamento da infra-estrutura de rede utilizada por eles.

4.1.1 Redes *Mesh* Sem Fio

Redes *mesh* sem fio (BRUNO; CONTI; GREGORI, 2005) (AKYILDIZ; WANG; WANG, 2005) (ABELÉM et al, 2007), também conhecidas como redes em malha sem fio, são redes em que o roteamento dos pacotes é feito colaborativamente entre os nodos, que podem ser fixos e móveis, com comunicação sem fio. Tais redes são auto-organizadas e auto-configuradas, possuindo nodos que estabelecem e mantém, dinamicamente, conectividade em malha entre si. Os nodos em uma rede *mesh*, além de suas funções como *host*, operam tipicamente também como roteadores, retransmitindo pacotes oriundos de outros nodos que não possuem transmissão sem fio direta para seus destinatários. Sua capacidade de auto-organização e auto-configuração permite que tais redes cresçam de modo incremental sempre que necessário, aumentando, com a inclusão de novos nodos, a conectividade, a área de cobertura e a confiabilidade da rede. Além disto, tais redes proporcionam a conectividade sem fio entre usuários mesmo que estes não possuam enlaces com linha de visada (*line-of-sight - LOS)*, através do roteamento entre múltiplos nodos.

Dois tipos de nodos são utilizados em redes *mesh*: roteadores *mesh* e clientes *mesh* (AKYILDIZ; WANG; WANG, 2005). **Roteadores *mesh*** provêm funcionalidades de roteamento entre os nodos da malha, além de suportar as funções de *gateway/bridge* de roteadores sem fio convencionais. Usualmente, estes nodos possuem mobilidade mínima e não possuem restrições severas quanto ao consumo de energia. Roteadores *mesh* podem ainda ser equipados com múltiplas interfaces sem fio de tecnologias distintas. **Clientes *mesh*** também suportam funcionalidades de roteamento entre os nodos da malha, porém não provêm funções de *gateway/bridge*, além de possuírem usualmente apenas uma única interface sem fio. Em virtude disto, clientes *mesh* podem ser implementados em equipamentos com hardware e software muito mais simples que roteadores *mesh*. Estes nodos podem ser fixos ou móveis e podem possuir restrições quanto ao consumo de energia demandado para suas operações.

A arquitetura de redes *mesh* pode ser dividida em três tipos. Em **redes *mesh* de infra-estrutura ou *backbone***, roteadores *mesh* formam uma infra-estrutura para clientes, criando uma malha de enlaces auto-configuráveis entre os roteadores. Esta malha provê um *backbone* para os clientes e permite a integração da rede *mesh* com outras tecnologias de rede através das funcionalidades de *gateway* e *bridge* nos roteadores. Em **redes *mesh* de clientes**, nodos clientes *mesh* formam uma rede em malha que será utilizada para o roteamento dos pacotes. Em virtude da necessidade de prover funções de roteamento e auto-configuração, os requisitos dos equipamentos destes nodos são superiores aos requisitos de nodos clientes em redes com arquitetura de infra-estrutura ou *backbone*. Por fim, **redes *mesh* híbridas** são formadas pela combinação das duas arquiteturas acima. Nestas redes, clientes *mesh* podem comunicar-

se através dos roteadores *mesh* ou através de outros clientes *mesh*. Esta arquitetura é mais flexível, já que a funcionalidade de roteamento nos clientes contribui para o aumento da conectividade e da área de cobertura das redes *mesh*, ao mesmo tempo em que a infra-estrutura formada pelos roteadores *mesh* permite a conectividade para outros tipos de redes.

As redes *mesh* surgiram a partir do antigo conceito de redes móveis *ad hoc*, conhecidas como *Mobile Ad-hoc NETworks* (MANETs). Estas redes são formadas por grupos de nodos móveis, conectados através de um meio sem fio, que se auto-organizam dinamicamente em topologias de rede temporárias e possibilitam a conectividade em áreas sem infra-estrutura pré-existente (BRUNO; CONTI; GREGORI, 2005). Considerando as redes *mesh* com arquitetura híbrida, estas diferem das redes *ad hoc* por características tais como: presença de um *backbone* sem fio com grande cobertura, conectividade e robustez (diferindo, portanto, da dependência de contribuições individuais de usuários finais em redes *ad hoc*); existência de equipamentos para roteamento (roteadores *mesh*) além do roteamento provido pelos usuários finais, que leva a menor processamento nestes usuários (diminuindo o consumo de energia e permitindo equipamentos de menor custo); e possibilidade de integração com outras redes existentes, incluindo redes sem fio e a Internet. Em função de suas características, alguns autores (AKYILDIZ; WANG; WANG, 2005) classificam as redes móveis *ad hoc* tradicionais como um sub-conjunto das redes *mesh* sem fio, já que as redes *mesh* requerem, além das técnicas utilizadas nas redes *ad hoc*, outros algoritmos e princípios mais sofisticados.

Os benefícios proporcionados pelas redes *mesh*, quando comparadas às diversas redes sem fio existentes, incluem:

- Menor custo e maior flexibilidade na implantação de redes, em virtude da utilização de nodos sem fio para prover a conectividade da rede e aumentar sua área de cobertura. Isto elimina, por exemplo, quando comparado com as redes locais sem fio 802.11, a necessidade de múltiplos equipamentos de ponto de acesso, que exigem cabeamento fixo até eles;
- Maiores cobertura e conectividade com a inclusão de novos usuários, através das facilidades de roteamento providas mesmo por nodos de usuários finais;
- Possibilidade de comunicação direta entre os nodos quando requerido, sem necessidade de utilizar para a comunicação, por exemplo, o ponto de acesso (em nodos em uma rede WiFi) ou a infra-estrutura da intranet (em nodos em uma empresa).

As redes *mesh* têm sido pesquisadas a partir de diversos padrões de redes sem fio existentes. Um grupo de trabalho foi formado no IEEE em 2004 (denominado IEEE 802.11s) (IEEE, 2009) para atender aos requisitos de redes *mesh* no padrão IEEE 802.11 (GLASS; PORTMANN; MUTHUKKUMARASAMY, 2008) (HIERTZ et al, 2007). Já o padrão IEEE 802.16d/3 WiMAX para redes metropolitanas sem fio tem uma especificação padronizada para operações em rede *mesh* (ZHANG; HU; CHEN, 2008). Além disto, soluções proprietárias para redes *mesh* foram também desenvolvidas por fabricantes distintos.

Existem, atualmente, várias projetos com redes *mesh* sem fio sendo desenvolvidas e testadas, aplicadas em cenários diversos tais como redes para acesso a campi universitários, redes metropolitanas, redes em ambientes rurais, etc. No Brasil, um exemplo é a rede *mesh* para acesso à rede do campus universitário em Niteroi/RJ,

implantada pelo grupo de trabalho da RNP denominado ReMesh (DUARTE et al, 2007). Exemplos em outros países incluem a rede UCSB MeshNet, para acesso ao campus da University of California em Santa Barbara (LUNDGREN et al, 2006); a rede Magnets, na cidade de Berlin (KARRER; BOTTA; PESCAPE, 2008); a rede na vila rural Wray, na Inglaterra (ISHMAEL et at, 2008). Outro importante projeto é denominado *One Laptop Per Child* (OLPC), que visa disponibilizar o uso da tecnologia da informação para educação em países em desenvolvimento (OLPC, 2009) (KRSTI; GARFINKEL, 2007). Os notebooks do projeto são projetados para serem de baixo custo e serem conectados a Internet através de uma rede *mesh* sem fio com *gateways* localizados em escolas. No Brasil, o projeto RUCA (Rede Um Computador por Aluno), administrado pela RNP e englobando cinco universidades brasileiras, objetiva realizar testes com a rede do programa (RNP, 2009) (CARRANO; MARTINS; MAGALHÃES, 2007).

Em virtude de características como a organização dinâmica, a grande variação na qualidade dos enlaces e a dificuldade de acesso físico aos equipamentos, o gerenciamento adequado e efetivo das redes *mesh* é de grande importância para a operação correta destas redes. Este gerenciamento, contudo, precisa ser realizado atendendo importantes requisitos (LUNDGREN et al, 2006) (DUARTE et al, 2007), que serão vistos a seguir.

Em redes *mesh*, a topologia da rede e suas características mudam freqüentemente ao longo do tempo em virtude das alterações na qualidade dos enlaces e do ambiente volátil em geral. Deste modo, o ambiente de gerenciamento necessita obter as informações de topologia da rede de modo freqüente, incluindo a coleta de métricas que reportem a qualidade dos enlaces e a largura de banda disponível, podendo incluir também informações de configuração e tráfego de cada nodo *mesh*. Em virtude da estrutura da rede, as informações coletadas devem ser obtidas coletivamente, ao longo dos nodos de toda a rede, a fim que esta possa ser avaliada adequadamente.

Como a topologia da rede varia ao longo do tempo, o gerenciamento da rede deve ter capacidade de fornecer, além da conectividade corrente, dados históricos da rede. A monitoração e a identificação da topologia corrente e histórica de tais redes são importantes aspectos de seu gerenciamento, necessários para um adequado gerenciamento de falhas, de desempenho, de configuração e de segurança.

O acesso físico aos equipamentos das redes *mesh* é usualmente bastante restrito. Estas limitações de acesso reforçam a necessidade de um gerenciamento completo dos seus nodos, incluindo suporte à configuração com controle da execução de atividades, de modo que estas sejam realizadas em sua totalidade ou haja o retorno para um estado seguro se um evento imprevisto ocorrer. Isto é necessário porque a execução parcial de alterações pode causar a interrupção da conectividade do nodo, que exigiria o acesso físico a este para a correção do problema.

O ambiente de gerenciamento deve suportar a heterogeneidade dos nodos na rede, que afeta as informações que serão reportadas por eles. Placas de rede de diferentes fabricantes, por exemplo, reportam freqüentemente informações de potência de sinal de modo distinto. Assim, o ambiente de gerenciamento deve estar preparado para lidar com estas diferenças quando o hardware envolvido nos equipamentos for heterogêneo, o que acontece freqüentemente.

A arquitetura do gerenciamento deve ser escalável, permitindo que novos nodos sejam inseridos na rede sem aumentar a complexidade ou diminuir a eficiência de suas

operações. Como as tarefas de gerenciamento evoluem ao longo do tempo, o gerenciamento deve permitir que novas funcionalidades sejam acrescentadas sem significativas atualizações ou mudanças no ambiente de gerenciamento existente. Além disto, a implantação de novos nodos na rede deve ser realizada do modo mais automático possível, exigindo pouca interação com o usuário.

Em função da elevada variação na qualidade dos enlaces das redes *mesh,* o ambiente de gerenciamento deve ter capacidade de lidar com freqüentes alterações no roteamento da rede. Estas alterações podem levar a interrupções em conexões utilizadas para gerenciamento de nodos, que podem ser tornar inacessíveis ou acessíveis através de diferentes conexões, interferindo na coleta de informações de gerenciamento. Além disto, certos nodos em redes *mesh* podem ser bastante voláteis, o que precisa ser considerado ao analisar o local de armazenamento dos dados coletados.

Por fim, o impacto do gerenciamento na rede deve ser mínimo. A fim de não afetar a conectividade da rede, as mensagens de gerenciamento devem consumir pouca largura de banda. Deste modo, arquiteturas de monitoração que empregam o *polling* de cada nodo individualmente devem ser cuidadosamente projetadas antes de serem utilizadas, já que podem causar um elevado tráfego na rede. Por outro lado, em virtude da estrutura das redes *mesh*, a utilização de um *probe* de monitoração passiva pode resultar na coleta de dados parciais da rede, já que nem todas as comunicações entre os nodos poderão ser monitoradas pelo *probe*, que visualizará apenas uma porção da rede. Além da conectividade, as restrições de recursos dos nodos *mesh* também devem ser consideradas, já que estes possuem muitas vezes baixo poder de processamento e espaço em disco limitado.

4.1.2 Ataques de Negação de Serviço Distribuídos

Inúmeros ataques são disparados contra a Internet nos dias atuais (MCPHERSON, 2010) (GTISC, 2008). Entre estes, os ataques de negação de serviço distribuídos (*Distributed Denial of Service* – DDoS) representam uma importante ameaça para a sua correta operação, sendo avaliados como uma das principais ameaças de segurança para o futuro recente (MCPHERSON, 2010).

Um ataque de negação de serviço (*Denial of Service* – DoS) objetiva impedir o uso legítimo de um serviço ou recurso da rede. Quando disparado a partir de múltiplos nodos, este ataque é denominado ataque de negação de serviço distribuído. Ataques DDoS (PENG; LECKIE; RAMAMOHANARAO, 2007) (MIRKOVIC; REIHER, 2004) consistem em um ataque coordenado em larga-escala, que podem ser realizados através de dois modos (PENG; LECKIE; RAMAMOHANARAO, 2007). No primeiro modo, pacotes cuidadosamente mal formados que exploram vulnerabilidades de software são enviados para o alvo. Este modo de ataque pode ser minimizado através de atualizações de software que corrijam as vulnerabilidades exploradas. Este ataque é denominado por **ataque semântico** por alguns autores (MIRKOVIC; REIHER, 2004). No segundo modo de ataque, um volume massivo de pacotes é enviado para o alvo de modo a consumir seus recursos e torná-los indisponíveis para os usuários legítimos. Os recursos focalizados podem incluir a capacidade de processamento ou memória de um servidor, a capacidade dos enlaces da rede, etc. Por suas características, este segundo modo de ataque é mais difícil de ser evitado, já que o ataque explora simplesmente o fato do alvo estar conectado a Internet, tendo sua força no volume do tráfego do ataque, ao invés do conteúdo do tráfego. Este modo de ataque é denominado **ataque de força bruta** por alguns autores (MIRKOVIC; REIHER, 2004). Ao longo deste documento, a menos

quando explicitamente definido, este modo de ataque será o abordado, e o termo ataque DDoS será utilizado para indicar este modo.

Os ataques DDoS são habitualmente executados através de duas etapas (PENG; LECKIE; RAMAMOHANARAO, 2007). Na etapa inicial, o atacante recruta múltiplos agentes na Internet e instala ferramentas de ataque nestes, transformando-os em "zumbis". Este processo pode ser realizado automaticamente, localizando sistemas vulneráveis na Internet, ou pode ser realizado através da distribuição de software de ataque disfarçado como uma aplicação útil. Na segunda etapa, o atacante emite um comando de início para as máquinas infectadas, e estas enviam os pacotes de ataque. Freqüentemente, os ataques são realizados empregando um endereço IP de origem falso no pacote a fim de dificultar a identificação das máquinas utilizadas, mecanismo conhecido como *IP spoofing* (MIRKOVIC; REIHER, 2004).

A defesa contra ataques DDoS de força bruta é prejudicada pela dificuldade em distinguir os pacotes legítimos dos pacotes do ataque, já que o atacante utiliza apenas volume, e não conteúdo, para realizar o ataque, fazendo uso de pacotes com as mesmas características dos pacotes legítimos. Outra característica dos ataques DDoS é que, em ataques em larga escala, a degradação da qualidade dos serviços atinge não apenas o alvo, mas também os demais enlaces envolvidos ao longo do caminho entre as máquinas origem e o alvo. Em virtude disto, ataques DDoS devem ser filtrados o mais próximo possível das máquinas de origem, evitando não apenas a interrupção do serviço no alvo, mas também que a largura de banda dos enlaces ao longo do caminho seja desperdiçada, prejudicando usuários legítimos.

A reação a ataques DDoS pode se dar em três estágios do caminho entre as máquinas origem zumbis e o alvo: **no alvo ou em sua rede**, **na rede intermediária** e **na rede de origem**.

Os mecanismos de reação ao ataque implantados **no nodo alvo ou em sua rede** são os mais simples de serem realizados. Tais mecanismos classificam o tráfego em vários tipos, objetivando priorizar o tráfego legítimo e filtrar o tráfego do ataque. Contudo, como muitos ataques DDoS imitam o tráfego legítimo para evitar sua filtragem, estes mecanismos não são efetivos e somente aliviam os danos do ataque. A eliminação eficaz do ataque precisa ser feita próximo as fontes de origem, o que tem sido buscado através de mecanismos de reação em **redes intermediárias**, que objetivam filtrar o tráfego de ataque usando roteadores entre as fontes de ataque e o alvo.

Importantes mecanismos de reação em redes intermediárias propostos baseiam-se na cooperação ativa entre roteadores. O mecanismo *Pushback* (IOANNIDIS; BELLOVIN, 2002) é uma destas propostas. Neste mecanismo, funcionalidades são acrescentadas aos roteadores para que estes detectem pacotes que provavelmente pertencem a um ataque e os filtrem preferencialmente. Os roteadores adjacentes anteriores no caminho do tráfego são também notificados para filtrar tais pacotes a fim de que os recursos de tais roteadores sejam também preservados para o tráfego legítimo, e o mecanismo é propagado progressivamente para outros roteadores. Na medida em que os roteadores em direção às fontes de ataque são notificados, mais tráfego legítimo é preservado.

Outro mecanismo que reage aos ataques na rede intermediária e é baseado na idéia de cooperação entre os roteadores foi proposto em (ZHANG; PARASHAR, 2006). Nesta abordagem, cada nodo de detecção (roteador) identifica anomalias no tráfego utilizando ferramentas de detecção de intrusão existentes e emprega um limitador para o tráfego identificado como ataque. Uma rede *overlay* P2P composta por estes roteadores

é utilizada para compartilhar as informações sobre o ataque para outros roteadores. As informações são enviadas para o roteador vizinho em direção ao alvo e enviadas randomicamente para os demais roteadores vizinhos. Ao receber informações sobre um ataque, o roteador ajusta seu limitador de tráfego para o tráfego indicado, de modo que o processo converge para que todos os nodos na rede P2P de defesa possuam uma informação global aproximada sobre o comportamento da rede.

Por fim, mecanismos para reação a ataques **na rede de origem** foram também propostos. No mecanismo D-WARD (MIRKOVIC; PRIER; REIHER, 2002), estatísticas dos fluxos de tráfego entre a rede origem e o resto da Internet são constantemente coletadas e comparadas com modelos do fluxo normal, a fim de identificar fluxos distintos, que são considerados ataques e filtrados ou limitados. Embora este mecanismo objetive uma defesa ideal, removendo o tráfego do ataque na origem, ele possui limitações, já que, em ataques em larga escala, o tráfego de cada origem pode ser muito reduzido e não ser possível identificá-lo no meio do tráfego legítimo.

Embora muitos estudos tenham sido desenvolvidos para o tratamento de ataques DDoS, apenas resultados limitados foram atingidos para o problema (PENG; LECKIE; RAMAMOHANARAO, 2007). A maior parte dos mecanismos propostos objetiva reagir ao tráfego no alvo ou em sua rede. Contudo, como visto acima, muito poucos tipos de ataque DDoS podem ser tratados apenas pelo alvo ou por nodos em redes isoladas (ZHANG; PARASHAR, 2006) (MIRKOVIC; REIHER, 2004), sendo muitas vezes necessário empregar um sistema de defesa distribuído e cooperativo implantado em vários pontos da Internet a fim de que as diversas combinações de máquinas zumbis e alvos de um ataque possam ser tratadas. Com esta abordagem, quando um ataque for detectado, medidas de defesa podem ser iniciadas próximas ao alvo e serem propagadas em direção às redes das máquinas origem, de modo que o tráfego do ataque possa ser filtrado próximo a origem. Assim, a abordagem permite não apenas uma detecção do ataque mais efetiva, como também minimiza seus prejuízos, já que a reação ao ataque é feita tanto para evitar a interrupção do serviço no alvo como também para impedir que haja degradação na qualidade dos serviços nos nodos do caminho entre as máquinas origem e o alvo.

4.1.3 Grades Computacionais

Grades computacionais (*grids computing*) (KOVALENKO; KORYAGIN, 2009) (KRAUTER; BUYYA; MAHESWARAN, 2002) (RANJAN; HARWOOD; BUYYA, 2008-b) (MANGANA, 2008) consistem em sistemas de computação distribuídos em rede que compartilham e agregam a força computacional de recursos disponíveis em máquinas heterogêneas localizadas em múltiplas organizações e domínios administrativos. Tais sistemas possuem alta capacidade computacional agregada para uso de aplicações, sendo utilizados para resolver problemas que demandam alto desempenho, alta vazão e alta disponibilidade. Além das grades computacionais, outros tipos de grades podem ser citadas, incluindo as grades de dados, que provêem uma infra-estrutura para sintetizar repositórios de dados distribuídos em larga escala; e a grades de serviços, que abrangem sistemas que provêem serviços que não são disponibilizados por uma única máquina (KRAUTER; BUYYA; MAHESWARAN, 2002).

As operações das grades computacionais envolvem a coordenação e o compartilhamento de recursos em organizações dinâmicas dispersas geograficamente.

As grades podem ser implementadas utilizado o conceito de *organização virtual (Virtual Organization, VO)* (FOSTER; KESSELMAN, 2001), que representa um conjunto de indivíduos ou organizações que compartilham os recursos de modo controlado, seguro e flexível, onde os participantes colaboram para atingir um objetivo global. Em grades implementadas seguindo o conceito de uma única organização virtual, todos os participantes aderem às mesmas políticas e prioridades para o compartilhamento dos recursos. As grades computacionais podem também ser implementadas utilizando outras abordagens para o compartilhamento dos recursos, tal como através de uma organização federada em que cada participante da grade possui autonomia completa para definir suas prioridades e políticas para os seus recursos (RANJAN; HARWOOD; BUYYA, 2008-b).

Um importante elemento das grades computacionais é o gerenciamento dos recursos da grade, conhecido por *Grid Resource Management* (GRM), responsável por controlar a disponibilização da capacidade computacional dos recursos da grade ao longo dos vários domínios administrativos envolvidos. Os recursos das grades são requisitados por aplicações, que podem, conforme a grade computacional utilizada, especificar restrições de qualidade de serviço (QoS) específicas. Cada requisição é considerada um *job*. As principais atividades do gerenciamento de recursos incluem descobrir os recursos, aceitar requisições (*jobs*) identificando seus requisitos, selecionar os recursos a serem utilizados para cada *job*, escaloná-los e monitorar os recursos ao longo do tempo a fim de executar os diversos *jobs* de modo eficiente (MANGANA, 2008). Como o gerenciamento pode manipular recursos de vários domínios administrativos, este deve possuir a confiança de todos os proprietários de recursos envolvidos, e é responsável por garantir que os recursos estejam sendo compartilhados aderindo às diferentes políticas de uso estabelecidas por cada domínio administrativo (KRAUTER; BUYYA; MAHESWARAN, 2002). O escalonamento dos *jobs* aos recursos das grades que pertencem a vários domínios administrativos é denominado *resource brokering* ou *superescalonamento* (*superscheduling*) por alguns autores (RANJAN; HARWOOD; BUYYA, 2008-a) (RANJAN; HARWOOD; BUYYA, 2008-b) (KRAUTER; BUYYA; MAHESWARAN, 2002). De modo análogo, as atividades de escalonamento são executadas através de *brokers* ou *superescalonadores*. O gerenciamento dos recursos faz uso de sistemas de gerenciamento de recursos locais, que controlam os recursos locais da grade, sendo responsáveis por gerenciar as filas de *jobs*, iniciar e monitorar a execução destes.

Um mecanismo de descoberta de recursos é utilizado para auxiliar o gerenciamento dos recursos e o escalonamento dos *jobs*, envolvendo a busca pelos tipos de recursos apropriados para atender os requisitos da requisição do usuário. Este mecanismo faz uso de um *serviço de informação* que indexa as informações dos recursos da grade através de diferentes organizações. Em serviços de informação com organização centralizada, consultas sobre os recursos são enviadas pelos *brokers* para um serviço de indexação de recursos centralizado, que também recebe as atualizações do estado dos recursos. Em serviços com organização hierárquica, serviços de informação são ligados direta ou indiretamente, onde as únicas ligações diretas entre nodos são do nodo pai para nodos filhos, formando, usualmente, uma estrutura em árvore. Por fim, em serviços de informação com organização descentralizada não há controle central, e a autonomia, a autoridade e a capacidade de processamento das consultas são distribuídas para todos os recursos, tal como, por exemplo, quando a estrutura de diretórios é organizada em uma

rede P2P dinâmica plana onde cada *organização virtual* mantém seus serviços de informação através de *peers* na rede (RANJAN; HARWOOD; BUYYA, 2008-b).

O escalonamento dos recursos ao longo dos vários domínios administrativos da grade pode ser baseado em diferentes estruturas. Alguns autores definem três categorias (KRAUTER; BUYYA; MAHESWARAN, 2002): estrutura centralizada, onde um único *broker* é responsável pela tomada de decisões do sistema completo; estrutura hierárquica, onde vários *brokers* são organizados hierarquicamente; e estrutura descentralizada. Outros autores definem duas categorias (RANJAN, 2007): estrutura centralizada e estrutura descentralizada. A abordagem centralizada possui como vantagens a facilidade de desenvolvimento e implantação, podendo, conceitualmente, produzir escalonamentos extremamente eficientes, já que a entidade central possui as informações sobre todos os *jobs* em execução. Esta abordagem, porém, possui sérias restrições quando utilizada para grades de grande tamanho. A abordagem descentralizada, por sua vez, possui vantagens relativas à tolerância a falhas, escalabilidade e autonomia, facilitando a utilização de políticas específicas para cada domínio administrativo. Esta abordagem é subdividida em duas categorias: estrutura descentralizada não coordenada e estrutura descentralizada coordenada. Na abordagem não coordenada, os *brokers* executam suas atividades de modo independente dos outros *brokers* do sistema, levando a problemas de balanceamento de carga entre a distribuição dos *jobs* nos recursos. Na abordagem coordenada, *mediadores* negociam condições dos recursos com sistemas gerentes dos recursos locais ou com outros *mediadores*.

A operação adequada de uma grade computacional inclui, ainda, o gerenciamento das redes envolvidas para que os acessos aos recursos da grade sejam possíveis. Deste modo, duas funções administrativas distintas podem ser identificadas: o *gerenciamento dos recursos da grade*, discutido nos parágrafos anteriores, responsável por gerenciar os recursos compartilhados da grade, seus usuários e permissões de acesso, etc.; e o *gerenciamento da infra-estrutura de rede utilizada pela grade*, responsável por manter a rede operando de modo adequado para que os recursos possam ser acessados (NEISSE, 2004).

O gerenciamento da rede requerido para a operação adequada de uma grade inclui as atividades de monitoração e configuração de parâmetros da rede, especialmente de parâmetros de QoS. Informações do estado e desempenho da infra-estrutura de rede são importantes para atividades da grade como o escalonamento, a migração e a monitoração de *jobs*, permitindo que as condições da rede sejam também consideradas para garantir o desempenho das aplicações sendo executadas na grade (CAMINERO et al, 2007) (TOMAS et al, 2009). Além da monitoração, a configuração dos recursos da rede pode também ser realizada, incluindo, por exemplo, a reserva de recursos de rede, tal como a reserva de largura de banda. Variando de acordo com a grade computacional, seus *jobs* e seus requisitos, a configuração dos recursos de rede pode abranger diversos domínios administrativos participantes, envolvendo, deste modo, a configuração de recursos de rede administrados por equipes distintas e autônomas. Esta configuração pode ser realizada tanto através da coordenação não automatizada entre a equipe administradora da grade computacional e a equipe administradora da rede de cada domínio administrativo envolvido, como pode ser realizada através de sistemas de gerenciamento que integrem o gerenciamento de grades e de redes.

Um exemplo de abordagem que propõe a utilização de informações de desempenho da infra-estrutura de rede dos domínios administrativos pertencentes a uma grade é apresentado em (CAMINERO et al, 2007) e (TOMAS et al, 2009). Tal abordagem

considera a latência da rede ao realizar o mapeamento entre *jobs* e recursos computacionais, considerando a latência de todos os enlaces envolvidos para a comunicação entre o usuário requisitando o *job* e cada recurso computacional sendo avaliado pelo escalonador, dentro do domínio administrativo do escalonador. A arquitetura da abordagem (CAMINERO et al, 2007) é baseada em diversas entidades, incluindo, entre outros, uma entidade responsável pelo escalonamento e uma entidade (denominada *Bandwidth Broker*) responsável por obter as informações de desempenho dos roteadores do domínio administrativo e controlar a largura de banda efetiva entre dois pontos da rede através de um algoritmo denominado *connection admission control* (controle de admissão de conexões). O emprego da entidade *Bandwidth Broker* foi realizado para manter a independência e a autonomia dos domínios administrativos, já que o algoritmo de controle das conexões faz uso de acesso direto aos roteadores.

A abordagem foi posteriormente implementada (TOMAS et al, 2009) estendendo um escalonador existente para que este inclua uma ferramenta para monitoração da rede, assim como para que considere mais um parâmetro para representar o estado da rede ao selecionar qual recurso computacional executará o *job*. A arquitetura é apresentada como escalável para ambientes com vários domínios administrativos. Quando é necessário submeter um *job* para outro escalonador, informações da largura de banda até os outros escalonadores que gerenciam os outros domínios são utilizadas para selecionar qual escalonador deve receber o *job*. Tal escalonador, por sua vez, ao receber o *job*, seleciona um de seus recursos para submetê-lo.

Outra abordagem para o gerenciamento da infra-estrutura de rede utilizada por grades é proposta em (NEISSE, 2004). Tal trabalho propõe o gerenciamento da infra-estrutura de redes utilizada por uma grade através de uma arquitetura baseada na tradução de políticas de gerenciamento de grades para políticas de gerenciamento de redes. As políticas da grade são definidas pelo administrador da grade e expressam as condições de operações destas. Tais políticas podem definir, por exemplo, os direitos de acesso dos usuários da grade aos seus recursos computacionais ou a qualidade no acesso aos recursos, através de reservas de processador, memória ou banda de rede. As políticas de rede, por sua vez, são criadas a partir de regras de tradução que objetivam a criação automática das políticas de rede, expressando configurações de rede necessárias para que a grade opere de modo adequado. Exemplos dos parâmetros a serem configurados incluem a definição da largura de banda mínima e máxima para fluxos de dados, assim como a definição da prioridade que os pacotes dos fluxos receberão na rede em relação aos demais pacotes. As regras de tradução são definidas pelos administradores da rede de cada domínio administrativo de acordo com os interesses locais do domínio, podendo ou não atender aos requisitos desejados pela grade.

Quando um administrador de grade deseja criar e aplicar uma política de grade, ele informa ao sistema a lista de domínios administrativos que participam da grade, de modo que os mecanismos de tradução de cada domínio administrativo possam ser identificados pelo sistema. O sistema interage então com os mecanismos de tradução de cada domínio administrativo envolvido, que, por sua vez, recuperam o conjunto de regras de tradução previamente definidas pelo administrador da rede do domínio e traduzem as políticas de grade recebidas em políticas de rede utilizando as regras de tradução. O mecanismo de tradução sinaliza a um conjunto de *Policy Decision Points* (PDP) (elementos responsáveis por traduzir as políticas de rede descritas em linguagem de alto nível para ações de configuração específicas dos dispositivos de rede) do domínio local para que estes apliquem as políticas de rede criadas. Os PDPs, então, as

aplicam em de um conjunto de *Policy Enforcement Points* (PEPs) (elementos da rede onde as políticas são efetivamente aplicadas). A comunicação entre o sistema editor de políticas da grade e o mecanismo de tradução de cada domínio administrativo envolvido, assim como entre cada mecanismo de tradução e os PDPs, é realizada através da tecnologia WebServices (NEISSE, 2004).

4.2 Metodologia para Análise do Gerenciamento em Contextos Modernos

As redes e os aspectos de rede apresentados acima são exemplos de situações encontradas nas redes atuais que possuem características distintas daquelas usualmente encontradas em redes tradicionais, incluindo a existência de múltiplos domínios administrativos, a necessidade de cooperação entre estes para a execução de funcionalidades, a presença de grande distribuição para a operação da rede, etc. Como anteriormente discutido, neste documento tais situações serão referidas como ***contextos modernos***.

As características distintas encontradas nos contextos modernos levam a requisitos de gerenciamento distintos quando comparados aos requisitos de gerenciamento de redes tradicionais. A fim de auxiliar o levantamento de tais requisitos e a análise das características do gerenciamento destes contextos, foi elaborada uma metodologia que se baseia em um conjunto de itens a serem analisados ao se planejar o gerenciamento de um contexto. Tal metodologia foi construída através do levantamento e da análise dos aspectos dos contextos de rede que lhes atribuem características modernas, sendo baseada em características funcionais a serem consideradas para o contexto.

A metodologia desenvolvida tem como foco principal os aspectos do contexto que levam à necessidade de arquiteturas de gerenciamento distribuídas e sem hierarquia administrativa, tais como a presença de múltiplos domínios administrativos na rede e outros fatores que acarretem em requisitos de distribuição do gerenciamento. A metodologia objetiva auxiliar a identificação dos paradigmas e dos modelos de gerenciamento adequados para o contexto, servindo ainda como roteiro para compreender melhor as características do contexto, as limitações e os requisitos para seu gerenciamento. Contribui também, desta forma, no planejamento das soluções de gerenciamento.

Cabe destacar que a metodologia não pretende fornecer uma definição específica acerca do paradigma ou do modelo de gerenciamento a ser adotado para um dado contexto, já que para este fim a metodologia necessitaria ser construída de modo específico e preciso para cada contexto, em virtude da heterogeneidade dos fatores envolvidos. Esta metodologia visa, sim, servir de guia para facilitar esta análise, fornecendo um roteiro de fatores que devem ser considerados para auxiliar a identificação das abordagens de gerenciamento mais adequadas para serem empregadas no contexto.

A metodologia é baseada em itens divididos em quatro grupos, objetivando-se que, ao final destes, existam informações para auxiliar a identificação do paradigma e do modelo a serem adotados para ao gerenciamento do contexto. O primeiro grupo de itens compreende a definição do contexto sendo analisado. Seus itens visam identificar se está sendo analisado uma arquitetura de rede ou um aspecto de rede (situação, aplicação, serviço, problema) de rede tradicional, porque tal contexto está sendo

analisado e o que se objetiva analisar, incluindo ainda a discussão se serão analisadas também soluções de gerenciamento já existentes.

O segundo grupo inclui itens para o levantamento e a análise do contexto propriamente dito, incluindo características da rede que afetam as aplicações e os serviços em geral (para contextos do tipo rede) e características da situação/aplicação/serviço/problema e da rede onde este se encontra (para contextos do tipo aspecto de rede). Abrange, entre outros, a estrutura do contexto, a presença de múltiplos domínios administrativos, a necessidade de interação ou cooperação entre os domínios, as restrições de QoS encontradas.

O terceiro grupo compreende as limitações e os requisitos para o gerenciamento do contexto em função das suas características levantadas no grupo anterior. Exemplos incluem considerações sobre o impacto do tráfego de gerenciamento, as limitações e as dificuldades para o gerenciamento causadas por restrições de QoS das redes, as restrições de recursos e os controles específicos requeridos, assim como quais são os requisitos específicos de gerenciamento para o contexto.

Por fim, o quarto grupo contém considerações acerca de como pode ser realizado o gerenciamento do contexto. Este grupo compreende itens sobre a arquitetura de gerenciamento, a necessidade de distribuição, o modo como são realizadas as interações entre as entidades de gerenciamento, a necessidade de interações entre as entidades de gerenciamento, a confiabilidade das informações recebidas, etc.

A separação em grupos objetivou organizar as informações seguindo um nível de conhecimento gradativo, a fim de que os itens de maior complexidade e que envolvem um número maior de fatores possam fazer uso da análise realizada em itens anteriores relacionados ou dos quais são dependentes. Como pode ser visto, o primeiro e segundo grupo contém itens que representam informações que devem ser levantadas sobre o contexto. O terceiro grupo contém itens que envolvem a análise a respeito de aspectos que devem ser considerados para o gerenciamento, tais como limitações e requisitos, considerando, de modo mais específico, informações obtidas nos itens do segundo grupo. O quarto grupo, por sua vez, contém itens que guiam a análise de como o gerenciamento pode ser realizado considerando as informações levantadas e analisadas nos três grupos anteriores.

Os itens a serem analisados em cada grupo são apresentados nas tabelas 4.1 a 4.4. Como será visto, alguns itens variam conforme o tipo de contexto sendo analisado, isto é, se este representa uma arquitetura de rede completa ou um particular aspecto de uma rede. Com fins didáticos, os itens dos dois tipos de contexto foram dispostos na mesma tabela, cada qual ocupando uma coluna se estes forem diferentes, objetivando permitir visualizar com facilidade as similaridades e as diferenças na análise de cada tipo de contexto. Já nas linhas onde o item aplica-se para ambos os tipos de contexto, o item foi disposto com uma coluna única para ambos os tipos.

Os itens de cada grupo não necessitam ser seguidos ou respondidos de forma inflexível; eles devem ser utilizados como uma orientação ou sugestão de aspectos a serem analisados. Além disto, para um dado contexto, alguns itens podem não ser aplicados; neste caso, eles não necessitam ser respondidos.

Tabela 4.1: Grupo 1- Definição do contexto sendo analisado

	Arquitetura de Rede Completa	**Aspecto de Rede**
	Definição da rede	**Definição do contexto (situação/ aplicação/ serviço/ problema)**
G1.1 Definição	1) Qual a rede sendo analisada?	1) Qual o contexto sendo analisado? *Qual o tipo de contexto: uma aplicação, serviço, problema, situação na rede? Qual o contexto? Qual a solução de gerenciamento sendo analisada?*
	2) Definir porque tal contexto está sendo analisado. *Está sendo analisado porque possui características distintas? Porque seu gerenciamento parece ser distinto ou complexo? Porque possui requisitos especiais de gerenciamento?*	
	3) Contextualizar o que se objetiva analisar. *Serão avaliadas possíveis soluções para o gerenciamento deste contexto? Serão avaliadas soluções já propostas?*	

Tabela 4.2: Grupo 2 - Características do contexto

	Arquitetura de Rede Completa	**Aspecto de Rede**
	Características da rede que afetam aplicações e serviços em geral	**Características do contexto (situação/ aplicação/ serviço/ problema) e da rede onde ele ocorre**
G2.1 Estrutura, funcionamento	1) Qual a organização, a estrutura da rede (topologia)? *Existe ponto central? Existe alguma forma de hierarquia? Algum trecho ou porção da rede tem hierarquia?*	1) Qual a organização, a estrutura existente no contexto? *Existe ponto central? Existe alguma forma de hierarquia? Algum trecho ou porção do contexto utiliza hierarquia?*
	2) Rede pode envolver mais de um domínio administrativo? Quando isto ocorre?	2) Contexto apresenta arquitetura distribuída? Pode envolver mais de um domínio administrativo?
	3) Se envolver mais de um domínio administrativo, como é a estrutura *dentro* e *entre* os domínios?	
	4) Que considerações podem ser feitas em relação à necessidade de domínios (e seus nodos) interagirem uns com os outros (e cooperarem, quando requerido)? *Há uma obrigação legal para interação e cooperação? É necessário para a própria funcionalidade? Existe a figura do nodo egoísta (nodo que utiliza recursos da rede sem contribuir para a comunidade)?*	
G2.2 Características que podem afetar o gerenciamento	5) Rede possui restrições de QoS? Possui limitações de recursos?	5) Contexto exige requisitos especiais de rede? Redes envolvidas possuem restrições de QoS ou possuem limitações de recursos? Contexto afeta condições da rede?
	6) Rede possui outras limitações importantes?	6) Contexto possui outras limitações, dificuldades importantes?

Tabela 4.3: Grupo 3 – Limitações e requisitos para o gerenciamento

	Arquitetura de Rede Completa	**Aspecto de Rede**
	Limitações e requisitos para o gerenciamento desta rede em função das características da rede	**Limitações e requisitos para o gerenciamento deste contexto em função das características deste**
G3.1 Limitações e restrições para o gerenciamento	1) Que considerações podem ser feitas sobre o tráfego de gerenciamento e seu impacto? *Possui restrições muito severas em relação ao tráfego de gerenciamento? Por quê?*	1) Que considerações podem ser feitas sobre o tráfego para gerenciamento do contexto? *Possui restrições muito severas em relação ao tráfego de gerenciamento? Por quê?*
	2) Que outras limitações e dificuldades de gerenciamento surgem por características da rede? *Considerar restrições de QoS das redes, restrições de armazenamento das informações de gerenciamento, controles ou mecanismos específicos requeridos, diversidade dos nodos, etc.*	2) Que outras limitações e dificuldades de gerenciamento surgem por características do contexto? *Considerar restrições de QoS das redes, restrições armazenamento das informações de gerenciamento, controles ou mecanismos específicos requeridos, diversidade dos nodos, etc.*
G3.2 Requisitos específicos de gerenciamento	3) Que requisitos específicos de gerenciamento são causados pelas características destas redes?	3) Que requisitos específicos de gerenciamento são causados pelas características do contexto?

Tabela 4.4: Grupo 4 – Análise do gerenciamento

	Arquitetura de Rede Completa	**Aspecto de Rede**
	Considerações sobre como pode ser realizado o gerenciamento da rede	**Considerações sobre como pode ser realizado o gerenciamento do contexto**
G4.1 Estrutura do gerenciamento	1) Rede exige distribuição na arquitetura de gerenciamento? *Exige para prover escalabilidade? Para oferecer tolerância a falhas? Para funcionalidades de gerenciamento serem mais efetivas? Por necessidades administrativas? Por outros fatores?*	1) Contexto exige distribuição na arquitetura de gerenciamento? *Exige para prover escalabilidade? Para oferecer tolerância a falhas? Para funcionalidades de gerenciamento serem mais efetivas? Por necessidades administrativas? Por outros fatores?*
	2) Quais as possíveis arquiteturas para as soluções de gerenciamento? *Pode existir estrutura centralizada? Hierárquica? Considerar a presença de diferentes domínios administrativos discutidos nos itens anteriores, se houverem.*	

	3) Como podem ser (ou são, se há uma ou mais soluções sendo analisadas) as interações de gerenciamento (solicitação, execução e controle de ações de gerenciamento)? *Quem solicita as ações de gerenciamento?* *Quem executa as ações de gerenciamento?* *Quem controla as ações de gerenciamento (são controladas por uma entidade de gerenciamento específica, ou cada entidade controla suas ações)?*
G4.2 Interações de gerenciamento	4) Considerações sobre a necessidade de interação entre as entidades de gerenciamento, suas obrigações, confiabilidade das informações recebidas, etc. *Há necessidade dos domínios (e seus nodos) interagirem uns com os outros para o fornecimento de informações ou a execução de atividades de gerenciamento?* *Como são os direitos e obrigações das entidades, em relação a ações de gerenciamento para outros domínios?* *Como é a confiança dos domínios/nodos para solicitarem informações uns dos outros, requisitarem ações, etc.?*

4.3 Análise dos Estudos de Caso de Contextos Modernos

A seção 4.1 apresentou três contextos modernos encontrados em redes atuais. Uma metodologia para avaliar tal tipo de contexto, por sua vez, foi discutida na seção anterior. A presente seção analisa os três estudos de caso de contextos apresentados na seção 4.1 utilizando tal metodologia, com o intuito de discutir quais paradigmas e modelos podem ser empregados no gerenciamento de cada contexto. Como contribuição adicional, tal análise auxilia a compreender as características de tais contextos, as restrições e os requisitos para seu gerenciamento.

4.3.1 Redes *Mesh* Sem Fio

Uma breve revisão sobre as redes *mesh* sem fio foi apresentada na seção 4.1.1. Estas redes possuem características distintas das tradicionais, tal como sua própria forma de comunicação, baseada na cooperação entre seus nodos. A análise das características de tais redes e de suas características de gerenciamento seguindo a metodologia proposta na seção 4.2 é apresentada nas tabelas a seguir. As informações utilizadas para esta análise foram obtidas a partir do levantamento apresentado na seção 4.1.1 e de publicações da área (LUNDGREN et al, 2006) (DUARTE et al, 2007) (JARRETT; WARD, 2006) (AKYILDIZ; WANG; WANG, 2005) (RIGGIO et al, 2007) (SANTHANAM et al, 2006) (SAILHAN et al, 2007), especialmente nos itens referentes à analise pertinente aos grupos 1, 2 e 3 da metodologia.

A análise realizada foi baseada no conceito de que certas redes *mesh* sem fio podem ter cada nodo administrado individualmente por seu próprio proprietário, representando o lado extremo de uma rede com múltiplos domínios administrativos (JARRETT; WARD, 2006), sendo um exemplo típico as redes *mesh* sem fio comunitárias (BRUNO; CONTI; GREGORI, 2005) (ISHMAEL et at, 2008). Com base neste conceito, diferentes tipos de redes *mesh* podem ser identificados, incluindo: redes pertencentes a apenas uma organização com apenas um domínio administrativo; redes onde há um *backbone mesh* formado por um ou mais domínios administrativos e clientes *mesh*

representando nodos com menor participação no processamento da rede, tal como em redes fornecidas por provedores; e redes com vários domínios administrativos sem hierarquia administrativa entre eles, tipicamente o encontrado em redes comunitárias. Em virtude de suas características particulares, esta análise enfocou de modo principal este último tipo de rede.

As tabelas 4.5 a 4.8 discutem os itens analisados para cada grupo da metodologia proposta. Para proporcionar melhor visualização, os itens da metodologia são apresentados em tabelas simples, um item por linha, sem separar os itens de acordo com as subdivisões dentro dos grupos, e sem apresentar os dados explicativos dos itens (dados destacados em estilo de fonte itálico nas tabelas da seção 4.2).

Tabela 4.5: Redes *mesh* sem fio - Definição do contexto sendo analisado (Grupo 1)

Item	**Considerações**
1) Qual a rede sendo analisada?	Redes *mesh* sem fio
2) Definir porque tal contexto está sendo analisado.	Estas redes possuem estrutura em malha dinâmica com roteamento realizado de forma cooperativa. A comunicação é realizada de modo coletivo: a conectividade da rede utiliza o conjunto de nodos pertencentes a esta. A topologia da rede precisa ser obtida verificando a rede como um todo (coletivamente) e é extremamente dinâmica. Alguns nodos possuem restrições severas de consumo de energia. Tais aspectos trazem dificuldades e características distintas para o gerenciamento destas redes. Por outro lado, um gerenciamento adequado destas redes é muito importante justamente em virtude da dinamicidade desta rede, da significativa flutuação na qualidade do sinal, da interrupção de conexões, da comunicação ser baseada na cooperação entre nodos, da necessidade de controle de nodos maliciosos e egoístas, entre outros (LUNDGREN et al, 2006)(DUARTE et al, 2007)(RIGGIO et al, 2007).
3) Contextualizar o que se objetiva analisar.	Objetiva-se analisar as características para o adequado gerenciamento de redes *mesh* sem fio, de modo a suprir suas principais necessidades de gerenciamento. Em especial, foca-se nesta análise redes que possam ser classificadas como pertencentes a vários domínios administrativos distintos, sem hierarquia administrativa entre eles.

Tabela 4.6: Redes *mesh* sem fio - Características do contexto (Grupo 2)

Item	**Considerações**
1) Qual a organização, a estrutura da rede (topologia)?	Os nodos da rede organizam-se em malha, tipicamente sem hierarquia entre eles. Contudo, dois níveis de organização são admitidos em certos contextos: em arquiteturas de infra-estrutura e arquiteturas híbridas, como visto na seção 4.1.1, há nodos formando um *backbone* e nodos com função de cliente. Dentro de um *backbone* e entre os clientes, não há nenhuma forma de organização, utilizando-se uma estrutura plana.

2) Rede pode envolver mais de um domínio administrativo? Quando isto ocorre?	As redes *mesh* sem fio podem envolver mais de um domínio administrativo, por exemplo, quando uma rede é composta por proprietários, residências e grupos diferentes. Isto ocorre freqüentemente em redes comunitárias e em redes rurais onde cada propriedade contribui com um roteador *mesh*: nestas redes, juntas, as propriedades colaboram (através de seus nodos) para criar a conectividade da rede. Pode-se considerar, nestes casos, que, no extremo, cada nodo é administrado individualmente, pelo seu próprio proprietário, formando uma rede com um nodo em cada domínio administrativo (JARRETT; WARD, 2006).
3) Se envolver mais de um domínio administrativo, como é a estrutura *dentro* e *entre* os domínios?	Em tais redes, não existe uma estrutura física distinta entre nodos do mesmo domínio administrativo e entre nodos de diferentes domínios, a menos que estas diferenças sejam devidas à arquitetura de rede empregada (por exemplo, redes de infra-estrutura, com nodos roteadores pertencentes a um domínio, e nodos clientes pertencentes a outros). Os nodos de tais redes são conectados por uma estrutura em malha através de meio sem fio, e a existência de diferentes domínios não afeta a estrutura em malha e sua topologia. A presença de diferentes domínios é, assim, tipicamente totalmente transparente para a estrutura e a topologia da rede. Em redes com arquitetura de infra-estrutura ou arquitetura mista, os nodos participantes do *backbone* e os nodos clientes podem fazer parte do mesmo domínio administrativo ou de domínios distintos, sem seu papel estar relacionado com o domínio a que faz parte. Podem existir redes que organizem os domínios conforme a arquitetura da rede (por exemplo, redes de infra-estrutura, com nodos roteadores pertencentes a um domínio, e nodos clientes pertencentes a outros), porém tais diferenças se devem à arquitetura.
4) Que considerações podem ser feitas em relação à necessidade de domínios (e seus nodos) interagirem uns com os outros (e cooperarem, quando requerido)?	Como visto acima, as redes *mesh* sem fio podem envolver mais de um domínio administrativo (*e.g.*, redes comunitárias), sendo a existência de domínios transparente para a rede. A comunicação destas redes é obtida através do roteamento provido cooperativamente pelos nodos, independente dos domínios administrativos a que eles fazem parte. Deste modo, a fim de manter a funcionalidade adequada da rede, todos os nodos devem cooperativamente retransmitir o tráfego de outros nodos: esta é uma necessidade para a manutenção adequada da rede. Contudo, especialmente pelo fato dos nodos poderem pertencer a múltiplos proprietários, nodos presentes no meio da rede podem começar a se comportar de modo egoísta (SANTHANAM et al, 2006)(JARRETT; WARD, 2006), descartando o tráfego originário de outros nodos ao invés de retransmiti-lo, com o intuito de maximizar a vazão de seu próprio tráfego. Este comportamento pode causar grandes danos na rede, se tornando ainda pior se o nodo estiver localizado em pontos próximos aos *gateways* com a Internet, já que nodos próximos a estes *gateways* concentram grande volume de tráfego sendo retransmitido.
5) Rede possui restrições de QoS? Possui limitações de recursos?	▪ Redes *mesh* sem fio são extremamente dinâmicas e possuem conectividade intermitente. Possuem significativa flutuação na qualidade do sinal causada pelo meio físico não confiável, obstáculos, interferências, nodos ocultos e combinações variáveis no ambiente (SAILHAN et al, 2007). ▪ Por sua estrutura em malha com conectividade através de múltiplos saltos, muitas vezes o tráfego entre dois nodos precisa passar por vários nodos intermediários até atingir seu destino. Isto faz com que

	uma transmissão consuma largura de banda em todos os enlaces envolvidos e demande processamento nos vários nodos intermediários. Deste modo, a largura de banda destas redes pode possuir restrições. ▪ Muitas vezes, nodos clientes *mesh* são instalados em equipamentos com hardware e software muito mais limitados que roteadores das redes. Assim, freqüentemente nodos cliente *mesh* possuem restrições de recursos, tais como baixo poder de processamento e espaço em disco limitado (DUARTE et al, 2007), além de restrições quanto ao consumo de energia disponível para suas operações (AKYILDIZ; WANG; WANG, 2005).
6) Rede possui outras limitações importantes?	▪ Como visto, redes *mesh* sem fio são extremamente dinâmicas e possuem conectividade intermitente (SAILHAN et al, 2007). Em função da elevada variação na qualidade dos enlaces destas redes, há freqüentes alterações no roteamento da rede, o que pode levar a interrupções em conexões existentes, tornando nodos inacessíveis ou acessíveis através de diferentes conexões. Além disto, certos nodos de tais redes podem ser bastante voláteis.

Tabela 4.7: Redes *mesh* sem fio - Limitações e requisitos para gerenciamento (Grupo 3)

Item	**Considerações**
1) Que considerações podem ser feitas sobre o tráfego de gerenciamento e seu impacto?	Em função da estrutura em malha com comunicação em múltiplos saltos discutida anteriormente, o tráfego de gerenciamento deve ser o menor possível. As tarefas de gerenciamento que causam maior tráfego (tal como a coleta de dados de desempenho) devem ser disparadas, sempre que possível, próximas aos nodos gerenciados, a fim de afetar um menor número de nodos com este tráfego. Em virtude disto, arquiteturas de monitoração que empregam o *polling* de cada nodo individualmente devem ser cuidadosamente avaliadas antes de serem utilizadas, já que podem causar um elevado tráfego na rede. Por outro lado, as particularidades desta rede precisam ser consideradas ao analisar mecanismos de monitoração: em virtude de sua estrutura, a utilização de um *probe* de monitoração passiva pode resultar na coleta de dados parciais da rede, já que nem todas as comunicações entre os nodos poderão ser monitoradas pelo *probe*, que visualizará apenas uma porção da rede (DUARTE et al, 2007).
2) Que outras limitações e dificuldades de gerenciamento surgem por características da rede?	Algumas dificuldades para o gerenciamento de redes *mesh* foram discutidas acima, incluindo: ▪ O impacto do gerenciamento na rede deve ser mínimo. O tráfego de gerenciamento deve ser mínimo e as restrições dos recursos devem ser consideradas. Além disto, *probes* passivos de monitoração podem possuir limitações para monitorar a rede completa, mas *polling* pode consumir muita largura de banda. Além destas, outras dificuldades devem ser consideradas, incluindo: ▪ As restrições de armazenamento que podem estar presentes em nodos destas redes, vistas acima, precisam ser consideradas ao se avaliar onde armazenar as informações de gerenciamento. Em nodos com restrições, é necessário armazenar no máximo pequena quantidade de informações. Além disto, é preciso armazenar as informações de modo que nodos que saiam da rede não levem consigo as informações

	de gerenciamento relevantes. Por fim, é preciso combinar as restrições de localização para armazenamento de dados e volatilidade dos nodos com a limitação do tráfego de gerenciamento, de modo que este não cause impacto na rede. Assim, arquiteturas de operações de gerenciamento que permitam armazenar as informações próximas aos nodos onde foram coletadas precisam ser consideradas, porém a volatilidade e as restrições de disco também precisam ser levadas em conta. ▪ Gerenciamento deve conseguir lidar com alterações freqüentes de roteamento. Nodos podem ficar inacessíveis ou passar a ser gerenciados através de outras conexões (DUARTE et al, 2007). ▪ Topologia e condições da rede mudam freqüentemente. Gerenciamento precisa lidar com esta dinamicidade, incluindo manutenção da topologia e de informações da rede (LUNDGREN et al, 2006). ▪ Redes possuem nodos muito heterogêneos, inclusive no modo como fornecem informações de gerenciamento: gerenciamento deve ser capaz de lidar esta característica. ▪ A estrutura das redes *mesh* que faz com que sua conectividade dependa de nodos participantes pertencentes a vários domínios administrativos exige mecanismos para segurança e controle de nodos maliciosos e egoístas.
3) Que requisitos específicos de gerenciamento são causados pelas características destas redes?	Como visto, as redes *mesh* possuem grande dinamicidade, com topologia e características mudando freqüentemente. Isto traz requisitos específicos de gerenciamento, tais como: ▪ As informações de topologia precisam ser obtidas de modo freqüente e dados históricos são importantes já que há grande dinamicidade da rede (LUNDGREN et al, 2006). ▪ As informações da rede coletadas no gerenciamento precisam ser obtidas coletivamente para serem efetivas. ▪ A monitoração destas redes é importante também para adaptar o comportamento do nodo dependendo de condições operacionais em particular (tais como tipo de tráfego, perturbações nos canais, estado da rede, presença de nodos egoístas e/ou maliciosos, etc.) (RIGGIO et al, 2007). ▪ As informações de gerenciamento necessitam estar disponíveis para todos os nodos da rede, de modo que cada nodo possa adaptar seu comportamento (RIGGIO et al, 2007). ▪ Como visto, redes *mesh* sem fio podem possuir nodos egoístas, que usam o serviço da rede, mas não realizam a retransmissão dos pacotes originados em outros nodos, prejudicando a conectividade destas redes e causando problemas de roteamento. Tais situações precisam ser detectadas e tratadas pelas atividades de gerenciamento.

Tabela 4.8: Redes mesh sem fio – Análise do gerenciamento (Grupo 4)

Item	Considerações
1) Rede exige distribuição na arquitetura de gerenciamento?	▪ Escalabilidade: A importância em gerar baixo volume de tráfego para o gerenciamento estimula ou até mesmo exige a distribuição do gerenciamento, a fim de que as atividades de gerenciamento possam ser coletadas e processadas próximas aos nodos onde as informações são originadas. Com distribuição, menor volume de tráfego é gerado, sendo consumida menor largura de banda e envolvendo menor número de nodos no processamento do tráfego de gerenciamento. ▪ Tolerância a falhas: A distribuição das atividades de gerenciamento permite lidar com a conectividade intermitente dos nodos nestas redes, evitando a interrupção das atividades de gerenciamento quando a comunicação entre nodos for perdida. ▪ Funcionalidade: A utilização de operações distribuídas traz benefícios para as atividades de gerenciamento destas redes pela capacidade de obter informações e atuar simultaneamente sobre diversas porções da rede. ▪ Necessidades administrativas: Como visto anteriormente, algumas redes possuem nodos em diferentes domínios administrativos. Nestas redes, é necessário o emprego de atividades de gerenciamento distribuídas, já que a administração dos nodos de cada domínio é feita pela equipe deste domínio, porém o gerenciamento exige a obtenção de informações da rede completa para atividades de monitoração e diagnóstico, incluindo informações de outros domínios, o que exige a interação entre o gerenciamento de cada domínio.
2) Quais as possíveis arquiteturas para as soluções de gerenciamento?	Arquiteturas centralizadas não são possíveis, em função das necessidades funcionais e administrativas, além de restrições quanto à escalabilidade e tolerância a falhas, como visto acima. Arquiteturas distribuídas hierárquicas não são adequadas em redes com vários domínios administrativos, já que um domínio não deseja e usualmente não permite que seus nodos sejam controlados por outros domínios. Assim, estas redes exigem o gerenciamento a partir de arquiteturas distribuídas, porém não hierárquicas.
3) Como podem ser (ou são, se há uma ou mais soluções sendo analisadas) as interações de gerenciamento (solicitação, execução e controle de ações de gerenciamento)?	▪ Requisição de ações de gerenciamento: Em redes *mesh* com vários domínios administrativos, ao menos um nodo em cada domínio deve poder requisitar que uma atividade de gerenciamento seja executada. Porém, como as redes *mesh* possuem estrutura plana (dentro de domínios e entre domínios), tipicamente qualquer nodo deveria poder disparar as requisições. Controles de permissões e acesso podem ser necessários para controlar que atividades um nodo de um domínio pode requisitar aos nodos dos demais domínios – porém as requisições devem poder ser realizadas por todos. ▪ Ações de gerenciamento: Pelas características distribuídas, pelo fato de serem extremamente dinâmicas e pelas necessidades de obtenção de topologia e histórico desta ao longo de toda a rede, as ações devem ser executadas de modo distribuído. Idealmente, todos os nodos da rede *mesh* deveriam executar atividades de gerenciamento. Controles para atribuir atividades com menores requisitos para nodos clientes *mesh* com maiores restrições de recursos podem

	ser utilizados. ▪ Controle das ações de gerenciamento: Pelas características distribuídas, as atividades de gerenciamento devem ser concebidas para que haja pouco controle a partir um (ou poucos) nodos. Uma solução plana seria a mais indicada, onde cada nodo controla a ação sendo executada em seu nodo, solicita as ações dos nodos vizinhos e todos os nodos executam de modo autônomo.
4) Considerações sobre a necessidade de interação entre as entidades de gerenciamento, suas obrigações, confiabilidade das informações recebidas, etc.	Diversas atividades de gerenciamento necessitam ser realizadas de modo distribuído ao longo de vários nodos da rede, exigindo inclusive a interação e a cooperação entre os vários nodos da rede para serem efetivas e o gerenciamento da rede não ser prejudicado (*e.g.*, identificação da topologia da rede, detecção de falhas e problemas de desempenho na rede, detecção de nodos maliciosos e egoístas, etc.). Como visto, tais nodos podem pertencer a diversos domínios administrativos, exigindo, desta forma, que as atividades de gerenciamento sejam executadas pelos vários domínios, que têm como benefícios os resultados das próprias atividades de gerenciamento. A exigência de cooperação entre os nodos para as atividades de gerenciamento, assim como as funções desempenhadas e disponíveis para estes, podem ser reguladas por contratos estabelecidos para a participação em redes *mesh*, variando de acordo com o tipo da rede. Por exemplo, numa rede metropolitana, mantida por um ou mais provedores, os nodos clientes *mesh* podem possuir direitos bem restritos, com poucas funções de gerenciamento disponíveis para eles. Já em redes comunitárias (foco desta análise), tipicamente não há condições especiais para nodos diferentes: os diversos nodos da rede devem, por exemplo, ter meios para identificar nodos maliciosos e nodos egoístas e tomar ações corretivas baseadas nestas informações. De modo análogo, todos os nodos de tais redes comunitárias tipicamente necessitam desempenhar as atividades de gerenciamento definidas. De forma semelhante, a confiabilidade das informações de gerenciamento fornecidas por outros nodos depende do tipo de rede *mesh* sem fio em questão. Em redes comunitárias, um controle elevado das informações recebidas de outros nodos é necessário em virtude da possível presença de nodos egoístas e maliciosos (JARRETT; WARD, 2006), que podem fornecer informações incorretas.

A análise realizada destaca que as redes *mesh* sem fio possuem características peculiares, como, por exemplo, a comunicação baseada na cooperação entre os múltiplos nodos, os enlaces com significativa flutuação na qualidade do sinal, a topologia dinâmica com interconexões intermitentes, a presença de nodos com recursos restritos, a possível existência de nodos egoístas, etc. Tais características dão origem a requisitos distintos de gerenciamento, tais como a necessidade de suportar alterações freqüentes de topologia e roteamento, a necessidade de obter informações ao longo de toda a rede para sua monitoração, a necessidade de detectar a presença de nodos egoístas, entre outros.

Os paradigmas adequados para o gerenciamento de tais redes variam conforme o tipo de rede sendo gerenciada. Em qualquer tipo de rede, como visto ao longo dos itens da tabela 4.8 (grupo 4), a utilização do paradigma centralizado não é possível, sendo necessário o emprego de paradigmas distribuídos. Dentre os paradigmas distribuídos, a utilização do paradigma fracamente distribuído não é recomendada por alguns

requisitos de gerenciamento destas redes. A tolerância a falhas, por exemplo, é aperfeiçoada com a forte distribuição das atividades de gerenciamento, já que redes *mesh* sem fio possuem conectividade intermitente, com elevada variação na qualidade dos enlaces da rede e presença de nodos voláteis, levando a interrupções em conexões utilizadas para o gerenciamento e ao particionamento da rede. Deste modo, o uso de forte distribuição das atividades de gerenciamento, com a atribuição de atividades de gerenciamento complexas ao longo de entidades presentes em um vasto número de nodos, permite que tais entidades tomem ações corretivas quando o contato com as outras entidades for perdido. Além disto, as funções de gerenciamento também podem ser aperfeiçoadas com a utilização de forte distribuição: em virtude da conectividade intermitente, a topologia e as informações de monitoração da rede precisam ser obtidas de modo freqüente e serem coletadas ao longo de toda a rede para serem efetivas. Assim, o emprego de entidades de monitoração ao longo de toda a rede possibilita que estas atividades sejam desempenhadas de modo mais preciso e com maior simultaneidade.

Deste modo, o emprego de paradigmas fortemente distribuídos é recomendado para o gerenciamento de redes *mesh* sem fio de qualquer tipo. Dentre os paradigmas fortemente distribuídos, paradigmas que definem a ocorrência de subordinação entre entidades podem ser empregados para redes com apenas um domínio administrativo ou redes que possuam uma hierarquia administrativa. Por outro lado, em redes com vários domínios administrativos, sem hierarquia administrativa entre eles, tal como em redes comunitárias típicas, um paradigma com subordinação não pode ser empregado, já que um domínio não pode ter autoridade sobre os demais. Informações de gerenciamento devem ser compartilhadas e trocadas entre os nodos de vários domínios, assim como atividades de gerenciamento podem ser solicitadas para outros domínios, porém as entidades possuem autonomia para a realização destas atividades, levando à necessidade de paradigmas fortemente distribuídos sem subordinação. De acordo com as taxonomias apresentadas na seção 3.2, tais condições se enquadram, em relação à taxonomia de Martin-Flatin, Znaty e Hubaux, no paradigma cooperativo fortemente distribuído. Em relação à taxonomia de Schönwälder, Quittek e Kappler, como esta concentra-se na estrutura das interações entre as entidades, sem determinar expressamente aspectos de subordinação, tais condições se enquadram no paradigma fortemente distribuído e no paradigma cooperativo, com a restrição de que os modelos de gerenciamento empregados suportem que as entidades realizem suas atividades com autonomia, controlando as atividades requisitadas por nodos de outros domínios.

4.3.2 Ataques de Negação de Serviços Distribuídos

A seção 4.1.2 discutiu a importância e a necessidade de muitos tipos de ataques DDoS de força bruta serem detectados e tratados nas *redes intermediárias* entre as múltiplas máquinas origem do ataque e o alvo. Em função deste requisito, tais mecanismos de detecção e reação apresentam características distintas dos mecanismos utilizados no gerenciamento de redes tradicional. A análise das características dos ataques DDoS e dos mecanismos utilizados para sua detecção e tratamento é apresentada nas tabelas a seguir. Para esta análise, dois mecanismos deste tipo foram identificados na literatura e analisados de modo particular: o proposto em (IOANNIDIS; BELLOVIN, 2002) e o proposto em (ZHANG; PARASHAR, 2006), ambos mecanismos de detecção e reação a ataques realizados em redes intermediárias baseados em uma arquitetura distribuída, fazendo uso da cooperação entre os roteadores destas redes.

Assim como nos contextos de gerenciamento anteriores, esta análise é baseada na metodologia apresentada na seção 4.2. As informações para esta análise foram obtidas no levantamento apresentado na seção 4.1.2, assim como em publicações relativas a ataques DDoS e mecanismos para detecção e tratamento destes (PENG; LECKIE; RAMAMOHANARAO, 2007) (MIRKOVIC; REIHER, 2004) (ZHANG; PARASHAR, 2006) (IOANNIDIS; BELLOVIN, 2002) (OLIVIERO; PELUSO; ROMANO, 2008).

Na metodologia proposta, os ataques DDoS representam "problemas modernos em redes tradicionais" e os mecanismos de detecção e tratamento para tais ataques representam "soluções de gerenciamento" para tais problemas. Cabe destacar que, neste caso, a metodologia é empregada tanto para analisar as características de "soluções de gerenciamento" em geral como para analisar algumas "soluções de gerenciamento" em particular, isto é, analisa-se os mecanismos de detecção e reação que são realizados em redes intermediárias, utilizando como exemplo os dois mecanismos específicos identificados na literatura (IOANNIDIS; BELLOVIN, 2002) e (ZHANG; PARASHAR, 2006).

As tabelas 4.9 a 4.12 discutem os itens analisados para cada grupo da metodologia. A apresentação dos dados analisados segue o mesmo formato empregado para disposição das tabelas e itens da análise de redes *mesh* sem fio.

Tabela 4.9: Ataques DDoS - Definição do contexto sendo analisado (Grupo 1)

Item	**Considerações**
1) Qual o contexto sendo analisado?	Ataques de negação de serviço distribuídos de força bruta, objetivando-se tratar os tipos de ataques em que os mecanismos de detecção e reação localizados no alvo ou em sua rede não são efetivos e em que os mecanismos localizados na rede origem possuem limitações (necessitando, desta forma, de mecanismos nas redes intermediárias entre os nodos origem *zumbis* e o alvo do ataque). Deste modo: ▪ Tipo de contexto que está sendo analisado: Um problema encontrado em redes atuais e a solução empregada para este. ▪ Contexto/situação/problema: Ataques de negação de serviço distribuídos de força bruta. ▪ Solução de gerenciamento sendo analisada: Mecanismos de detecção e reação a ataques realizados em redes intermediárias, que visam filtrar o tráfego de ataques utilizando roteadores entre as fontes do ataque e o alvo. Dois mecanismos propostos na literatura são analisados como exemplos.
2) Definir porque tal contexto está sendo analisado.	Muitos tipos de ataques de negação de serviço distribuídos não são tratados de modo eficaz através de mecanismos executados na rede destino ou nodo alvo (ZHANG; PARASHAR, 2006)(MIRKOVIC; REIHER, 2004). Tais tipos de ataques precisam ser tratados através de mecanismos de detecção e reação executados nas redes intermediárias entre os nodos de origem *zumbis* e o nodo alvo. Importantes mecanismos de tratamento a ataques são executados com a cooperação dos roteadores intermediários entre os nodos origem do ataque e o nodo alvo. Tais roteadores realizam procedimentos para detectar pacotes que podem pertencer a um ataque e filtrar preferencialmente estes pacotes, propagando esta informação para

	outros roteadores (IOANNIDIS; BELLOVIN, 2002) (ZHANG; PARASHAR, 2006). Mecanismos de tratamento a ataques como estes representam abordagens de gerenciamento com características distintas, que são executados utilizando arquiteturas de gerenciamento alternativas às tradicionalmente empregadas.
3) Contextualizar o que se objetiva analisar.	Objetiva-se avaliar as características dos mecanismos de detecção e reação a ataques executados em redes intermediárias, tomando como exemplos dois mecanismos existentes na literatura, propostos em (IOANNIDIS; BELLOVIN, 2002) e (ZHANG; PARASHAR, 2006). Para esta análise, quando necessário, as características do problema (ataques de negação de serviço distribuídos) serão também discutidas.

Tabela 4.10: Ataques DDoS - Características do contexto (Grupo 2)

Item	**Considerações**
1) Qual a organização, a estrutura existente no contexto?	Os ataques DDoS são originados a partir de múltiplos pontos da Internet, que podem estar presentes em diferentes domínios administrativos. Do mesmo modo, os caminhos entre os nodos origem do ataque e o nodo alvo perpassam diversos domínios administrativos, sem hierarquia administrativa entre eles.
2) Contexto apresenta arquitetura distribuída? Pode envolver mais de um domínio administrativo?	Os ataques são previamente preparados para serem disparados de modo distribuído, possivelmente originados em múltiplos domínios administrativos e perpassando múltiplos domínios administrativos até atingirem o alvo.
3) Se envolver mais de um domínio administrativo, como é a estrutura *dentro* e *entre* os domínios?	Em ataques de negação de serviço, tipicamente não existe diferenciação para o ataque se os nodos utilizados na origem do ataque e na propagação do ataque fazem parte do mesmo domínio administrativo e de domínios administrativos distintos. A presença de diferentes domínios é, assim, transparente para o ataque sendo realizado.
4) Que considerações podem ser feitas em relação à necessidade de domínios (e seus nodos) interagirem uns com os outros (e cooperarem, quando requerido)?	Como visto acima, os ataques DDoS envolvem vários domínios administrativos, porém a existência dos domínios é tipicamente transparente para o ataque sendo realizado. Os ataques utilizam a propagação de pacotes empregada normalmente na Internet, tendo sua força no volume de tráfego gerado. Não há necessidade de nenhuma forma distinta de cooperação entre domínios ou nodos para o ataque ser realizado.

5) Contexto exige requisitos especiais de rede? Redes envolvidas possuem restrições de QoS ou possuem limitações de recursos? Contexto afeta condições da rede?	▪ Como os ataques exploram a geração de um excessivo volume de tráfego, redes com recursos limitados (como largura de banda limitada, pouco poder de processamento, etc.) podem sofrer degradação do serviço da rede. Se estas redes se localizarem próximas ao nodo alvo, esta degradação tipicamente será maior, já que tais redes concentrarão maior número de pacotes do ataque originados de múltiplas máquinas origem zumbis. ▪ Alguns nodos envolvidos no ataque, especialmente os localizados próximos ao nodo alvo ou o próprio nodo alvo, possivelmente sofrerão de limitações de processamento, memória, etc., durante um ataque, já que este explora exatamente o consumo excessivo de recursos.
6) Contexto possui outras limitações, dificuldades importantes?	▪ O objetivo dos ataques DDoS envolve o consumo excessivo de recursos, de modo a torná-los indisponíveis para os usuários legítimos. Como o ataque explora simplesmente o fato do alvo estar conectado a Internet, tendo sua força no volume do tráfego do ataque, há dificuldade em distinguir os pacotes legítimos dos pacotes do ataque, o que torna a defesa contra ataques DDoS mais complexa. ▪ Os ataques são freqüentemente realizados empregando um endereço IP de origem falso no pacote a fim de dificultar a identificação das máquinas utilizadas (*IP spoofing*) (MIRKOVIC; REIHER, 2004).

Tabela 4.11: Ataques DDoS - Limitações e requisitos para o gerenciamento (Grupo 3)

Item	**Considerações**
1) Que considerações podem ser feitas sobre o tráfego para gerenciamento do contexto?	Como visto, ataques DDoS exploram o envio de um volume massivo de pacotes para um nodo alvo, e, com isto, causam volume de tráfego elevado na rede do nodo alvo e nas redes intermediárias, especialmente se estas se localizarem próximo ao nodo alvo. Deste modo, o tráfego de gerenciamento deve ser pequeno, a fim de não sobrecarregar mais as redes sob influência do ataque em curso. Além disto, durante um ataque, como tais redes estão com sobrecarga de tráfego, o tráfego de gerenciamento pode ser perdido.
2) Que outras limitações e dificuldades de gerenciamento surgem por características do contexto?	A detecção e a reação a ataques DDoS é dificultada por algumas características destes ataques, tais como: ▪ A degradação da qualidade dos serviços durante um ataque atinge não apenas o alvo, mas também os demais enlaces envolvidos ao longo do caminho entre as máquinas origem e o alvo. ▪ Os ataques são freqüentemente realizados empregando *IP spoofing*. ▪ Os ataques são baseados no envio de um volume elevado de pacotes normais, dificultando a distinção entre os pacotes legítimos e os pacotes do ataque. ▪ Como muitos ataques DDoS imitam o tráfego legítimo para evitar sua filtragem, mecanismos de detecção localizados no nodo alvo ou em sua rede não são efetivos para eliminação do ataque e somente aliviam os danos de tais ataques: a eliminação eficaz do ataque precisa ser feita de modo distribuída, em redes mais próximas às fontes de origem (MIRKOVIC; REIHER, 2004)(PENG; LECKIE; RAMAMOHANARAO, 2007). ▪ Como os mecanismos de detecção e tratamento dos ataques necessitam ser realizados ao longo das redes presentes nos caminhos

	entre os múltiplos nodos origem zumbis e o alvo, estes terão de ser realizados em uma área ampla, envolvendo redes em múltiplos domínios administrativos, a fim de cobrirem diversas escolhas de nodos origem e o nodo alvo.
3) Que requisitos específicos de gerenciamento são causados pelas características do contexto?	Mecanismos de detecção e tratamento aos ataques devem atender certos requisitos, incluindo: ▪ A fim de evitar que o consumo de largura de banda nos enlaces ao longo do caminho entre os nodos origem e o nodo alvo, prejudicando usuários legítimos que utilizam estas redes, ataques DDoS devem ser filtrados o mais próximo possível das máquinas origem. ▪ Como mecanismos de detecção e reação a ataques executados no nodo alvo ou em sua rede têm sido considerados pouco eficazes em muitos tipos de ataques, e mecanismos realizados na rede origem tem apresentado limitações (PENG; LECKIE; RAMAMOHANARAO, 2007) (MIRKOVIC; REIHER, 2004), a eliminação eficaz dos ataques tem sido buscada por alguns autores através de mecanismos de reação em redes intermediárias, que visam filtrar tráfego de ataque usando roteadores entre as fontes de ataque e o alvo (IOANNIDIS; BELLOVIN, 2002) (ZHANG; PARASHAR, 2006).

Tabela 4.12: Ataques DDoS - Análise do gerenciamento (Grupo 4)

Item	Considerações
1) Contexto exige distribuição na arquitetura de gerenciamento?	▪ Como visto acima, mecanismos de detecção e reação a ataques executados em redes intermediárias têm sido avaliados como necessários para eliminação eficaz de muitos tipos de ataques. Estes mecanismos realizam a filtragem do tráfego de ataque em roteadores das redes, sendo executados de modo distribuído e fazendo uso de um mecanismo de comunicação entre tais roteadores para mantê-los informados do ataque (PENG; LECKIE; RAMAMOHANARAO, 2007). ▪ Além de necessários para a eficácia do tratamento aos ataques, o emprego de mecanismos deste tipo auxilia a reduzir o volume de tráfego gerado nos enlaces das redes entre os nodos origem e o nodo alvo, minimizando a degradação dos serviços por usuários legítimos nestas redes.
2) Quais as possíveis arquiteturas para as soluções de gerenciamento?	Os mecanismos de detecção e reação a ataques realizados em redes intermediárias são baseados em uma arquitetura distribuída. Tal arquitetura não deve ser estruturada de modo hierárquico, uma vez que mecanismos hierárquicos não são possíveis pela presença de vários domínios administrativos nas redes intermediárias. Os mecanismos em particular analisados neste documento (IOANNIDIS; BELLOVIN, 2002) (ZHANG; PARASHAR, 2006) utilizam uma arquitetura distribuída não hierárquica que faz uso de cooperação entre os roteadores destas redes.
3) Como podem ser (ou são, se há uma ou mais soluções sendo analisadas) as	Em relação aos mecanismos analisados em particular, propostos em (IOANNIDIS; BELLOVIN, 2002) e (ZHANG; PARASHAR, 2006): ▪ Ambos os mecanismos iniciam em qualquer roteador que detecta uma assinatura de congestionamento. Este roteador filtra o tráfego correspondente a esta assinatura e informa outros roteadores,

interações de gerenciamento (solicitação, execução e controle de ações de gerenciamento)?	conforme a abordagem de cada mecanismo. No mecanismo proposto em (IOANNIDIS; BELLOVIN, 2002), informa-se os roteadores vizinhos anteriores no caminho do tráfego de modo que estes também filtrem tais pacotes e o mecanismo é empregado progressivamente para os demais roteadores vizinhos anteriores. Roteadores podem também enviar mensagens solicitando o cancelamento da filtragem. No mecanismo proposto em (ZHANG; PARASHAR, 2006), utiliza-se um protocolo para disseminação das mensagens para outros roteadores. Estes, por sua vez, utilizam a informação recebida para ajustar sua taxa de limitação do tráfego, além de retransmitirem a mensagem. ▪ Deste modo, qualquer roteador pode iniciar o processo de reação e enviar informações sobre o ataque para outros, dando origem ao processo de filtragem destes. O mecanismo de reação é executado por todos os roteadores que estiverem de acordo com este. ▪ Não há nenhuma entidade específica controlando o processo de filtragem. Cada roteador inicia e modifica a filtragem conforme os dados detectados por este e as informações recebidas dos demais roteadores.
4) Considerações sobre a necessidade de interação entre as entidades de gerenciamento, suas obrigações, confiabilidade das informações recebidas, etc.	O resultado eficaz do mecanismo exige a execução do tratamento e filtragem dos pacotes por vários roteadores, mesmo que domínios administrativos distintos. Contudo, a interação entre roteadores de diferentes domínios administrativos para a realização do mecanismo possui importantes questões relativas a segurança e políticas, uma vez que o mecanismo interfere em aspectos críticos das funções da rede (tal como a filtragem do tráfego sendo transmitido) e consome recursos dos nodos onde o mecanismo é realizado. Assim, questões importantes a serem consideradas nestes sistemas incluem como garantir que a informação recebida de outros domínios é confiável (a fim de que não seja manipulada por ataques ou utilizada de modo indevido) e como gerenciar riscos e responsabilidades por ações incorretas (por exemplo, possibilidade ou não de responsabilização se um roteador toma uma decisão incorreta e bloqueia um tráfego legítimo importante) (PENG; LECKIE; RAMAMOHANARAO, 2007). Mecanismos propostos para tratar estas questões incluem a construção de relacionamentos de confiança baseados no modelo *web-of-trust*, onde a certificação acontece entre *pares* ao invés de utilizando uma entidade certificadora central. Nesta proposta, os roteadores enviam suas mensagens assinadas digitalmente a fim de que os roteadores receptores das informações de ataque possam validar a autenticidade dos transmissores (ZHANG; PARASHAR, 2006). Além disto, mecanismos para avaliar a confiabilidade de informações originárias de outras fontes podem também ser avaliados, tal como a abordagem REFACING (OLIVIERO; PELUSO; ROMANO, 2008), que propõe um modelo para avaliar o nível de confiança dos componentes da rede envolvidos em uma detecção de ataques DDoS. Em relação à motivação para interação e cooperação, contratos podem ser estabelecidos para auxiliar este fim, a fim de fornecer estímulo para que todos os domínios envolvidos cooperem igualmente para as atividades e proporcionem benefício recíproco.

A análise realizada permite destacar que os mecanismos de detecção e reação a vários tipos de ataques DDoS possuem características particulares, exigindo que tais mecanismos sejam executados de modo distribuído em vários pontos da Internet para tratarem de modo eficaz ataques que apresentam diversas combinações de máquinas origem *zumbis* e alvo. Dois mecanismos em particular identificados na literatura foram analisados como exemplo: o proposto em (IOANNIDIS; BELLOVIN, 2002) e o proposto em (ZHANG; PARASHAR, 2006).

Um mecanismo executado de modo distribuído em vários pontos da Internet envolve a utilização de modelos que seguem paradigmas fortemente distribuídos sem subordinação entre as entidades, já que presença de vários domínios administrativos impossibilita o emprego de paradigmas com esta forma de relacionamento. De acordo com as taxonomias apresentadas na seção 3.2, em relação à taxonomia de Martin-Flatin, Znaty e Hubaux, tais condições se enquadram apenas no paradigma cooperativo fortemente distribuído. Considerando a taxonomia de Schönwälder, Quittek e Kappler, tais condições apontam para o emprego de modelos baseados no paradigma fortemente distribuído e no paradigma cooperativo, com a restrição de que tais modelos suportem que as entidades realizem suas atividades com autonomia, possuindo poder de decisão sobre as atividades requisitadas por roteadores de outros domínios.

Em relação aos dois mecanismos analisados de modo específico, ambos seguem, em relação à taxonomia de Schönwälder, Quittek e Kappler, o paradigma cooperativo, já que todos os roteadores envolvidos no mecanismo poderiam ser enquadrados no papel de gerentes de nível intermediário, sendo, portanto, o número de elementos com papel de gerente equivalente ao número de elementos do ambiente de gerenciamento. Em relação à taxonomia de Martin-Flatin, Znaty e Hubaux, o enquadramento dos mecanismos analisados na taxonomia deve ser cuidadosamente avaliado, já que a taxonomia reporta o emprego de agentes inteligentes para o paradigma cooperativo fortemente distribuído.

4.3.3 Grades Computacionais

Como apresentado na seção 4.1.3, as grades computacionais são sistemas distribuídos em rede que oferecem alta capacidade computacional fazendo uso de recursos dispersos em múltiplos domínios administrativos. A operação adequada de uma grade inclui, entre outros fatores, o gerenciamento da infra-estrutura de rede utilizada pela grade, responsável por manter a rede operando de modo correto para que os diversos recursos da grade possam ser acessados e utilizados conforme demandado. Este gerenciamento inclui atividades de monitoração e configuração de parâmetros da rede (tais como a obtenção de informações de desempenho e a configuração de reserva de largura de banda), que são utilizadas para as operações da grade como escalonamento, migração e monitoração dos *jobs*.

Como as grades estendem-se ao longo de vários domínios administrativos, o gerenciamento da infra-estrutura de rede utilizada por elas possui características particulares quando comparado ao gerenciamento de redes tradicionais. A análise destas características e das abordagens utilizadas para o gerenciamento da infra-estrutura de rede em grades é apresentada nas tabelas a seguir. Além do exame das características de gerenciamento em geral, duas abordagens apresentadas na literatura foram analisadas como exemplo: a proposta em (CAMINERO et al, 2007) e (TOMAS et al, 2009), e a proposta em (NEISSE, 2004). Assim como nos contextos de rede anteriores, esta análise é baseada na metodologia apresentada na seção 4.2. As informações para esta análise

foram obtidas no levantamento apresentado na seção 4.1.3, assim como em publicações relativas às grades computacionais, ao gerenciamento de recursos das grades e ao gerenciamento de infra-estrutura de rede requerido para operação de grades (RANJAN; HARWOOD; BUYYA, 2008-a) (RANJAN; HARWOOD; BUYYA, 2008-b) (KRAUTER; BUYYA; MAHESWARAN, 2002) (CAMINERO et al, 2007) (TOMAS et al, 2009) (NEISSE, 2004).

Na metodologia utilizada, as grades computacionais representam "situações modernas em redes tradicionais" e as abordagens para o gerenciamento da infra-estrutura de rede requerido para a operação adequada das grades representam "soluções de gerenciamento" para tais situações. Cabe destacar que, neste caso, a metodologia é empregada para analisar as características de "soluções de gerenciamento" em geral com a análise de algumas "soluções de gerenciamento" em particular, isto é, são analisadas as particularidades do gerenciamento da infra-estrutura de rede requerido para o funcionamento das grades computacionais em geral, utilizando como exemplo duas abordagens específicas identificadas na literatura (CAMINERO et al, 2007) (TOMAS et al, 2009) e (NEISSE, 2004).

As tabelas 4.13 a 4.16 discutem os itens analisados para cada grupo da metodologia. A apresentação dos dados analisados segue o mesmo formato empregado para a disposição das tabelas e dos itens das análises dos contextos anteriores.

Tabela 4.13: Grades computacionais - Definição do contexto sendo analisado (Grupo 1)

Item	**Considerações**
1) Qual o contexto sendo analisado?	Grades computacionais, objetivando-se analisar as características do gerenciamento da infra-estrutura de rede requerido para o funcionamento das grades. Deste modo: ▪ Tipo de contexto que está sendo analisado: Uma situação encontrada em redes atuais e a solução de gerenciamento empregada nesta situação. ▪ Contexto/situação: Grades computacionais ▪ Solução de gerenciamento sendo analisada: Abordagens de gerenciamento da infra-estrutura de rede utilizada por grades computacionais. Duas abordagens identificadas na literatura são analisadas como exemplo.
2) Definir porque tal contexto está sendo analisado.	As operações em grades computacionais envolvem a coordenação e o compartilhamento de recursos computacionais dispersos em diversos domínios administrativos. A execução de modo apropriado de operações da grade como escalonamento, migração e monitoração de *jobs* requer, além de outros fatores, o gerenciamento da infra-estrutura de rede utilizada pela grade, de forma a garantir que os parâmetros da rede sejam também considerados para prover os requisitos de qualidade de serviço definidos pelas aplicações da grade (NEISSE, 2004)(CAMINERO et al, 2007)(TOMAS et al, 2009). Em função das características das grades (tais como a coordenação e o compartilhamento de recursos em vários domínios administrativos e a presença de diferentes equipes de administradores para o gerenciamento da grade e da rede), o gerenciamento da infra-estrutura de rede utilizada requer abordagens de gerenciamento com características distintas das utilizadas de modo tradicional no gerenciamento de redes.

3) Contextualizar o que se objetiva analisar.	Objetiva-se avaliar as características de soluções de gerenciamento de redes para que seja oferecido suporte de rede adequado às operações de grades computacionais, tomando como exemplo duas abordagens de gerenciamento propostas na literatura em (NEISSE, 2004) e em (CAMINERO et al, 2007)(TOMAS et al, 2009). Para esta análise, as características da situação (grades computacionais) serão também discutidas.

Tabela 4.14: Grades computacionais - Características do contexto (Grupo 2)

Item	**Considerações**
1) Qual a organização, a estrutura existente no contexto?	As grades computacionais consistem em sistemas distribuídos que agregam a força computacional de recursos dispersos geograficamente. As grades podem ser implementadas de diferentes modos, abrangendo, por exemplo, sistemas que seguem o conceito de uma única organização virtual (em que todos os participantes da grade aderem às mesmas políticas e prioridades para o compartilhamento de recursos, e todos colaboram para atingir um objetivo global) e sistemas que seguem o conceito de organização federada (em que cada participante da grade possui autonomia completa para definir suas prioridades e políticas para os seus recursos) (RANJAN; HARWOOD; BUYYA, 2008-a). Em função do modo com a grade é concebida e de definições de seu projeto, diferentes arquiteturas são empregadas para suas principais atividades (KRAUTER; BUYYA; MAHESWARAN, 2002), incluindo o escalonamento dos recursos na grade, que pode ser realizado através de arquiteturas centralizada (onde um único *mediador* é responsável pela tomada de decisões do sistema completo), hierárquica (onde vários *mediadores* são organizados hierarquicamente) e descentralizada.
2) Contexto apresenta arquitetura distribuída? Pode envolver mais de um domínio administrativo?	As grades computacionais são sistemas distribuídos que tipicamente envolvem a coordenação e o compartilhamento de recursos de múltiplos domínios administrativos, dispersos geograficamente.
3) Se envolver mais de um domínio administrativo, como é a estrutura *dentro* e *entre* os domínios?	Como visto acima, as grades podem ser implementadas seguindo diferentes conceitos, que dão origem a diferentes abordagens para o compartilhamento dos recursos entre seus participantes. Por exemplo, em uma abordagem, o acesso a todos os recursos da grade pode ser feito de modo independente do domínio administrativo a que este faz parte, utilizando uma interação totalmente colaborativa entre os participantes. Em outra, o controle aos recursos compartilhados é rigidamente dependente do domínio administrativo a que o recurso faz parte. Em qualquer uma das abordagens, mecanismos para gerenciamento dos recursos (incluindo o escalonamento dos *jobs* para os recursos) podem ser realizados de diferentes modos. Por exemplo, na primeira abordagem exemplificada acima, poderiam ser utilizadas arquiteturas de escalonamento centralizadas, hierárquicas e descentralizadas entre os domínios administrativos pertencentes à grade; no segundo modo, arquiteturas centralizadas e hierárquicas não são indicadas já que cada domínio tem autonomia sobre o gerenciamento dos seus recursos.

4) Que considerações podem ser feitas em relação à necessidade de domínios (e seus nodos) interagirem uns com os outros (e cooperarem, quando requerido)?	O compartilhamento dos recursos computacionais das grades é parte dos objetivos do próprio sistema de uma grade, que visa justamente agregar a força computacional dos seus múltiplos recursos. Diferentes modos de compartilhamento dos recursos podem ser utilizados, variando conforme o conceito sobre o qual a grade está implementada (uma única organização virtual, uma organização federada, etc.). Tipicamente, acordos de cooperação são estabelecidos entre as organizações participantes da grade, que definem as políticas de compartilhamento e uso dos seus recursos de acordo com os benefícios econômicos obtidos pelas organizações participantes (NEISSE, 2004)
5) Contexto exige requisitos especiais de rede? Redes envolvidas possuem restrições de QoS ou possuem limitações de recursos? Contexto afeta condições da rede?	As grades possibilitam agregar a força computacional de recursos dispersos geograficamente, suportando a execução de diversos tipos de aplicações, incluindo computação de alto desempenho, compartilhamento de dados, colaboração interativa, simulações. Um conjunto significativo destas aplicações apresentam requisitos especiais de rede como grande largura de banda disponível, sensibilidade ao atraso (latência) e sensibilidade à variação do atraso (*jitter*) (NEISSE, 2004). As grades operam sobre a infra-estrutura de rede existente, tipicamente utilizando a Internet para a interligação entre diferentes organizações. Deste modo, os requisitos de qualidade de serviço das redes sobre as quais a grade opera afetam a qualidade do serviço das aplicações executadas sobre as grades.
6) Contexto possui outras limitações, dificuldades importantes?	▪ Como visto acima, as grades exigem requisitos especiais de rede para execução de vários tipos de aplicações. A qualidade de serviço de acesso aos recursos da grade pelos usuários e aplicações pode ser definida pela equipe administradora da grade. Contudo, as redes sob as quais as grades operam são administradas por outras equipes de administradores, e a equipe administradora da grade não possui autoridade sobre a administração das redes envolvidas. ▪ Além disto, os requisitos de QoS para a execução de uma aplicação podem exigir requisitos de QoS não apenas das redes dos domínios administrativos da grade, mas também das redes utilizadas para a interconexão destes domínios, administrada por equipes também distintas.

Tabela 4.15: Grades computacionais - Limitações e requisitos para o gerenciamento (Grupo 3)

Item	Considerações
1) Que considerações podem ser feitas sobre o tráfego para gerenciamento do contexto?	As grades operam tipicamente sobre a Internet. De modo geral, não se identificam restrições especiais relativas ao volume de tráfego empregado para o gerenciamento de redes requerido para as grades.

2) Que outras limitações e dificuldades de gerenciamento surgem por características do contexto?	O gerenciamento das redes utilizadas pelas grades é dificultado por alguns aspectos, tais como: ▪ Os requisitos de qualidade de serviço para os usuários e as aplicações das grades são controlados por uma equipe de administração da grade. Tipicamente, esta equipe não é a mesma que administra a rede sobre a qual a grade opera e não há subordinação entre as equipes. ▪ A rede, além de ser o meio para acesso aos recursos compartilhados na grade, é também utilizada por diversos outros usuários e sistemas. Deste modo, a equipe administradora da rede precisa atender os requisitos de todos os usuários, necessitando conciliar as demandas de cada um. ▪ Em aplicações que fazem uso de recursos da grade distribuídos ao longo de vários domínios administrativos, pode ser importante gerenciar requisitos de QoS que envolvam não apenas as redes que provêem o meio de cada domínio administrativo participante da grade, mas também as redes que interconectam estes domínios.
3) Que requisitos específicos de gerenciamento são causados pelas características do contexto?	O gerenciamento da infra-estrutura de redes utilizada por uma grade deve atender certos requisitos: ▪ O gerenciamento da rede deve ser responsável por manter a rede operando de modo adequado para que os diversos recursos compartilhados da grade possam ser acessados e utilizados atendendo aos requisitos de qualidade de serviço demandados pelas aplicações da grade. ▪ Atividades de monitoração e configuração de tais redes podem ser necessárias (NEISSE, 2004) (CAMINERO et al, 2007) (TOMAS et al, 2009). ▪ Em certos contextos, pode ser importante prover também o gerenciamento das redes envolvidas na interconexão entre os domínios administrativos da grade (além do gerenciamento das redes utilizadas em tais domínios).

Tabela 4.16: Grades computacionais - Análise do gerenciamento (Grupo 4)

Item	Considerações
1) Contexto exige distribuição na arquitetura de gerenciamento?	▪ Como visto acima, as grades envolvem o compartilhamento de recursos dispersos em diferentes domínios administrativos. Deste modo, as redes utilizadas pelas grades são localizadas em domínios administrativos distintos, e controladas por diferentes equipes de administradores. É necessário, assim, que seja realizado o gerenciamento de redes dispersas por vários domínios administrativos, sem hierarquia administrativa entre eles. ▪ Adicionalmente, além do gerenciamento das redes dos domínios administrativos sobre os quais a grade opera, pode também ser importante realizar o gerenciamento das redes que provêem a interconexão entre os domínios administrativos da grade.
2) Quais as possíveis arquiteturas para as soluções de gerenciamento?	O gerenciamento da infra-estrutura de rede para a utilização da grade deve ser distribuído ao longo dos vários domínios administrativos a que a grade faz parte. Em alguns contextos, pode ser importante que ele seja distribuído também ao longo das demais redes que proporcionam a interconexão de tais domínios. Com isto, a arquitetura para o gerenciamento destas redes deve ser baseada em uma estrutura distribuída

	não hierárquica. As abordagens de gerenciamento analisadas neste documento utilizam arquiteturas distribuídas. Na abordagem proposta em (NEISSE, 2004), quando um administrador da grade deseja aplicar uma política com parâmetros de QoS de rede, ele informa quais domínios administrativos devem ser configurados e o sistema interage com o mecanismo de tradução de cada domínio administrativo envolvido. Cada mecanismo de tradução irá utilizar o conjunto de regras de tradução previamente definida pelo administrador da rede daquele domínio e traduzir as políticas de grade em políticas de rede. Na abordagem proposta em (CAMINERO et al, 2007) (TOMAS et al, 2009), a entidade responsável pelo escalonamento do domínio onde a aplicação será executada interage com a entidade *Bandwidth Broker* do domínio requisitando o controle da largura de banda entre dois pontos da rede.
3) Como podem ser (ou são, se há uma ou mais soluções sendo analisadas) as interações de gerenciamento (solicitação, execução e controle de ações de gerenciamento)?	Em relação às abordagens avaliadas como exemplo, na proposta em (NEISSE, 2004): ▪ As requisições por ações de gerenciamento são feitas pelo sistema onde o administrador da grade requer a aplicação de uma política de grade que contém requisitos de QoS de rede. Este sistema será o responsável por interagir com o mecanismo de tradução de cada domínio administrativo envolvido. ▪ As atividades de gerenciamento de redes iniciam no mecanismo de tradução do domínio administrativo, que gera as políticas de rede com base na política de grade requisitada pelo sistema da grade e nas regras de tradução previamente definidas pelo administrador da rede do domínio. Tais regras são então aplicadas dentro do domínio administrativo através dos PDPs e PEPs. ▪ Não há uma entidade única controlando as ações de gerenciamento em cada domínio. O mecanismo de tradução do domínio sinaliza aos PDPs para que estes apliquem as políticas de rede geradas para o domínio. Cada PDP, por sua vez, aplica as políticas em PEPs. Em relação a abordagem proposta por (CAMINERO et al, 2007) (TOMAS et al, 2009): ▪ As requisições de ações de gerenciamento são feitas pela entidade responsável pelo escalonamento do domínio. ▪ As atividades de gerenciamento são executadas e controladas pela entidade *Bandwidth Broker* do domínio, que é responsável por obter as informações de desempenho dos roteadores daquele domínio e controlar a largura de banda efetiva entre dos pontos desta rede.
4) Considerações sobre a necessidade de interação entre as entidades de gerenciamento, suas obrigações, confiabilidade das informações recebidas, etc.	▪ As grades são tipicamente controladas por acordos de cooperação entre as organizações participantes. Embora as redes sobre as quais as grades operem sejam administradas por equipes distintas, por serem redes das mesmas organizações, o gerenciamento dos requisitos de QoS de tais redes poderiam ser, sob certos aspectos, abordados em tais acordos. ▪ Em contextos onde é necessário também o gerenciamento das redes que provêem a interconexão entre diferentes domínios administrativos das grades, outros acordos ou meios de controle teriam que ser estabelecidos.

Como visto ao longo das tabelas anteriores, o gerenciamento da infra-estrutura de rede utilizada pelas grades computacionais possui aspectos distintos, incluindo sua abrangência pelos diversos domínios administrativos que compartilham recursos em uma grade, podendo ainda demandar requisitos de QoS nas redes que provêem a interconexão de tais domínios. Tais domínios são administrados por equipes distintas, sem hierarquia administrativa entre eles. Além disto, tais redes são administradas por equipes distintas da equipe responsável pela administração da grade, também sem hierarquia entre elas.

Em função destas características, o gerenciamento de redes para suporte às grades computacionais deve ser realizado através de modelos que seguem paradigmas de gerenciamento distribuídos sem subordinação entre as entidades, uma vez que a presença de múltiplos domínios administrativos impossibilita o uso de paradigmas que empreguem subordinação de um domínio sobre outro, além de não existir tal forma de relacionamento entre o gerenciamento dos recursos da grade e o gerenciamento das redes utilizadas pelas grades.

De acordo com as taxonomias apresentadas na seção 3.2, tais condições se enquadram, pela taxonomia de Martin-Flatin, Znaty e Hubaux, apenas no paradigma cooperativo fortemente distribuído, já que este é o único que apresenta distribuição sem delegação vertical. Em relação à taxonomia de Schönwälder, Quittek e Kappler, tais condições se enquadram no paradigma fracamente distribuído, no paradigma fortemente distribuído e no paradigma cooperativo, com a restrição de que os modelos de gerenciamento empregados suportem a autonomia do domínio para a realização das atividades de gerenciamento de redes, permitindo-os controlar as ações requisitadas pela grade e pelas entidades de gerenciamento de outros domínios.

Considerando as duas abordagens de gerenciamento analisadas como exemplo, na proposta em (NEISSE, 2004), o sistema da grade computacional interage com a entidade de gerenciamento responsável pelo mecanismo de tradução em cada domínio administrativo em que os requisitos de QoS de rede precisam ser configurados. Esta entidade, por sua vez, usa regras de tradução previamente definidas pelo administrador da rede para traduzir as políticas de grade em políticas de rede e sinaliza aos PDPs que apliquem estas políticas em PEPs. Deste modo, entre a entidade responsável pelo mecanismo de tradução, os PDPs e os PEPs, identifica-se a presença de subordinação para a execução de tarefas. Já as interações entre o sistema de grade e as entidades responsáveis pelo mecanismo de tradução de cada domínio não podem ser enquadradas em situações com subordinação, uma vez que cabe à entidade responsável pelo mecanismo de tradução avaliar se cada solicitação será atendida, e como, em função das opções definidas pelo administrador da rede do domínio.

Nesta abordagem, o sistema de grade pode ser visto como uma aplicação que solicita atividades de gerenciamento de redes, do mesmo modo que outras aplicações e usuários desta rede também podem fazê-lo. Não há interação direta entre as entidades de gerenciamento de rede dos vários domínios: as demandas de gerenciamento de redes são solicitadas pelo sistema da grade computacional, onde uma entidade deste sistema interage com a entidade de gerenciamento de redes responsável pelo mecanismo de tradução de cada domínio.

Considerando a abordagem proposta em (CAMINERO et al, 2007) (TOMAS et al, 2009), as ações de gerenciamento são solicitadas pela entidade responsável pelo escalonamento dos *jobs* da grade no domínio, que interage com a entidade de

gerenciamento *Bandwidth Broker* do domínio para que esta obtenha as informações de desempenho dos roteadores e realize o controle da largura de banda efetiva entre dois pontos da rede do domínio. Detalhes sobre os mecanismos utilizados pela entidade *Bandwidth Broker* para definir como será feita a execução das ações de gerenciamento de redes não são fornecidos pelas referências.

Por fim, em grades computacionais onde os requisitos de QoS de redes sejam necessários não apenas para as redes dos domínios administrativos sobre as quais a grade opera, mas também para as redes que provêem a interconexão entre tais domínios administrativos, outras abordagens devem ser utilizadas. Nesta situação, poder-se-ia avaliar a viabilidade de um modelo de gerenciamento de redes que seguisse paradigmas cooperativos, tal como um em que a grade interagisse com o ambiente de gerenciamento de redes de um único domínio administrativo e solicitasse requisitos de QoS para o caminho completo entre dois pontos, mesmo que tal caminho envolvesse outros domínios. O ambiente de gerenciamento deste domínio, por sua vez, seria responsável por interagir com os demais domínios administrativos envolvidos no caminho repassando as solicitações recebidas do sistema da grade.

4.4 Considerações Finais

Este capítulo discutiu o gerenciamento de redes atuais com características modernas, abordando alguns contextos modernos de rede como estudos de caso e analisando paradigmas e modelos adequados para o gerenciamento destes. Inicialmente, na seção 4.1, três contextos modernos foram apresentados como estudos de caso, incluindo uma arquitetura de rede com características modernas (redes *mesh* sem fio) e duas situações com características modernas presentes em redes tradicionais (ataques de negação de serviço e grades computacionais). Com o intuito de auxiliar a análise de contextos como estes, uma metodologia foi proposta na seção 4.2. Esta metodologia, além de auxiliar a identificação dos paradigmas de gerenciamento adequados para um dado contexto, permite compreender melhor suas características, assim como as limitações e os requisitos para seu gerenciamento.

A análise de cada um dos três estudos de caso de contextos modernos utilizando a metodologia proposta foi então abordada na seção 4.3. A análise realizada demonstrou que os contextos avaliados são exemplos de redes ou situações onde o gerenciamento não pode ser realizado de modo adequado através dos paradigmas tradicionais, isto é, do paradigma centralizado e do paradigma hierárquico fracamente distribuído: tais contextos exigem o emprego de paradigmas distintos.

5 MODELO E ARQUITETURA DE GERENCIAMENTO DISTRIBUÍDO BASEADO EM P2P

Os capítulos anteriores discutiram as limitações dos paradigmas de gerenciamento centralizados e fracamente distribuídos para o gerenciamento de redes atuais, discutindo a necessidade de modelos de gerenciamento baseados nos paradigmas fortemente distribuídos. Entretanto, como abordado nestes capítulos, embora modelos de gerenciamento seguindo tais paradigmas tenham sido propostos baseados em algumas tecnologias, estes modelos foram raramente aplicados no gerenciamento de redes reais e poucos exemplos de sua utilização são encontrados atualmente. Neste contexto, destaca-se a importância de investigar modelos de gerenciamento alternativos baseados nos paradigmas fortemente distribuído para o gerenciamento de redes atuais.

Uma tecnologia que se mostra promissora para o desenvolvimento de tais modelos é a tecnologia P2P, apresentada ao longo do capítulo 2. Em virtude de suas características tais como descentralização, auto-organização, transparência, facilidades para compartilhamento de recursos e facilidades para colaboração, sistemas P2P podem ser investigados como uma tecnologia que provê suporte para a distribuição das operações de gerenciamento para os diversos nodos da rede, trazendo benefícios como escalabilidade, tolerância a falhas e colaboração entre administradores humanos. A tecnologia P2P tem sido largamente utilizada em diversas áreas de aplicação nas redes reais, de produção, o que ressalta sua relevância de ser investigada como uma tecnologia alternativa para o desenvolvimento de tais modelos de gerenciamento.

O emprego de um modelo de gerenciamento distribuído baseado na tecnologia P2P para o gerenciamento das redes atuais é investigado neste capítulo e nos capítulos a seguir. Em virtude dos diferentes usos empregados para o termo P2P, cabe destacar que o que se busca analisar neste documento é a adequação e o modo de emprego da tecnologia P2P como suporte à realização das atividades de gerenciamento de redes, empregando uma infra-estrutura P2P na base da arquitetura de gerenciamento. Busca-se assim, nesta perspectiva, **analisar a tecnologia P2P como infra-estrutura para prover suporte à realização das atividades de gerenciamento**.

Este capítulo propõe um modelo de gerenciamento distribuído baseado em P2P e uma arquitetura para um ambiente de gerenciamento que materializa tal modelo. A seção 5.1 apresenta o modelo proposto, seguido pela seção 5.2 que aborda a arquitetura do ambiente de gerenciamento proposta, apresentando suas características, sua estrutura e sua organização. A seção 5.3 discute as principais funcionalidades de gerenciamento das diversas áreas FCAPS em tal ambiente, abordando como a infra-estrutura P2P e a arquitetura fortemente distribuída suportada pelo ambiente podem ser utilizadas para aperfeiçoar as atividades de gerenciamento. Por fim, a seção 5.4 apresenta uma breve

discussão sobre os outros aspectos que poderiam ter sido enfocados em uma arquitetura para um ambiente de gerenciamento baseado no modelo proposto.

5.1 Modelo de Gerenciamento de Redes Distribuído Baseado em P2P

O modelo de gerenciamento de redes distribuído baseado em P2P agrega aos modelos de gerenciamento tradicionais as funcionalidades proporcionadas pela utilização de uma infra-estrutura formada por uma rede P2P. Este modelo visualiza uma rede P2P como uma infra-estrutura que pode ser utilizada para prover suporte para que as operações de gerenciamento sejam desempenhadas com forte distribuição. Nesta perspectiva, os serviços introduzidos pelas redes P2P provêm características inovadoras que podem ser utilizadas para aprimorar o modo como as operações de gerenciamento são desempenhadas em modelos tradicionais. Assim, características de redes P2P, tais como descentralização, auto-organização, facilidades para localização de recursos, facilidades para compartilhamento de arquivos e facilidades para colaboração podem agora ser utilizadas pelo modelo de gerenciamento distribuído, trazendo diversas potencialidades para as facilidades de gerenciamento suportadas pelo modelo.

No modelo de gerenciamento distribuído baseado em P2P, cada *peer* na rede P2P representa uma entidade de gerenciamento, responsável por realizar algumas ações. O conjunto de todos os *peers* da rede *overlay* forma o sistema de gerenciamento, que é responsável por levar e manter a rede gerenciada no estado adequado para sua operação. Os *peers* que compõem o sistema de gerenciamento podem assumir diferentes papéis, cada qual com uma função particular, representando um tipo de entidade de gerenciamento. O modelo proposto é composto por quatro tipos de entidades:

- ***Entidade para interface com o administrador da rede (IA)***: fornece aplicações e ferramentas para a interface do ambiente de gerenciamento com o administrador humano. O *peer* representado por esta entidade, reagindo a requisições de administradores humanos, se comunica com outros *peers* a fim de realizar uma tarefa de gerenciamento.
- ***Entidade para controle dos recursos gerenciados (CRG)***: responsável pela comunicação com os agentes dos recursos gerenciados, este *peer* realiza ações de gerenciamento sobre tais recursos. O *peer* representado por esta entidade recupera informações dos equipamentos gerenciados e reporta o estado destes, além de prover funcionalidades para configuração destes recursos. Este *peer* não possui contato direto com usuários humanos, interage apenas com outros *peers* da rede.
- ***Entidade para serviços de gerenciamento (SG)***: oferece funcionalidades de gerenciamento para o ambiente, tais como mapeamento entre as entidades e os recursos gerenciados, informações de topologia, etc. Este *peer* não possui contato direto com usuários humanos, interage apenas com outros *peers* da rede.
- ***Entidade de infra-estrutura de rede P2P (IP2P)***: representa os *peers* genéricos que compõem a rede P2P e oferecem funcionalidades desta rede, porém não oferecem funcionalidades de gerenciamento. Os *peers* deste tipo aprimoram a conectividade e os serviços da rede P2P, acrescentando *peers* adicionais à rede P2P além dos *peers* que provém também funcionalidades de gerenciamento. O *peer* representado por esta entidade reage a requisições

de outros *peers* na rede. Este *peer* não possui contato direto com usuários humanos, interage apenas com outros *peers* da rede.

Os *peers* representados pelas três primeiras entidades simultaneamente executam ações de gerenciamento e realizam funções de rede P2P. Os *peers* representados pela quarta entidade, por sua vez, apenas realizam funções de rede P2P, aprimorando as funcionalidades desta rede. A figura 5.1 esquematiza o modelo.

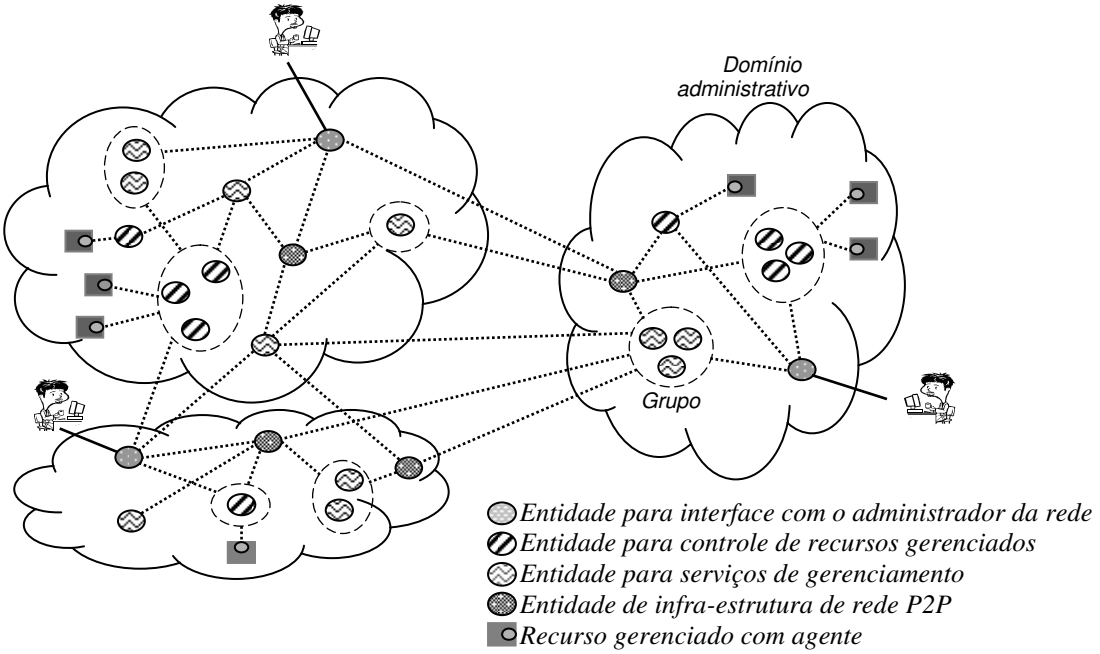


Figura 5.1: Esquema do modelo de gerenciamento distribuído baseado em P2P

No modelo, a *entidade para controle dos recursos gerenciados* pode ser vista de modo unificado com o software de gerenciamento do recurso real, dando origem a uma visão estendida das funcionalidades de gerenciamento do recurso, que passa a conter duas partes distintas: a primeira, formada pelo recurso gerenciado real, seus serviços e seu software de gerenciamento nativo; a segunda, formada pela entidade do modelo responsável pelo gerenciamento de tal recurso. Com isto, o suporte a gerenciamento nativo existente nos diversos equipamentos da rede, em geral rígido e limitado, pode ser estendido pela inclusão da entidade responsável pelo gerenciamento deste recurso. A figura 5.2 esquematiza a visão de um recurso gerenciado.

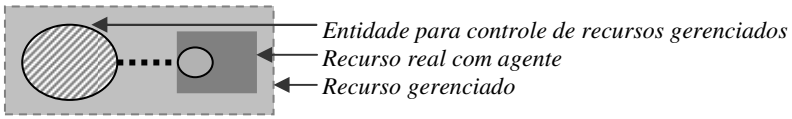


Figura 5.2: Visão de um recurso gerenciado

A abordagem discutida acima possibilita que o modelo seja empregado para o gerenciamento das redes tradicionais encontradas na maior parte das organizações nos dias de hoje, nas quais há a presença de um grande número de equipamentos heterogêneos na rede com suporte nativo ao gerenciamento rígido e limitado. Deste modo, o modelo proporciona o gerenciamento destes equipamentos com a extensão das suas funcionalidades, trazendo flexibilidade para o gerenciamento da rede.

As ações de gerenciamento podem ser executadas no modelo por um único *peer* ou por um ***grupo de peers***. Um *grupo de peers* representa um conjunto de *peers* que possuem interesses em comum, possuindo similaridades sob um ou mais aspectos e usualmente um conjunto de políticas e ou capacidades em comum. Este conceito, presente em algumas infra-estruturas e *middlewares* P2P (CHAN et al, 2007) (BROGI et al, 2008) (PALLER; KOKKINEN, 2008) (GONG, 2001) sob diferentes abordagens, é também apresentado por alguns autores através do termo *comunidade de peers* (CHAN et al, 2007) e é definido como uma forma de agrupamento baseada em interesse e similaridade (MESHKOVA et al, 2008).

Sob este contexto, um *grupo de peers* pode ser visto, no modelo, como uma entidade virtual unificada formada pelo conjunto dinâmico de *peers* membros do grupo, sendo visto, para o resto da rede, como uma entidade virtual única. Esta visão unificada permite que funcionalidades adicionais sejam oferecidas pelos grupos. A arquitetura do ambiente de gerenciamento proposta neste documento, por exemplo, suporta mecanismos de distribuição de carga e tolerância a falhas fazendo uso deste conceito, como será visto na seção 5.2.3. A figura 5.1, vista acima, esquematiza exemplos de *peers* individuais e *grupos de peers* responsáveis por ações de gerenciamento. Cabe destacar que, pelo modelo, não há restrições quanto às participações em grupo que cada *peer* possui: um *peer* pode não fazer parte de nenhum grupo, ou pode participar de vários grupos distintos. O que é definido é que cada ação de gerenciamento pode ser executada por um *peer* individual ou por um *grupo de peers*.

Além das ações de gerenciamento desempenhadas pelas três primeiras entidades (*entidades IA, CRG e SG*), todas as quatro entidades (*entidades IA, CRG, SG e IP2P*) oferecem e executam as facilidades atribuídas para *peers* da rede *overlay* que fornece a infra-estrutura do modelo. Inerentes à infra-estrutura P2P, estas facilidades variam conforme a infra-estrutura P2P empregada e incluem funcionalidades que provêem mecanismos essenciais da rede P2P e funcionalidades que provêem serviços da rede, tais como descoberta de *peers*, indexação, busca e transferência de arquivos, armazenamento, autenticação, etc. Deste modo, as facilidades proporcionadas pela infra-estrutura P2P são incorporadas ao modelo de gerenciamento, sendo integradas às atividades de gerenciamento.

A seção a seguir apresenta uma arquitetura para um ambiente de gerenciamento baseado neste modelo.

5.2 Arquitetura do Ambiente de Gerenciamento Distribuído Baseado em P2P

O modelo de gerenciamento discutido na seção anterior representa uma visão conceitual das principais entidades presentes no gerenciamento de redes baseado em P2P e como estas entidades estão organizadas. Este modelo é materializado no gerenciamento de redes real através de uma arquitetura que define um ambiente de gerenciamento. Este ambiente é projetado de modo a atender aos requisitos de gerenciamento já identificados nos modelos de gerenciamento de redes tradicionais (que se mantêm necessários neste novo modelo) e aos requisitos surgidos com os contextos modernos de rede.

Esta seção propõe a arquitetura para um ambiente com este objetivo. Inicialmente, é discutido o enfoque abordado na arquitetura proposta. Na seção seguinte, são discutidas as características da infra-estrutura P2P sobre a qual o ambiente é baseado. As seções

posteriores apresentam a estrutura da arquitetura, assim como seus serviços e aplicações.

5.2.1 Enfoque Abordado na Arquitetura

A arquitetura de um ambiente de gerenciamento distribuído baseado em P2P como o proposto pode ser analisada a partir de diferentes enfoques. Um primeiro enfoque aborda o modo como as operações de gerenciamento são realizadas no ambiente fortemente distribuído. Este enfoque considera como as funcionalidades de gerenciamento são estruturadas no ambiente distribuído baseado em P2P e como é realizada a execução de suas tarefas, considerando a infra-estrutura P2P sobre o qual o ambiente está estruturado e a utilização de forte distribuição para a execução das atividades de gerenciamento.

Um segundo enfoque avalia os mecanismos de controle requeridos no ambiente para que as atividades sejam executadas com os requisitos de segurança e controle adequados. Este enfoque considera, por exemplo, os mecanismos para controle de acesso às informações de gerenciamento, aos recursos gerenciados e às atividades de gerenciamento, assim como os mecanismos para controle das atividades de gerenciamento em ambientes com a presença de múltiplos domínios administrativos não subordinados uns aos outros. Um terceiro enfoque diz respeito aos controles de segurança requeridos no ambiente para que este se mantenha seguro a ataques externos. Relacionado ao enfoque anterior, este terceiro enfoque aborda de modo principal a segurança do ambiente em relação a sua utilização para fins não previstos, por usuários não pertencentes ao ambiente; o segundo enfoque, por sua vez, aborda o controle do ambiente para o uso por seus próprios usuários. Por fim, um quarto enfoque que pode ser empregado ao analisar a arquitetura do ambiente diz respeito à sua implantação e à sua manutenção ao longo do tempo.

A arquitetura proposta neste trabalho abordará o primeiro enfoque discutido acima — a execução de operações de modo fortemente distribuído baseada em uma rede P2P —, que será analisado ao longo deste capítulo e nos capítulos posteriores. Os demais enfoques serão discutidos apenas de modo breve neste documento, na seção 5.4.

5.2.2 Características da Infra-estrutura P2P

A arquitetura de gerenciamento de redes proposta é estruturada sobre uma infra-estrutura P2P, de modo a fazer uso das características e funcionalidades desta infra-estrutura para a realização das atividades de gerenciamento. Esta infra-estrutura P2P não precisa ser concebida para a arquitetura de gerenciamento: a arquitetura de gerenciamento visa fazer uso de uma infra-estrutura P2P já existente, sendo, contudo, necessário que esta suporte determinados mecanismos e funcionalidades para ser empregada, como será discutido a seguir.

A infra-estrutura P2P a ser empregada deve ser de propósito geral, sem ter sido concebida com enfoque em um tipo específico de aplicação (tais como compartilhamento de arquivos ou colaboração), como discutido na seção 2.2. Como discutem Chan et al, muitas aplicações P2P existentes usualmente são limitadas para propósito de compartilhamento de dados armazenados, possuindo habilidades restritas para delegar processamento para outros *peers* na rede. Esta restrição, aceitável para aplicações simples como aplicações de compartilhamento de arquivos, impossibilita fazer uso da força computacional provida pela rede P2P em toda sua extensão,

impossibilitando o desenvolvimento de aplicações complexas (CHAN et al, 2007). Deste modo, a infra-estrutura P2P a ser empregada no ambiente de gerenciamento deve ser uma infra-estrutura de propósito geral.

Diferentes abordagens têm sido empregadas para definir, agrupar e organizar os diversos mecanismos e funcionalidades requeridos em redes P2P de propósito geral (ABERER et al, 2005) (PALLER; KOKKINEN, 2008) (BROGI et al, 2008) (ARNEDO-MORENO; HERRERA-JOANCOMARTI, 2009). A arquitetura de gerenciamento proposta não é restrita a nenhuma destas organizações específicas, devendo, contudo, possuir os diversos mecanismos e funcionalidades de infra-estruturas como estas, que incluem os mecanismos essenciais requeridos tipicamente em qualquer infra-estrutura P2P e os mecanismos que provém suporte para o desenvolvimento de aplicações de propósito geral e complexas.

Entre os mecanismos essenciais requeridos tipicamente em qualquer infra-estrutura P2P, encontram-se os associados *à manutenção e à comunicação da rede overlay*, responsáveis por manter a rede *overlay* operando de modo eficiente, mesmo que na presença de alterações na topologia e falhas de nodos. Entre estes, podem ser citados: os *mecanismos para manutenção e associação de peers na rede overlay*, incluindo entrada de *peers* na rede fazendo uso de mecanismos para autenticação do *peer*, saída *amigável* de *peers* da rede (saídas informadas) e saída de *peers* da rede por falha do nodo (saídas não informadas); os *mecanismos para manutenção e auto-organização da rede overlay*, relacionados aos anteriores, incluindo os mecanismos para monitoração dos *peers* na rede e os mecanismos de manutenção do *overlay* específicos da arquitetura de rede empregada (tais como, por exemplo, o estabelecimento, a consulta e a monitoração de *super-peers*, se uma arquitetura de rede híbrida com esta técnica for empregada); e os *mecanismos para o provimento e o gerenciamento da comunicação entre os peers da rede*, incluindo o envio e o recebimento de mensagens, e o roteamento eficiente de mensagens através da rede *overlay*.

Além destes, os mecanismos essenciais requeridos tipicamente em qualquer infra-estrutura P2P incluem ainda os *mecanismos para indexação e descoberta de recursos na rede P2P* (RISSON; MOORS, 2006) (MESHKOVA et al, 2008), incluindo *peers*, arquivos, grupos, componentes de software, serviços, etc., de acordo com os recursos presentes na rede P2P. Tais mecanismos das redes P2P provêm a busca consistente e eficiente de recursos dentro da rede, suportando alterações na topologia da rede e falhas de nodos. Os mecanismos de indexação e descoberta representam importantes funcionalidades das redes P2P e estão, assim como os mecanismos de manutenção e comunicação da rede P2P, extremamente relacionados à arquitetura e à estrutura utilizadas na rede P2P.

Em adição às funcionalidades e aos mecanismos vistos acima, tipicamente presentes em qualquer aplicação ou infra-estrutura P2P, a infra-estrutura P2P empregada no ambiente de gerenciamento deve possuir facilidades de propósito geral que permitam o desenvolvimento de aplicações complexas sobre tal infra-estrutura (PALLER; KOKKINEN, 2008) (CHAN et al, 2007). Necessita, assim, possuir facilidades gerais tais como aquelas que provém suporte para compartilhamento de arquivos, armazenamento de dados, comunicação e colaboração, assim como necessita suportar facilidades para o uso de *grupos de peers* e para invocações de serviços.

O conceito de *grupos de peers*, como discutido anteriormente na seção 5.1, existe em algumas infra-estruturas e *middlewares* de abstração P2P (CHAN et al, 2007)

(BROGI et al, 2008) (PALLER; KOKKINEN, 2008) (GONG, 2001) e permite que *peers* sejam agrupados de acordo com interesses ou similaridades. Cada *grupo de peers* pode ser visto como uma sub-rede dentro da rede P2P, possuindo um conjunto dinâmico de *peers* membros e permitindo, entre outros aspectos, que os limites do grupo sejam utilizados para acordar políticas de uso e de segurança, assim como para controlar o acesso a recursos. Deste modo, em relação à infra-estrutura para o ambiente de gerenciamento, esta deve possuir mecanismos para suporte a *grupos de peers* (PALLER; KOKKINEN, 2008) (CHAN et al, 2007) (GONG, 2001), entre os quais se incluem funcionalidades e tratamentos tais como: criação de grupos, destruição de grupos, entrada de *peers* no grupo fazendo uso de mecanismos de autenticação, saída amigável de *peers* do grupo (saída informada), falha de *peers* do grupo (saída não informada), envio de mensagens para um dado membro ou para todos os membros do grupo, iteração entre os membros do grupo, etc.

O conceito de serviços e a invocação destes devem também ser suportados na infra-estrutura P2P, a fim de prover suporte para o desenvolvimento de serviços de gerenciamento, como será abordado na seção 5.2.5. Diversas infra-estruturas e *middlewares* P2P baseados em serviços para a interação entre os *peers* têm sido propostos para o desenvolvimento de aplicações complexas (CHAN et al, 2007) (PALLER; KOKKINEN, 2008) (BROGI et al, 2008) (GONG, 2001). Os serviços e suas invocações podem ser vistos, neste contexto, como um mecanismo para compartilhar a lógica e os recursos computacionais entre os nodos da rede P2P. Entre as funcionalidades requeridas na infra-estrutura para suporte aos serviços, incluem-se: publicação de serviços, descoberta de serviços na rede (associado ao mecanismo de descoberta de recursos da rede P2P) e invocação de serviços.

Por fim, a infra-estrutura P2P deve prover facilidades que permitam a associação de serviços a *grupos de peers*, de modo que o oferecimento de serviços por um *grupo de peers* já seja suportado ou possa ser implementado sobre a infra-estrutura. A associação entre grupos e serviços está presente em algumas abordagens P2P, seguindo diferentes mecanismos (BROGI et al, 2008) (GONG, 2001) (CHAN et al, 2007). Os serviços de *peer* e os serviços de grupo da arquitetura de gerenciamento baseada em P2P serão abordados nas seções posteriores.

Em relação às características requeridas da infra-estrutura P2P, esta deve, como tipicamente ocorre nas infra-estruturas P2P, ser escalável, suportar as variações na conectividade da rede, possuir capacidade de auto-organização, oferecer transparência para as aplicações, prover suporte à colaboração e ao compartilhamento dos recursos. A rede da infra-estrutura requerida na arquitetura de gerenciamento, contudo, não possui tipicamente uma abrangência extremamente ampla, como ocorre em diversas aplicações de compartilhamento de arquivos como eDonkey, Kazaa, etc. Com relação à volatilidade dos nodos da rede P2P e à dinamicidade da topologia da rede P2P, na maior parte dos contextos de rede, um grande parcela dos *peers* possuirá baixa volatilidade, em virtude de estarem presentes em nodos voltados para a operação e o gerenciamento da rede, como roteadores, servidores, etc. Contudo, certos contextos de rede podem possuir nodos muito voláteis, tais como no gerenciamento de redes *mesh* sem fio ou mesmo no gerenciamento de redes com a presença de muitos nodos móveis.

Esta seção apresentou os principais mecanismos, funcionalidades e características requeridas da infra-estrutura P2P a ser utilizada para a arquitetura de gerenciamento. As seções a seguir abordam a arquitetura do ambiente de gerenciamento propriamente dita.

5.2.3 Estrutura do Ambiente

O ambiente de gerenciamento proposto é estruturado através de serviços e aplicações, que são utilizados para a execução das funcionalidades de gerenciamento. Os serviços e aplicações são organizados em categorias de acordo com seus objetivos, compreendendo duas categorias: categoria de **serviços estruturais do ambiente P2P** e categoria de **serviços e aplicações de gerenciamento de redes.** As funcionalidades destas categorias são desenvolvidas sobre uma **camada de infra-estrutura P2P básica**.

A **camada de infra-estrutura P2P básica** contém o conjunto de mecanismos de comunicação, manutenção e organização da rede *overlay*, assim como as demais funcionalidades providas pela infra-estrutura P2P. Esta camada deve ser implementada através do uso de uma infra-estrutura P2P existente, que, como visto na seção anterior, deve oferecer ou poder ser estendida para prover os serviços de uma infra-estrutura P2P de propósito geral e que permita o desenvolvimento de aplicações complexas, incluindo, além do suporte para facilidades gerais, o suporte para o uso de *grupos de peers* e para a invocação de serviços.

Nesta camada, o substrato P2P existente empregado é estendido para que os *grupos de peers* suportem distribuição de carga e tolerância a falhas, seguindo, por exemplo, mecanismos tais como os propostos em (GRANVILLE; ROSA; PANISSON; MELCHIORS; ALMEIDA; TAROUCO, 2005) e (PANISSON, 2007). Com o suporte a distribuição de carga, as atividades de gerenciamento podem ser distribuídas de modo transparente entre os diversos *peers* do grupo, de forma balanceada, sem deixarem de ser vistas como se atribuídas para uma entidade única. A distribuição das atividades para cada *peer* pode considerar diversos fatores, tais como processamento de CPU, consumo de memória, confiabilidade do *peer*, número de *hops* entre o *peer* e o equipamento gerenciado, volume de tráfego nos enlaces entre o *peer* e o equipamento gerenciado, entre outros. Grupos podem também ser utilizados para prover maior tolerância a falhas na disponibilidade de serviços, através da implementação de mecanismos nos grupos para que, mesmo quando *peers* entrem e deixem grupos dinamicamente, ao menos um *peer* sempre seja membro do grupo. Isto pode ser provido através de um serviço do próprio grupo que monitora periodicamente os *peers* ativos naquele grupo, ativando outros *peers* se necessário, ou pode ser provido através de um serviço da rede P2P responsável pela monitoração de grupos ativos.

A **categoria dos serviços estruturais do ambiente P2P**, por sua vez, contém serviços úteis para qualquer ambiente distribuído que são proporcionados pela infra-estrutura P2P básica disponibilizada pela camada vista acima. Conforme o substrato de infra-estrutura P2P empregado, serviços desta categoria podem já ser oferecidos, parcialmente ou totalmente, pela própria infra-estrutura P2P. Em virtude disto, esta categoria pode ser integrada parcialmente com a camada de infra-estrutura P2P básica da arquitetura.

Uma das principais funcionalidades desta categoria é o mecanismo de envio de notificações, que deve ser projetado através de abordagem *publish-subscribe* baseada em P2P. O mecanismo de envio de notificações proporciona a propagação de mensagens para nodos interessados indicando eventos ocorridos na rede. Este mecanismo é utilizado por serviços relacionados às diversas atividades de gerenciamento, tais como as atividades de monitoração de redes (reportando informações críticas de recursos gerenciados), de monitoração de desempenho (indicando limiares atingidos em valores obtidos na coleta de dados de desempenho) e

de configuração (reportando novas versões de software). Outra importante funcionalidade desta categoria é o mecanismo de armazenamento.

Por fim, a **categoria de serviços e aplicações de gerenciamento de redes** compreende as facilidades utilizadas para o gerenciamento de redes propriamente dito. Esta categoria inclui (*i*) facilidades já presentes nos ambientes de gerenciamento de redes tradicionais que se mantém necessárias no novo ambiente e (*ii*) facilidades cuja disponibilidade surgiu a partir das potencialidades do ambiente distribuído baseado em P2P. Entre o primeiro grupo (*i*), mesmo que já implementadas nos ambientes de gerenciamento tradicionais, diversas funcionalidades podem ser remodeladas para obter benefícios das características e potencialidades do novo ambiente distribuído baseado em P2P, de modo a atender às necessidades de distribuição, escalabilidade, tolerância a falhas, suporte à heterogeneidade, colaboração entre múltiplos domínios administrativos e alto grau de mudanças das redes modernas. Exemplos destas incluem as funcionalidades de *polling* e coleta de dados de desempenho; o envio de eventos de recursos gerenciados e a utilização de ferramentas de registro de problemas. O segundo grupo (*ii*), por sua vez, engloba funcionalidades que se tornaram possíveis graças à utilização do ambiente distribuído baseado em P2P, atendendo demandas originadas com as necessidades apresentadas pelas novas redes modernas. Exemplos incluem ferramentas que permitam maior interação e colaboração entre administradores humanos, inclusive de domínios administrativos diferentes; ferramentas para compartilhamento e reutilização de parâmetros de gerenciamento e configuração; e mecanismos para distribuição facilitada de imagens de software para os equipamentos gerenciados.

A figura 5.3 apresenta um esquema da estrutura entre as categorias do ambiente de gerenciamento distribuído. O esquema representa a estrutura das categorias no ambiente completo, *composto pela união de todos os peers que formam o ambiente de gerenciamento*: as categorias apresentadas estão, deste modo, *distribuídas entre diversos peers*. Cada funcionalidade pode ser executada por um único serviço ou aplicação ou por um conjunto destes, como será discutido na seção 5.2.5. Por sua vez, os serviços estruturais estão distribuídos, tipicamente, sobre todos os *peers* do ambiente. Por fim, a infra-estrutura P2P básica está distribuída entre todos os *peers* que compõem o ambiente.

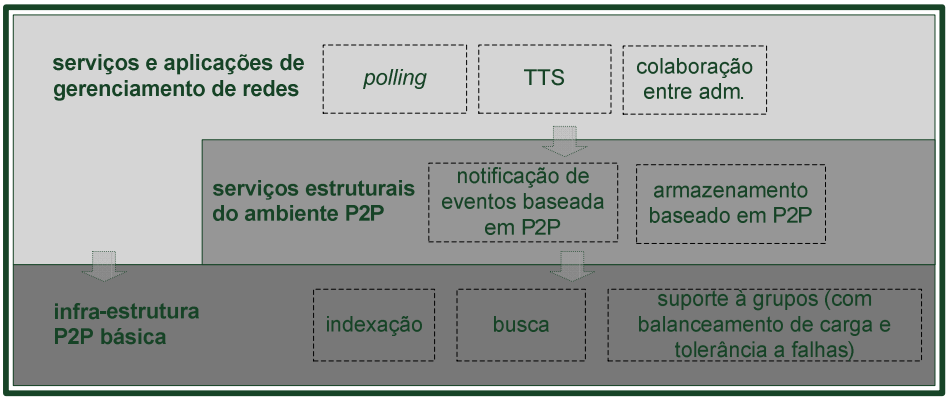
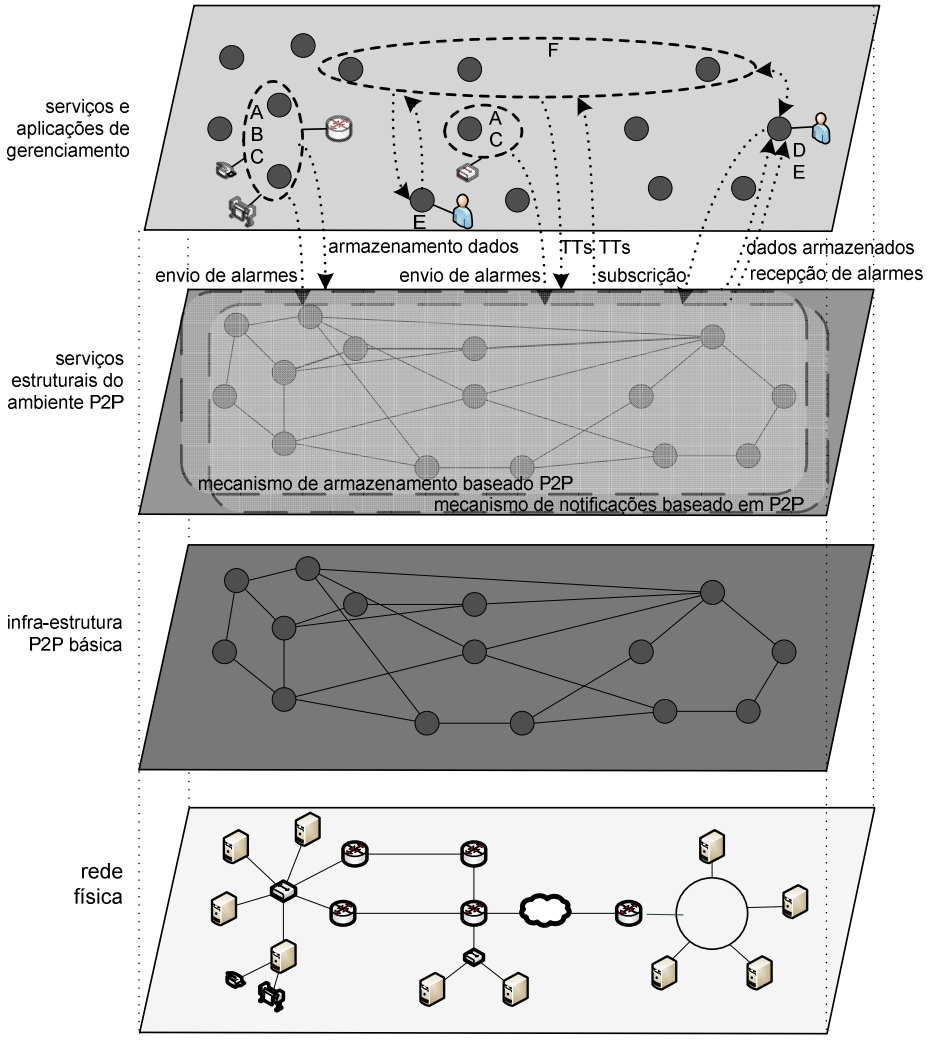


Figura 5.3: Estrutura das categorias do ambiente

5.2.4 Visão Esquemática do Ambiente

Como discutido acima, o gerenciamento da rede como um todo é realizado utilizando, de modo integrado, diversos serviços e aplicações, que interagem com outras

categorias e níveis do ambiente. Uma visão esquemática do ambiente proposto com algumas funcionalidades de gerenciamento como exemplo é apresentada na figura 5.4. Como será discutido na seção seguinte, uma funcionalidade de gerenciamento pode ser executada por um único serviço de gerenciamento ou por um conjunto de serviços. Contudo, a fim de proporcionar maior clareza na figura, as funcionalidades de gerenciamento foram representadas de modo simplificado, sem detalhar os serviços específicos utilizados para sua execução. Além disto, com o intuito de manter a clareza, as interações dos dois níveis superiores com os demais níveis, que ocorrem no ambiente, não foram detalhadas no esquema: apenas algumas interações entre os dois níveis superiores foram apresentadas como exemplo.



Legenda – Funcionalidades de Gerenciamento

A – Recepção de alarmes dos recursos gerenciados
B – Polling do estado dos recursos
C – Coleta periódica de dados de performance
D – Visualização de alarmes em tempo real
E – Ferramenta para execução de testes colaborativos
F – Registro e diagnóstico de falhas utilizando TTS e RBC

Figura 5.4: Visão do ambiente proposto

O primeiro nível do esquema, na porção inferior da figura, apresenta a visão dos recursos físicos da rede. O segundo nível ilustra uma rede P2P sobre estes recursos. Esta rede é responsável por prover a infra-estrutura P2P básica e é implementada utilizando um substrato P2P existente. O terceiro nível demonstra a categoria de serviços

estruturais do ambiente P2P. Neste nível, duas funcionalidades são representadas: o mecanismo de notificações baseado em P2P e o mecanismo de armazenamento baseado em P2P. Como apresentado na figura, os serviços estruturais são formados por um conjunto de *peers*, possivelmente o conjunto completo de *peers* do ambiente. Estes serviços são vistos, para as camadas superiores, como serviços do próprio ambiente P2P, e não como serviços providos por *peers* específicos, de modo semelhante ao que ocorre com os serviços da infra-estrutura P2P básica (*e.g.*, busca de recursos na rede P2P).

Por fim, o nível superior representa as facilidades para gerenciamento de redes, exemplificando algumas funcionalidades de gerenciamento que podem estar presentes no ambiente. Na porção esquerda superior deste nível, um *grupo de peers representando entidades para controle dos recursos gerenciados* é apresentado. Este grupo é responsável por monitorar alguns recursos de rede, provendo facilidades para recepção de eventos, *polling* do estado dos recursos e coleta de dados de desempenho. Outros *grupos de peers* são representados na porção central da figura. Entre estes, os *peers* do grupo na porção superior da figura representam *entidades para serviços de gerenciamento* responsáveis por fornecer uma funcionalidade para registro e diagnóstico de falhas. Além destes, dois *peers* representando *entidades para interface com o administrador de rede* são demonstrados. Em um destes *peers*, uma ferramenta para visualização em tempo real dos eventos ocorridos nos recursos está sendo executada, enquanto o outro *peer* acessa uma ferramenta de um *trouble ticket system* (TTS) para registro de problemas que utiliza *Case-Based Reasoning* (Raciocínio Baseado em Casos - RBC). Em adição, ambos os *peers* executam ferramentas para execução de testes colaborativos. Considerações sobre estas e outras funcionalidades de gerenciamento serão discutidas na seção 5.3.

5.2.5 Serviços e Aplicações

As atividades de gerenciamento são executadas na arquitetura do ambiente através de serviços e de aplicações de gerenciamento. As aplicações proporcionam a interação com os administradores humanos da rede; os serviços, por sua vez, não suportam esta característica.

Cada serviço é responsável por executar uma ou mais tarefas específicas. O serviço pode realizar completamente sua tarefa sem chamar outro serviço, ou pode depender de outros serviços adicionais para que a tarefa seja concluída, definindo **composições de serviços**. Deste modo, atividades de gerenciamento podem ser decompostas em serviços com funções mais específicas, criando composições de serviços que representam as atividades de gerenciamento e permitindo a reutilização de um mesmo serviço para diversas atividades de gerenciamento.

Os serviços invocados em uma composição podem fazer parte da mesma categoria de serviços ou de categorias distintas, conforme exemplificado anteriormente na figura 5.4. Deste modo, serviços responsáveis por atividades de gerenciamento podem, por exemplo, invocar outros serviços de gerenciamento, assim como podem invocar serviços estruturais do ambiente P2P (*e.g.*, serviço de armazenamento).

Os serviços invocados em uma composição podem ser desempenhados pelo próprio *peer* ou por *peers* distintos, de acordo com as limitações específicas dos serviços envolvidos. Deste modo, dois tipos de dependências entre serviços foram definidos para a arquitetura proposta: ***dependência local*** e ***dependência geral***. Uma *dependência local*

representa uma restrição de que o serviço chamado necessita ser executado no mesmo *peer* do serviço invocando-o: esta ressalva é necessária em alguns contextos em virtude de requisitos especiais de desempenho ou implementação. Uma *dependência geral*, por sua vez, representa a invocação de um serviço sem restrições. A *dependência local* está relacionada ao serviço consumidor: um serviço pode ser invocado com *dependência local* por um serviço consumidor, e invocado remotamente por outro.

Dois tipos de serviços são definidos na arquitetura: serviços de *peer* e serviços de *grupos de peers*. Os serviços de *peer* são atribuídos para um único *peer*. Os serviços de *grupos de peers*, por sua vez, são atribuídos para um *grupo de peers*, que são, em conjunto, responsáveis por executar a tarefa disponibilizada pelo serviço. Estes serviços usufruem dos benefícios proporcionados pelo suporte a *grupos de peers* discutidos anteriormente, incluindo distribuição de carga e tolerância a falhas. O modo como as tarefas são distribuídas entre os *peers* do grupo é transparente para o restante da arquitetura e para as composições em que o serviço fizer parte.

Do mesmo modo como ocorre com os serviços, as aplicações de gerenciamento podem realizar suas tarefas de modo independente, ou podem invocar um ou mais serviços para que sua funcionalidade seja concluída. Estas interações ocorrem seguindo as mesmas diretivas explicitadas acima. Uma aplicação, contudo, não pode ser invocada por outra aplicação ou serviço; ela pode apenas invocar outros serviços, agindo no papel de consumidor na interação. Algumas composições de serviços, iniciadas por aplicações e serviços, serão abordadas posteriormente no estudo de caso do capítulo 7.

5.3 Análise das Principais Funcionalidades em um Ambiente de Gerenciamento Distribuído Baseado em P2P

A partir da investigação das atividades de gerenciamento necessárias em um ambiente de gerenciamento distribuído baseado em P2P como o proposto, foi realizado um levantamento das principais funcionalidades de gerenciamento em tais ambientes, que se distribuem ao longo das diversas áreas funcionais de gerenciamento FCAPS. As principais funcionalidades identificadas em tal levantamento são listadas abaixo. Cabe destacar que tal listagem não almeja ser um arrolamento estanque das funcionalidades requeridas no ambiente. Visa, sim, auxiliar a compreensão do ambiente proposto e fornecer uma relação de funcionalidades de gerenciamento relacionadas a tal ambiente.

Categoria de Serviços Estruturais do Ambiente P2P:

- mecanismo para envio de notificações *publish-subscribe* baseado em P2P;
- mecanismo de armazenamento baseado em P2P.

Categorias de Serviços e Aplicações de Gerenciamento de Redes:

- envio e recebimento de notificações de eventos de recursos gerenciados;
- *polling* do estado dos recursos gerenciados;
- coleta periódica de dados de desempenho;
- facilidades de gerenciamento de falhas para aprimorar a interação entre administradores humanos;
- sistemas de registro de problemas distribuídos;

- facilidades para compartilhamento e reutilização de parâmetros de gerenciamento e configuração;
- distribuição de novas imagens de software para os equipamentos gerenciados.

As seções a seguir apresentam considerações sobre estas funcionalidades, discutindo suas principais características e potencialidades no ambiente distribuído baseado em P2P proposto, organizadas de acordo com a categoria a que fazem parte. É importante salientar que tais discussões não objetivam descrever a arquitetura das funcionalidades ou fornecer detalhes de projeto destas; cada funcionalidade pode ser projetada seguindo diferentes arquiteturas de execução baseadas na arquitetura do ambiente proposto. Tais discussões visam, sim, repensar estas principais funcionalidades de gerenciamento no novo ambiente, de modo a fornecer uma visão de como estas podem ser remodeladas e aprimoradas para fazer uso da infra-estrutura P2P e da estrutura fortemente distribuída do ambiente proposto. A arquitetura e o detalhamento para duas destas funcionalidades, realizadas através da atividade de *polling*, são discutidos posteriormente como estudo de caso no capítulo 7.

5.3.1 Categoria de Serviços Estruturais do Ambiente P2P

Esta categoria inclui funcionalidades úteis para qualquer ambiente distribuído, que são utilizadas por serviços e aplicações do ambiente. Duas funcionalidades podem ser listadas para esta categoria: envio de notificações e armazenamento.

5.3.1.1 Mecanismo para Envio de Notificações Publish-Subscribe baseado em P2P

Diversas atividades de gerenciamento de redes utilizam o envio de notificações de eventos para a realização de suas funcionalidades. A monitoração da rede, por exemplo, inclui a propagação de eventos (incluindo alarmes) dos recursos gerenciados para as aplicações de gerenciamento. Inicialmente, como, por exemplo, em plataformas de gerenciamento baseadas em SNMP, esta interação era feita, tipicamente, configurando o endereço IP de um ou mais gerentes nos agentes SNMP, que enviavam *Traps* SNMP diretamente para os gerentes configurados. Este mecanismo, contudo, não é adequado para as redes atuais, que exigem uma abordagem de comunicação com maior escalabilidade e que permita um menor acoplamento entre as entidades gerenciadas e as entidades com papel de gerente. Uma abordagem que se mostra adequada neste contexto e tem sido largamente utilizada para o envio de notificações em ambientes distribuídos é baseada no paradigma *publish-subscribe* (BEHNEL; FIEGE; MÜHL, 2006) (EUGSTER et al, 2003) (MAHAMBRE; KUMAR; BELLUR, 2007).

O paradigma *publish-subscribe* baseia-se em *subscribers* (assinantes) e *publishers* (publicadores). Os assinantes representam as entidades que se subscrevem para receber notificações que atendem determinados requisitos. Os publicadores, por sua vez, representam as entidades responsáveis por gerar e publicar notificações de eventos na infra-estrutura *publish-subscribe*, que é responsável por transmitir as notificações para os assinantes interessados no evento.

A implantação de um serviço de notificações baseado numa infra-estrutura *publish-subscribe* em um ambiente de gerenciamento de redes resulta em benefícios para diversas funcionalidades de gerenciamento, que podem agora fazer uso de um mecanismo escalável, eficiente e flexível para o envio de notificações de qualquer tipo.

No ambiente proposto, este serviço de notificações tem como benefício a possibilidade de integração com a rede P2P sobre a qual o ambiente de gerenciamento está estruturado. A utilização da rede P2P para a infra-estrutura *publish-subscribe* tem sido estudada em diversos sistemas (CHOI; PARK, 2005) (COURTENAGE; WILLIAMS, 2006) (GUPTA et al, 2004) (KOUBARAKIS et al, 2003), que fazem uso da rede P2P para localizar as subscrições e rotear as notificações para assinantes interessados através dos mecanismos de comunicação e busca providos pela rede. O serviço de envio de notificações, selecionado como um exemplo entre os serviços estruturais no ambiente proposto, será discutido posteriormente no capítulo 6.

5.3.1.2 Mecanismo para Armazenamento de Dados baseado em P2P

O mecanismo para armazenamento de dados no ambiente proposto provê funcionalidades para manipulação destes recursos, incluindo busca, inclusão, atualização e remoção de dados. Este mecanismo é requerido por diversas operações de gerenciamento. As funcionalidades de *polling* do estado dos recursos gerenciados e coleta periódica de dados de desempenho, por exemplo, que serão discutidas nas seções 5.3.2.2 e 5.3.2.3 e detalhadas no capítulo 7, necessitam deste mecanismo para armazenar os valores de estado e desempenho obtidos dos parâmetros gerenciados. Outros exemplos incluem as atividades de configuração dos equipamentos gerenciados, que fazem uso deste mecanismo para armazenar os parâmetros configurados, e as facilidades para gerenciamento de falhas, que requerem este mecanismo para armazenar roteiros de testes, mapas da topologia da rede, etc.

O armazenamento de dados em redes P2P faz uso das facilidades para compartilhamento de recursos destas redes, em um mecanismo no qual os dados são armazenados de modo distribuído entre os diversos *peers* da rede de modo transparente às aplicações. Contudo, importantes requisitos devem ser considerados ao avaliar o mecanismo de armazenamento a ser projetado em um ambiente P2P, incluindo, entre outros, a eficiência e a precisão para localização dos recursos armazenados, o desempenho na inclusão e na alteração dos dados, a possibilidade de distribuir os recursos armazenados de modo balanceado entre os diversos nodos e o acesso permanente aos dados (HASAN et al, 2005).

Um importante aspecto a ser considerado no armazenamento de dados em redes P2P diz respeito às variações destas redes, tal como a saída não informada de *peers* da rede, que podem tornar dados armazenados nestes nodos indisponíveis. O mecanismo de armazenamento requerido no ambiente de gerenciamento, contudo, deve ser capaz de prover alta disponibilidade dos dados sempre que requerido, já que estes podem ser indispensáveis para a realização de diversas operações de gerenciamento. A fim de lidar com este requisito, técnicas de redundância para o armazenamento em redes P2P têm sido pesquisadas. Entre os esquemas de redundância que podem ser avaliados para uso no mecanismo, incluem-se o uso da replicação simples do objeto em diferentes nodos, o armazenamento do objeto particionado em múltiplas partes com a geração de partes adicionais contendo paridade, o armazenamento de uma cópia completa do objeto combinado com o armazenamento do objeto particionado, etc (WILLIAMS et al, 2007). Em adição a tais técnicas, a fim de prover maior disponibilidade e aumentar a eficiência do mecanismo de armazenamento, a seleção dos *peers* para depósito dos dados pode considerar critérios tais como a largura de banda suportada pelo *peer*, a disponibilidade deste na rede P2P, etc.

5.3.2 Categoria de Serviços e Aplicações para Gerenciamento de Redes

A categoria de serviços e aplicações de gerenciamento de redes inclui as facilidades do ambiente que realizam o gerenciamento dos equipamentos da rede. Algumas destas facilidades já são utilizadas e necessárias em ambientes de gerenciamento tradicionais, porém sua transposição para um ambiente de gerenciamento distribuído baseado em P2P deve ser analisada com vistas a identificar o modo como cada facilidade deve ser suportada no novo ambiente, assim como as potencialidades e limitações de suas utilizações neste novo contexto. Outras facilidades são novas em ambientes de gerenciamento e são proporcionadas por características deste novo ambiente tais como o emprego de um ambiente fortemente distribuído e o suporte à colaboração e ao compartilhamento de dados provido pela infra-estrutura P2P. Nas seções a seguir, serão discutidas as principais facilidades de gerenciamento de redes no contexto do novo ambiente.

5.3.2.1 Envio de Notificações de Eventos dos Recursos Gerenciados

Diversos recursos de rede possuem capacidade de enviar mensagens assíncronas reportando eventos ocorridos no próprio equipamento. Estas mensagens são geradas pelo software de gerenciamento (agente) presente em cada equipamento e são enviadas através dos protocolos ou abordagens de gerenciamento suportadas pelo software, como, por exemplo, o envio de mensagens *Trap* em recursos gerenciados através do protocolo SNMP.

Em um ambiente de gerenciamento tradicional, há um pequeno número de entidades inteligentes envolvidas no gerenciamento e um grande número de entidades responsáveis apenas por reportar o estado de equipamentos. Nestes ambientes, os recursos gerenciados tipicamente enviam as mensagens de seus eventos diretamente para as entidades inteligentes interessadas em informações sobre a ocorrência deste evento. Esta abordagem, contudo, não é adequada para o gerenciamento das redes atuais, possuindo limitações de escalabilidade, tolerância a falhas e flexibilidade.

Em virtude disto, no ambiente de gerenciamento distribuído baseado em P2P, uma nova abordagem é empregada, fazendo uso do suporte à forte distribuição das atividades de gerenciamento e da infra-estrutura disponibilizada pela rede P2P. Nesta proposta, *grupos de peers para controle dos recursos gerenciados* são responsáveis por receber as notificações geradas pelos recursos, converter estas notificações para o modelo de informação do ambiente de gerenciamento proposto e publicar estas notificações no ambiente através do mecanismo de envio de notificações *publish-subscribe*. Os *peers* interessados no recebimento de notificações de eventos de qualquer equipamento gerenciado comunicam este interesse através de mensagens de subscrição para o mecanismo de envio de notificações, e este mecanismo transmite notificações publicadas através de sua infra-estrutura.

5.3.2.2 Polling do Estado dos Recursos Gerenciados

A funcionalidade de *polling* para a monitoração do estado de recursos na rede compreende a requisição periódica de consultas ao estado destes recursos pelas aplicações gerente. As informações coletadas permitem, por exemplo, detectar condições críticas que requerem alguma reação do ambiente de gerenciamento para que a rede gerenciada retorne a um estado estável e adequado, tal como a identificação de um módulo do equipamento com erro, uma interface em falha, etc.

Quando executada através dos modelos de gerenciamento tradicionais, a funcionalidade de *polling* para monitoração das redes atuais, compostas por grande número de recursos gerenciados, se torna um aspecto crítico, em virtude do volume de tráfego gerado e do poder de processamento requerido para a manipulação das informações serem proibitivos. Deste modo, o *polling* dos recursos tem sido evitado sempre que possível, sendo substituído por outros métodos para a obtenção das informações, tal como a instrumentalização dos recursos gerenciados para que estes enviem automaticamente notificações quando situações anômalas forem detectadas internamente.

A eliminação da funcionalidade de *polling*, contudo, não pode ser realizada em muitas situações. Isto acontece, por exemplo, quando uma aplicação de gerenciamento precisa monitorar o estado de uma variável de um equipamento que não gera eventos. Isto acontece, também, quando a notificação é enviada pelo equipamento fazendo uso de um mecanismo de transporte não confiável tal como o protocolo *User Datagram Protocol* (UDP) utilizado por mensagens *Trap* do protocolo SNMP. Como pode ser observado em investigações recentes no uso real do protocolo SNMP para o gerenciamento de redes (SCHÖNWÄLDER et al, 2007), isto ocorre freqüentemente: notificações SNMPv2 com confirmação (mensagens *Inform-Request*) são raramente encontradas no uso do protocolo SNMP em redes de produção reais. Além disto, tais pesquisas confirmaram que a monitoração das redes baseadas em *polling* respondem pela maioria do tráfego SNMP gerado. Isto indica que embora alternativas ao *polling* existam, o *polling* tradicional ainda é extensivamente utilizado.

Contudo, as arquiteturas de *polling* dos modelos de gerenciamento tradicionais não são apropriadas para serem aplicadas nas redes atuais. Em tais arquiteturas, o *polling* de todos os equipamentos é executado por uma única ou poucas entidades de gerenciamento localizadas nas estações de gerenciamento, o que causa sérios problemas de escalabilidade, já que há uma grande sobrecarga de tráfego nestas estações e nos enlaces de rede próximos a elas. Além disto, tais arquiteturas possuem problemas de tolerância a falhas, já que se a comunicação entre o recurso gerenciado e a estação de gerenciamento é perdida, a monitoração do recurso é interrompida.

No ambiente de gerenciamento distribuído baseado em P2P, uma arquitetura de *polling* distribuída pode ser empregada de modo que as tarefas envolvidas no *polling* sejam distribuídas para um grande número entidades, ao longo de toda a rede, e, com isto, as informações dos recursos gerenciados possam ser requisitadas por entidades próximas a estes (de acordo com a topologia da rede). Neste contexto, a tarefa de *polling* pode ser implementada através de um serviço provido por um *grupo de peers para controle de recursos gerenciados*. Este serviço se torna responsável por monitorar os recursos gerenciados, gerando e publicando notificações de eventos quando uma situação indesejável for identificada. Isto pode ser realizado equipando estes *peers* com módulos de software preparados para gerenciar de modo efetivo cada recurso em particular. Tais módulos não necessariamente precisam estar presentes na configuração original do *peer*: eles podem ser obtidos através de serviços de manutenção do ambiente que façam uso do suporte oferecido pela rede P2P, como será abordado na seção 5.4.3. Deste modo, ao identificar informações sobre um equipamento a ser gerenciado (*e.g.*, tipo de equipamento, versão e fabricante), o *peer* pode enviar uma mensagem indagando quais outros *peers* possuem tal módulo. Ao receber tais informações, o *peer* pode contatar um destes, fazer o *download* do módulo de software, ativá-lo localmente e iniciar o gerenciamento do recurso.

Quando comparada ao *polling* de ambientes tradicionais, a operação de *polling* no ambiente de gerenciamento proposto tem como benefício a distribuição das tarefas de gerenciamento para um grande número de nodos, reduzindo a concentração do tráfego gerado nos enlaces da rede e o poder de processamento requerido. Isto difere dos ambientes tradicionais, nos quais a tarefa de *polling* é usualmente designada para um número muito pequeno de estações. Além disto, no ambiente apresentado, diversas facilidades são providas pelo uso de grupos, como tolerância a falhas e a possibilidade de distribuir o *polling* entre todos os *peers* membros do grupo de acordo com parâmetros tais como poder de processamento e capacidade de memória de cada *peer*, confiabilidade do *peer*, número de nodos entre o *peer* e o recurso gerenciado, largura de banda nos enlaces entre o *peer* e o recurso gerenciado, entre outros. Uma arquitetura para *polling* no ambiente distribuído baseado em P2P proposto é apresentada como estudo de caso no capítulo 7.

5.3.2.3 Coleta Periódica de Dados de Desempenho

A coleta periódica de dados de desempenho dos recursos gerenciados compreende a obtenção periódica de informações de desempenho dos recursos gerenciados, com vistas à detecção de limiares de desempenho excedidos, identificação de tendências, etc. Com arquitetura tradicional para coleta de informações semelhante à arquitetura do *polling* para verificação do estado corrente, a coleta periódica de dados de desempenho é, assim como o *polling* de estado, uma das atividades que causa maior volume de tráfego nos enlaces da rede se realizada do modo tradicional, com poucas entidades com papel de gerente responsáveis pela coleta dos dados. Deste modo, abordagens alternativas para realizar esta funcionalidade necessitam ser investigadas em um ambiente de gerenciamento que vise prover escalabilidade.

Em contextos em que o recurso gerenciado possuir suporte, este pode ser configurado para fazer a coleta periódica de seus próprios dados de desempenho, armazenando-os localmente para uso posterior. Tais dados podem ser então requisitados periodicamente por uma entidade com papel de gerente, por exemplo, uma vez ao dia. Entretanto, tal facilidade não é suportada pela maior parte dos recursos gerenciados, situações em que uma abordagem distinta deve ser empregada. Em tais situações, uma abordagem semelhante à proposta para o *polling* de estado no ambiente distribuído baseado em P2P pode ser empregada. Neste contexto, *peers para controle dos recursos gerenciados* são designados pra fazer a coleta dos dados através de um serviço de grupo, sendo cada grupo responsável por um conjunto de recursos. Esta abordagem, assim como no *polling* de estado, se beneficia das características proporcionadas pelo suporte a grupos na rede P2P, que permitem desenvolver mecanismos para selecionar o *peer* do grupo que desempenhará a atividade segundo critérios de distribuição de carga, proximidade na rede entre o *peer* e o recurso gerenciado, etc., além de prover maior tolerância a falhas.

Uma arquitetura para *polling* no ambiente distribuído baseado em P2P que pode ser empregada para coleta de dados de desempenho é apresentada como estudo de caso no capítulo 7.

5.3.2.4 Facilidades de Gerenciamento de Falhas para Aprimorar a Interação entre Administradores Humanos

As atividades de gerenciamento de falhas requerem, muitas vezes, a presença de administradores humanos para serem executadas, como ocorre, por exemplo, com as

atividades para diagnóstico de falhas. Estas atividades podem ser beneficiadas com a inclusão de facilidades que possibilitem maior interação entre administradores humanos. No ambiente proposto, o suporte à cooperação, inerente ao ambiente P2P, facilita o desenvolvimento de ferramentas de gerenciamento voltadas para a colaboração entre diferentes administradores, inclusive aqueles pertencentes a domínios administrativos distintos. Um exemplo é uma ferramenta que possibilite auxiliar a execução de testes em um enlace que ultrapasse os domínios de um domínio administrativo e exija a interação dos diversos domínios envolvidos para seu diagnóstico.

Ferramentas de mensagem instantânea, voz e compartilhamento de arquivos são os exemplos mais comuns de facilidades que podem ser empregadas no ambiente proposto para prover maior interação entre administradores humanos. Além destes, outras facilidades mais específicas para gerenciamento de redes podem ser desenvolvidas, tais como ferramentas para execução e acompanhamento de testes através de vários domínios administrativos, ferramentas para construção de mapas da topologia da rede, ferramentas para monitorar a rede com visão compartilhada, etc.

5.3.2.5 Sistemas de Registros de Problemas Distribuídos

Sistemas de registros de problemas (*trouble ticket systems*) (CLEMM, 2007) são ferramentas utilizadas pelos administradores de rede para gerenciamento das falhas ocorridas nos recursos da rede, auxiliando nas tarefas de monitorar os problemas ocorridos, manter um registro de seus ciclos de vida e armazenar a memória histórica das falhas da rede. Tais sistemas são empregados tradicionalmente para o registro de problemas de um único domínio administrativo de rede, sendo utilizadas unicamente pela equipe responsável pelo seu gerenciamento. Contudo, quando transpostas para um ambiente distribuído baseado em P2P, tais sistemas podem ser aprimorados para fazer uso das facilidades para compartilhamento de dados e colaboração da infra-estrutura P2P, sendo aprimorados para realizar o compartilhamento de registros de problemas entre os diversos domínios administrativos e permitir que a memória histórica de um domínio possa ser utilizada para aumentar o conhecimento dos demais domínios da rede.

Alguns sistemas de registros de problemas foram aperfeiçoados no passado para utilizar uma técnica da Inteligência Artificial denominada *Case-Based Reasoning* (Raciocínio Baseado em Casos - RBC) (BARTSCH-SPORL; LENZ; HUBNER, 1999) (KOLODNER, 1993) (MCBURNEY; PARSONS, 2005) para diagnóstico de falhas. Estes sistemas propõem soluções para problemas correntes usando registros de problemas de situações anteriores (casos), como o sistema Dumbo (MELCHIORS; TAROUCO, 2000) (MELCHIORS, 1999). Tais sistemas, inicialmente designados para ambientes de gerenciamento tradicionais, podem agora ser aperfeiçoados com sua transposição para o novo ambiente de gerenciamento de redes distribuído baseado em P2P. O suporte a compartilhamento de arquivos da infra-estrutura P2P facilita o uso de bases distribuídas de casos, possibilitando a integração de bases de casos de diferentes domínios administrativos. Além disto, o suporte à localização de recursos proporcionado pelos mecanismos de busca da infra-estrutura P2P pode ser utilizado para a recuperação de casos similares. Isto permite que a busca seja realizada de modo paralelizado, uma vez que o cálculo da similaridade dos casos é distribuído ao longo de toda a rede, sendo realizado nos *peers* onde os casos estão armazenados, de modo similar ao proposto em (BERKOVSKY; KUFLIK; RICCI, 2005).

Além de permitir o aperfeiçoamento dos mecanismos de recuperação de sistemas de registro de problemas com RBC, o suporte à colaboração da infra-estrutura P2P pode ser também utilizado para aprimorar tais sistemas para que estes forneçam ferramentas para auxiliar os administradores de rede no diagnóstico da falha. Deste modo, fazendo uso de informações registradas nos casos recuperados, tais sistemas podem ser adaptados para disparar automaticamente a execução de ferramentas de cooperação e comunicação entre os administradores dos domínios envolvidos na falha (através dos *peers para interface com o administrador da rede*), assim como podem ser utilizados para propor (através de *peers para interface com o administrador da rede*) ou ativar automaticamente (através de *peers para controle dos recursos gerenciados*) a execução de testes integrados entre os vários domínios, entre outros.

5.3.2.6 Facilidades para Compartilhamento e Reutilização de Parâmetros de Gerenciamento e Configuração

O suporte a compartilhamento de dados oferecido pelas redes P2P pode também ser utilizado no ambiente proposto para auxiliar a configuração do ambiente de gerenciamento e dos recursos da rede, aprimorando e mesmo automatizando as tarefas de configuração para que estas façam uso de dados já presentes em outras entidades de gerenciamento do ambiente. Um exemplo é a monitoração de recursos da rede através de *peers para controle dos recursos gerenciados*: a monitoração de dois equipamentos similares é realizada, tipicamente, fazendo uso de parâmetros também similares (*e.g.*, informações sendo monitoradas, freqüência de consulta, limiares estabelecidos para geração de alarme para cada informação). Em virtude destas similaridades, um administrador de rede pode reaproveitar os parâmetros de configuração da monitoração de um equipamento para outros, utilizando-os de modo idêntico ou com apenas pequenos ajustes.

No ambiente proposto, esta característica pode ser explorada, por exemplo, para o desenvolvimento de ferramentas que auxiliem a configuração dos parâmetros de monitoração. Estas ferramentas, utilizando o suporte provido pela infra-estrutura P2P para busca e compartilhamento de dados, podem realizar a busca por contextos similares ao que está sendo configurado em outros *peers* da rede e recuperar os arquivos com os parâmetros de monitoração, apresentando-os ao administrador para confirmação. A busca pode considerar as características do equipamento, tais como o tipo de equipamento, a versão e o protocolo de gerenciamento utilizado, e as características de gerenciamento relacionadas, tais como a funcionalidade para o qual o equipamento está destinado, o domínio administrativo a que ele faz parte, a relevância do equipamento na rede, etc. A ferramenta pode ainda possuir mecanismos para implantar estes parâmetros automaticamente, conforme políticas estabelecidas pelo administrador.

De modo similar, ferramentas para configuração dos recursos gerenciados podem também fazer uso de parâmetros de configuração empregados para outros recursos similares. Assim, ferramentas para compartilhar tais parâmetros podem ser disponibilizadas aos administradores, de modo que as informações relativas à configuração de recursos presentes nas diversas *entidades para controle dos recursos gerenciados*, mesmo que de domínios administrativos distintos, possam ser reutilizadas nas demais entidades. Assim como na monitoração, a busca pelos parâmetros empregados para configurar recursos similares pode considerar as características dos recursos, tais como o tipo do equipamento, a versão, os serviços de rede oferecidos pelo

recurso, e o protocolo de gerenciamento utilizado. Por fim, além destas informações, exemplos adicionais de dados que podem ser compartilhados e reutilizados no ambiente proposto incluem as subscrições para recebimento de eventos e os parâmetros para a configuração de coleta de dados de desempenho.

Técnicas de Inteligência Artificial como RBC podem também ser empregadas para aprimorar o processo de identificação de contextos similares. Com esta abordagem, os arquivos com os parâmetros de configuração e as subscrições passam a ser vistos como casos, e cada *peer* que contém estes arquivos é visto como uma base de casos. O processo de recuperação RBC utiliza as bases de casos distribuídas nos vários *peers* para seu mecanismo de busca e casamento, proporcionando a utilização de técnicas elaboradas para identificar dados similares nos demais *peers* da rede.

As ferramentas para compartilhamento e reaproveitamento de informações podem ainda ser combinadas com ferramentas para colaboração entre administradores humanos de vários domínios, fazendo uso do suporte à colaboração proporcionado pela infra-estrutura P2P do ambiente. Esta integração é útil, por exemplo, em uma situação em que é necessário configurar equipamentos em mais de um domínio administrativo, como na configuração de um enlace que ultrapassa diversos domínios. Deste modo, estas ferramentas podem prover a cooperação entre domínios e, simultaneamente, compartilhar informações de configuração entre eles, oferecendo possibilidade de aplicar tais configurações de modo semi-automático. Tais ferramentas se tornam ainda mais relevantes nas redes atuais pela existência de funcionalidades que precisam ser configuradas em diversos domínios administrativos, tal como a configuração de uma reserva de banda ou a configuração dos requisitos de QoS da rede para as demandas de grades computacionais.

5.3.2.7 Distribuição de Novas Imagens de Software para os Equipamentos Gerenciados

Uma das atividades que fazem parte da área de gerenciamento de configuração é a manutenção das imagens de software instaladas nos equipamentos gerenciados. No ambiente de gerenciamento proposto, esta tarefa, tradicionalmente trabalhosa, pode ser facilitada com a inclusão de mecanismos que fazem uso do ambiente distribuído e do suporte ao compartilhamento de arquivos e à busca de recursos da infra-estrutura P2P.

Assim, quando um administrador humano recebe de um fabricante uma nova versão de software para um determinando tipo de equipamento, ele informa na ferramenta correspondente (localizada em um *peer para interface com o administrador da rede*) quais são as características da nova imagem, tais como o tipo de equipamento, a versão da imagem, a exigência de atualização (crítica, recomendada, opcional) e os efeitos de sua instalação (não interrupção dos serviços do equipamento, interrupção temporária sem reinicialização do equipamento, reinicialização do equipamento). Duas abordagens podem então ser empregadas para atualizar a imagem nos equipamentos.

Na primeira abordagem, o *peer para interface com o administrador na rede* realiza a busca na rede indagando quais equipamentos gerenciados são do tipo indicado e quais *peers para controle dos recursos gerenciados* são responsáveis por estes equipamentos. A partir dos equipamentos retornados, a ferramenta pode, se desejado, aplicar filtros introduzidos a partir de políticas pré-configuradas para identificar quais equipamentos podem ou não ser atualizados (utilizando, por exemplo, informações de que equipamentos podem sofrer interrupção no momento). Em seguida, a lista dos equipamentos é apresentada ao administrador da rede, que faz alterações se necessário.

Após a confirmação do administrador, a ferramenta envia a nova imagem de software aos *peers para controle dos recursos gerenciados* correspondentes. A instalação da nova imagem pode ser feita imediatamente pelas entidades utilizando o protocolo de gerenciamento ou o mecanismo disponibilizado pelo equipamento, ou pode ser agendada para momento posterior, se assim estiver sido selecionado pelo administrador.

Esta primeira abordagem concentra grande controle na ferramenta no *peer para interface com o administrador da rede*, permitindo a intervenção humana em diversas etapas. Exige, também, que os *peers para controle dos recursos gerenciados* sejam equipados com um módulo de software que realize a atualização da imagem, porém este componente possui função simplificada, sendo responsável apenas pela instalação da imagem propriamente dita.

Na segunda abordagem para a atualização de imagem, mais controle é transferido para os *peers para controle dos recursos gerenciados*, que são equipados com um módulo de gerenciamento mais elaborado. Após o administrador humano informar as características da nova imagem, a ferramenta no *peer para interface com o administrador da rede* divulga no ambiente de gerenciamento a disponibilidade de uma nova imagem. Esta divulgação pode ser feita através de um serviço de notificação: segundo esta abordagem, quando os *peers para controle dos recursos gerenciados* iniciam o gerenciamento de um dado equipamento, estes se subscrevem para receber eventos acerca deste tipo de equipamento. Quando uma versão é disponibilizada pelo administrador humano, a ferramenta envia um evento indicando a presença de uma nova imagem de software para o serviço de envio de notificações, que transmite o evento para os *peers* assinantes. Quando estes *peers* recebem a notificação, consultam políticas pré-configuradas e decidem se devem fazer a atualização. Se sim, fazem o *download* da nova imagem do *peer para interface com o administrador da rede* e a instalam no equipamento.

5.3.2.8 Outras Funcionalidades de Gerenciamento de Redes

Em virtude de sua forte distribuição e da infra-estrutura P2P, o ambiente proposto provê ainda benefícios para diversas outras funcionalidades de gerenciamento de redes. O gerenciamento de configuração, por exemplo, inclui em suas funcionalidades a manutenção do registro dos equipamentos e serviços que estão instalados na rede, assim como a configuração destes. No ambiente proposto, a existência dos *peers para controle dos recursos gerenciados* e o suporte da infra-estrutura P2P facilita esta atividade (como será discutido em 5.4.3), já que estes podem ser mais facilmente equipados com módulos de software específicos para o gerenciamento de cada equipamento, que permitem auditar a configuração dos equipamentos e identificar quando alterações forem realizadas. Tais informações, por sua vez, podem ser mantidas através do serviço de armazenamento do ambiente e serem consultadas pelas diversas aplicações e serviços interessados.

As tarefas do gerenciamento de segurança da rede podem também ser aprimoradas quando transpostas para o ambiente proposto. Mecanismos para detecção a ataques DDoS podem ser aperfeiçoados para fazerem uso do suporte oferecido pela infra-estrutura P2P para a realização de suas operações, tal como o proposto em (ZHANG; PARASHAR, 2006), discutido anteriormente nas seções 4.1.2 e 4.3.2. Além destes, ferramentas para segurança da rede podem ser adaptadas para fazer uso do suporte a compartilhamento de conteúdo e a colaboração proporcionado pela infra-estrutura P2P, possibilitando o compartilhamento de informações de segurança entre os diversos

domínios administrativos gerenciados pelo ambiente. Por exemplo, ferramentas que utilizam RBC para detecção de tentativas de intrusão, como a proposta em (LOCATELLI et al, 2004) podem ser adaptadas para recuperar casos similares armazenados em bases de casos de ferramentas localizadas em outros nodos da rede, inclusive em domínios administrativos distintos. De modo similar, listas de nodos suspeitos detectados pelas ferramentas de segurança podem ser compartilhadas entre as ferramentas dos demais domínios, permitindo ainda que estas sejam comparadas e contribuam para melhorar o mecanismo de detecção, tal como, por exemplo, aumentando a valoração de um nodo considerado suspeito em mais de uma lista.

5.4 Arquiteturas para o Modelo Proposto com Outros Enfoques

A arquitetura proposta neste documento enfoca o modo como as operações de gerenciamento são realizadas no ambiente. Este enfoque analisa como as diversas funcionalidades de gerenciamento são estruturadas e executadas num ambiente com forte distribuição das atividades de gerenciamento, considerando a infra-estrutura P2P sobre a qual o ambiente está estruturado. A análise da arquitetura sob esta perspectiva discute as potencialidades e limitações do uso da infra-estrutura P2P, assim como do emprego de forte distribuição na execução das atividades.

Outras facetas, contudo, podem ser enfocadas ao investigar uma arquitetura para um ambiente que materialize o modelo de gerenciamento distribuído baseado em P2P proposto. Neste contexto, como apresentado anteriormente, três outros enfoques principais podem ser abordados para a arquitetura. Estes enfoques não são isolados uns dos outros: diversos objetivos são abordados em simultâneo por mais de um enfoque, assim como diversos aspectos de dois ou mais enfoques estão relacionados.

As seções a seguir discutem brevemente as principais características de arquiteturas que abordem estes enfoques. Com objetivo de simplificar a terminologia no restante deste documento, o enfoque abordado neste documento será referido, quando necessário, como *enfoque na execução fortemente distribuída baseada em P2P*.

5.4.1 Arquitetura com Enfoque nos Mecanismos para Controle, Coordenação e Segurança

Um segundo enfoque para a investigação e a definição da arquitetura de um ambiente de gerenciamento baseado no modelo proposto aborda os mecanismos requeridos no ambiente para que as atividades de gerenciamento sejam desempenhadas de acordo com os requisitos de controle, coordenação e segurança adequados, considerando seu uso normal, por usuários autorizados. Este enfoque analisa os procedimentos requeridos para que as atividades de gerenciamento sejam realizadas de modo controlado em ambientes com múltiplos administradores de rede, inclusive para operações que envolvam múltiplos domínios administrativos não subordinados uns aos outros. Analisa, também, dentro deste contexto, quais os controles necessários para que as informações e as atividades de gerenciamento sejam acessadas por usuários com nível de acesso adequado.

Uma arquitetura sob este enfoque para um ambiente baseado no modelo proposto deve considerar vários aspectos. Um destes é a segurança do gerenciamento (CLEMM, 2007), disciplina que envolve garantir que as operações de gerenciamento são seguras. Deste modo, a arquitetura deve prover facilidades para garantir que o acesso às aplicações de gerenciamento, às informações de gerenciamento e às interfaces de

gerenciamento dos recursos seja realizado apenas por entidades com os direitos de acesso apropriados. Em um ambiente baseado em uma infra-estrutura P2P como no modelo proposto, é necessário um mecanismo de autorização que ofereça facilidades que permitam atribuir níveis de acesso diferenciados aos recursos gerenciados e às diversas funcionalidades do ambiente de gerenciamento, de acordo com os *peer* envolvidos, o usuário realizando operações de gerenciamento através destes, a equipe a que o usuário faz parte e o domínio administrativo a que pertencem. Deste modo, este mecanismo deve considerar diferentes dimensões ao definir os níveis de acesso, considerando tanto os *peers* envolvidos, como o usuário, a equipe e o domínio a que faz parte, em relação às permissões de acesso aos recursos gerenciados (*e.g.*, equipamentos de rede), às informações de gerenciamento (*e.g.*, dados de estado e desempenho coletados dos recursos gerenciados, dados acerca da configuração dos recursos armazenados no ambiente de gerenciamento, dados informativos sobre os recursos) e à execução de atividades de gerenciamento (*e.g.*, subscrever-se para receber eventos de recursos, solicitar coleta de dados de desempenho, configurar equipamento da rede).

Esta arquitetura precisa também considerar aspectos para controlar e coordenar as operações de gerenciamento ao longo das entidades de gerenciamento envolvidas, especialmente nas situações que envolvem entidades presentes em diferentes domínios administrativos. Estes controles estão relacionados aos mecanismos de segurança descritos acima, já que, por exemplo, a solicitação de uma atividade de gerenciamento que envolva diversos domínios exige um nível de acesso para a execução de uma ou mais operações em múltiplos domínios, assim como exige acesso às informações de gerenciamento necessárias para a execução destas operações. Tais aspectos envolvem ainda os mecanismos para controle da cooperação entre os múltiplos domínios, que podem ser investigados a partir de diferentes abordagens.

Uma abordagem que pode ser investigada é o emprego de políticas para definir o grau e as características de cooperação de cada domínio administrativo. Neste contexto, cada domínio administrativo definiria políticas que determinassem fatores tais como: prioridade para a execução de operações de gerenciamento solicitadas por outros domínios; volume de operações solicitadas por outros domínios que será aceito (que pode ser definido por número de operações, por grau de processamento requerido para a operação, por "peso" atribuído para a execução de cada operação, etc.); volume de recursos do domínio que pode ser destinado para a execução destas operações; entre outros. Estas políticas poderiam incluir regras relacionadas ao nível de acesso do usuário requisitando a operação ou responsável pelo serviço que faz a requisição, assim como dos recursos e das informações de gerenciamento envolvidos na operação solicitada. Poderiam, ainda, ser relacionadas a todos os domínios administrativos externos ou a domínios específicos, permitindo definir diferentes graus de cooperação para cada domínio de acordo com parcerias estabelecidas, organização a que o domínio faz parte, etc. Tais políticas seriam atribuídas dentro de cada domínio administrativo, para definir as regras dentro do domínio, existindo um grupo de políticas para cada domínio. Além disto, abordagens da área de Inteligência Artificial podem também ser investigadas para prover mecanismos para cooperação das entidades pertencentes aos vários domínios. Estas abordagens podem investigar, por exemplo, o emprego de modelos baseados em agentes para proporcionar a cooperação entre as entidades.

Considerando a arquitetura proposta neste documento, que tem enfoque na execução de atividades de gerenciamento de forma fortemente distribuída e baseada em P2P, os mecanismos para controle e segurança discutidos nesta seção poderiam ser investigados

numa dimensão adicional às categorias e camadas definidas anteriormente na figura 5.3, sendo relacionados a estas. Estes mecanismos podem incluir, por exemplo, serviços para autenticação e controle de acesso, relacionados à categoria dos serviços estruturais do ambiente. Por sua vez, os mecanismos para controle da cooperação entre as entidades e seus múltiplos domínios podem estar relacionados às diversas categorias e à camada P2P definidas anteriormente, uma vez que serviços e aplicações destas poderiam requerer tais mecanismos de controle. Estes mecanismos poderiam ser investigados, assim, de modo integrado às categorias do ambiente e à camada P2P, provendo serviços independentes e funcionalidades integradas aos serviços de gerenciamento, aos serviços estruturais e aos serviços da camada P2P. A figura 5.5 apresenta uma extensão da figura 5.3 (apresentada na seção 5.2.3) sob este contexto. Diferente da figura da seção 5.2.3, a figura abaixo não pretende definir a estrutura da arquitetura segundo os mecanismos discutidos nesta seção: ela visa, apenas, apresentar uma estrutura que possa ser utilizada como alternativa e perspectiva inicial para investigações adicionais de uma arquitetura que siga este segundo enfoque.

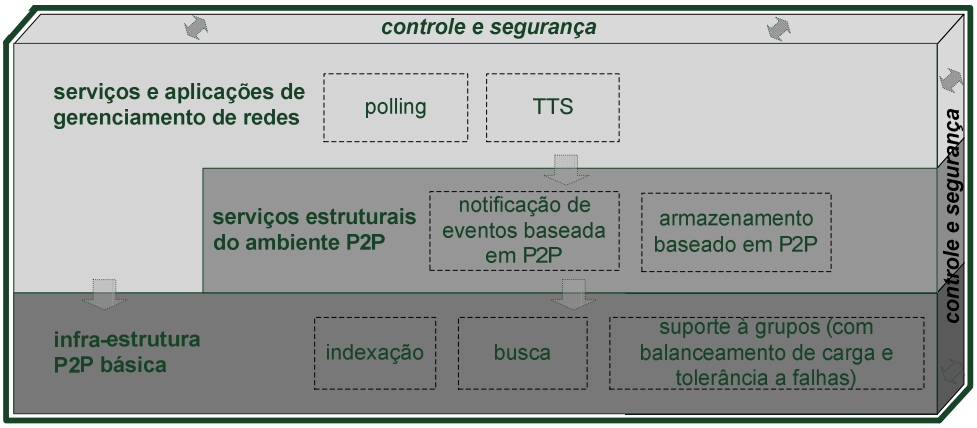


Figura 5.5: Estrutura com mecanismos de controle e segurança

5.4.2 Arquitetura com Enfoque na Segurança Contra Elementos Externos

Um terceiro enfoque ao definir a arquitetura para um ambiente que materialize o modelo de gerenciamento distribuído baseado em P2P proposto diz respeito aos controles de segurança requeridos para o ambiente para que este se mantenha seguro a ataques externos. Relacionado ao enfoque discutido na seção anterior, e com alguns requisitos simultâneos, este enfoque objetiva a segurança do ambiente em relação à sua utilização para fins não usuais e não previstos, que não são realizados por usuários do sistema. O enfoque anterior, por sua vez, tem como finalidade os controles do ambiente para uso por seus próprios usuários.

Assim como na arquitetura discutida na seção acima, a arquitetura para um ambiente sob este enfoque considera a segurança do gerenciamento, disciplina que visa garantir que as operações de gerenciamento são seguras. Neste enfoque, contudo, a arquitetura deve suportar funcionalidades que permitam evitar a interrupção das atividades de gerenciamento; evitar ataques externos; manter trilhas de auditoria de segurança que registrem as operações de gerenciamento realizadas, entre outros.

A utilização de uma infra-estrutura P2P no ambiente como o proposto traz diversas dificuldades para a segurança do gerenciamento. Redes P2P são suscetíveis a brechas de segurança de *peers* maliciosos (GASPARY et al, 2007) (LUA et al, 2005) (DEPAOLI;

MARIANI, 2004), que podem agir como clientes ou servidores na rede e podem causar diversos tipos de ataque na rede, tais como: ataques de negação de serviço (DASWANI; GARCIA-MOLINA; YANG, 2003); ataques de roteamento, como o ataque Eclipse (SINGH et al, 2004) em que um conjunto de *peers* maliciosos esconde nodos corretos vizinhos através do descarte ou re-roteamento de mensagens destinadas a estes; ataques que forjam múltiplas identidades, como o ataque Sybil (DOUCEUR, 2002). Deste modo, como o ambiente de gerenciamento controla todos os equipamentos e serviços gerenciados da rede, o uso de uma infra-estrutura P2P para este ambiente precisa considerar os diversos requisitos de segurança. No ambiente proposto, estes requisitos se tornam ainda mais relevantes pela presença de múltiplos domínios administrativos no ambiente, já que a inclusão destes torna mais difícil garantir a presença de apenas nodos confiáveis (AHMED et al, 2007).

Importantes requisitos de segurança podem incluir ainda mecanismos para autenticação entre *peers* e mecanismos de integridade para garantir que mensagens entre os *peers* não sejam alteradas, tal como proposto em (CHIRITA et al, 2004). Em menor freqüência, em redes nas quais as mensagens de gerenciamento contêm informações consideradas sensíveis à corporação (*e.g.*, número de falhas em determinados equipamentos e serviços), mecanismos de confidencialidade também são indicados, impedindo que mensagens capturadas por nodos maliciosos possam ser decifradas.

Considerando a arquitetura proposta neste documento, introduzida ao longo da seção 5.2, os mecanismos para segurança do ambiente poderiam ser investigados, assim como na arquitetura discutida na seção anterior, numa dimensão adicional às categorias e camadas definidas anteriormente na figura 5.3. Neste contexto, mecanismos para a segurança do ambiente poderiam ser investigados de modo integrado às categorias e, principalmente, à camada P2P, garantindo a segurança do ambiente a partir dos serviços de gerenciamento, serviços estruturais e serviços da rede P2P.

5.4.3 Arquitetura com Enfoque na Implantação e Manutenção do Ambiente

Um quarto enfoque que pode ser abordado ao definir uma arquitetura para um ambiente baseado no modelo de gerenciamento proposto diz respeito à implantação e à manutenção do ambiente de gerenciamento ao longo do tempo. Uma arquitetura definida sob este enfoque analisa os mecanismos para a implantação inicial do ambiente de gerenciamento, a implantação de um novo domínio administrativo em um ambiente já existente, a inclusão de novos recursos gerenciados no ambiente existente, a atualização do ambiente de gerenciamento, etc.

A implantação e a manutenção de um ambiente baseado no modelo proposto se beneficiam pelas potencialidades oferecidas pela infra-estrutura P2P, incluindo seus serviços para localização e compartilhamento. Tal infra-estrutura proporciona, deste modo, o desenvolvimento de facilidades que podem ser destinadas, por exemplo, para a instalação e a manutenção de componentes de software do ambiente de gerenciamento.

Uma funcionalidade para *auto-instalação sob-demanda de novos componentes de software em entidades de gerenciamento* é um exemplo. Ao longo do tempo, novos recursos, incluindo equipamentos e serviços, são instalados na rede. Isto se torna ainda mais acentuado nas redes atuais, já que novas demandas são continuamente apresentadas pelos usuários e há grande heterogeneidade de tecnologias. Em virtude disto, as diversas entidades envolvidas no gerenciamento necessitam ser atualizadas com freqüência para que um gerenciamento efetivo possa ser oferecido.

Em um ambiente baseado no modelo proposto, esta atualização é facilitada pelas funcionalidades de localização de recursos e pelo suporte ao compartilhamento de arquivos da infra-estrutura P2P. Assim, uma funcionalidade pode ser projetada para que, quando um *peer* deseje oferecer um serviço para o qual não possui o componente de software instalado, ele procure na rede quais *peers* possuem tal componente, escolha um e faça seu *download* automaticamente, sem necessitar da interação do administrador humano. Tal funcionalidade pode ser utilizada, por exemplo, quando um *peer para controle dos recursos gerenciados* descobre um novo equipamento para o qual não possui os componentes de software necessários para gerenciamento, ou quando o administrador humano designa que uma determinada funcionalidade deve ser executada por um dado *peer* que ainda não está equipado para esta funcionalidade.

Outra funcionalidade que pode ser desenvolvida permite uma *atualização facilitada de versões de componentes de software em entidades de gerenciamento*, permitindo trazer maior simplicidade para a evolução do ambiente de gerenciamento na medida em que novas funcionalidades de gerenciamento forem desenvolvidas ou que o suporte para novos equipamentos ou novas versões destes seja requerido. Esta atualização, usualmente trabalhosa em um ambiente tradicional, pode ser facilitada no ambiente pela inclusão de facilidades que utilizem o suporte à localização de recursos e ao compartilhamento de arquivos da infra-estrutura P2P, de modo similar ao discutido acima. Esta funcionalidade pode ser projetada, por exemplo, para fazer uso de uma aplicação no *peer para interface com o administrador humano*, onde o administrador da rede pode indicar a disponibilidade de uma nova versão de componente de software. A aplicação pode utilizar os mecanismos de busca de recursos da infra-estrutura P2P para identificar os *peers* que possuem tal componente de software instalado e os notificar sobre a disponibilidade de uma nova versão. Os *peers* interessados podem então fazer o download da nova versão e a instalar automaticamente.

Uma arquitetura sob este quarto enfoque aborda, ainda, a implantação inicial do ambiente. Neste contexto, a arquitetura investiga, entre outros, meios para simplificar a implantação inicial dos *peers* no ambiente, a definição dos *grupos de peers* do ambiente (*e.g.*, *grupos de peers para controle dos recursos gerenciados*), a definição dos recursos gerenciados por cada grupo e o posicionamento dos *peers* nos grupos existentes. Estas definições devem considerar, inclusive, a proximidade entre os *peers* responsáveis pela execução das tarefas de gerenciamento e os recursos gerenciados, de modo a diminuir o tráfego nos enlaces da rede, assim como outros fatores que podem ser utilizados para cálculo da distribuição de tarefas entre os *peers* membros de um *grupo de peers*.

Considerando a arquitetura proposta neste documento, introduzida ao longo da seção 5.2, as funcionalidades para implantação e manutenção do ambiente poderiam ser investigadas como uma categoria adicional do ambiente de gerenciamento. Esta categoria conteria os serviços e as aplicações relacionados às estas facilidades, incluindo aquelas facilidades proporcionadas pelo ambiente distribuído baseado em P2P proposto. A figura 5.6 esquematiza uma estrutura inicial alternativa de uma arquitetura que integrasse os quatro enfoques discutidos.

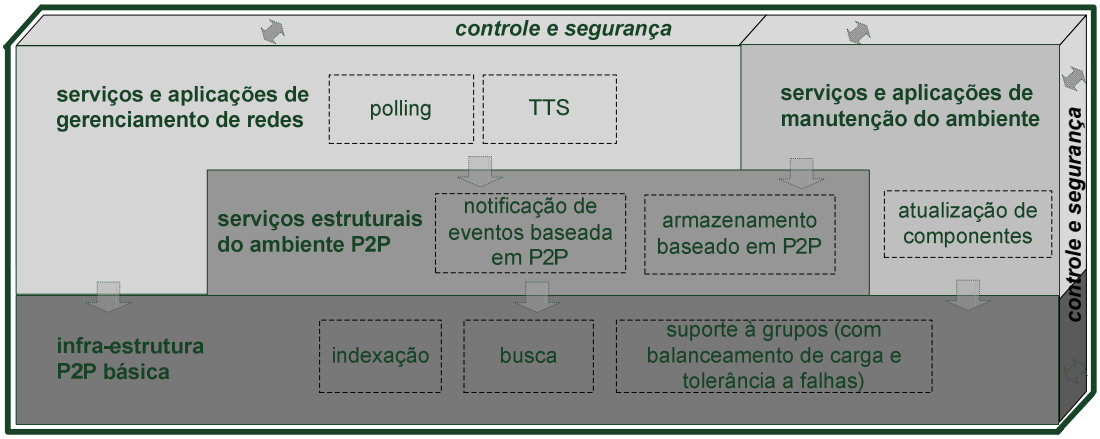


Figura 5.6: Estrutura com os diversos mecanismos integrados

5.5 Considerações Finais

Este capítulo abordou o modelo e a arquitetura de gerenciamento baseado em P2P. A seção inicial propôs o modelo de gerenciamento, incluindo sua concepção e entidades. A seção a seguir propôs a arquitetura de um ambiente de gerenciamento que materializa este modelo no gerenciamento de redes reais. Nesta seção, foram apresentados e discutidos o enfoque seguido pela arquitetura, as características da infra-estrutura de rede P2P empregada, a estrutura do ambiente de gerenciamento e a sua organização em serviços e aplicações. A seção 5.3 abordou as principais funcionalidades estruturais e de gerenciamento em tal ambiente, discutindo como estas funcionalidades podem ser remodeladas e aprimoradas no novo ambiente em virtude deste estar concebido sobre uma infra-estrutura P2P e proporcionar forte distribuição das atividades de gerenciamento. Por fim, a seção 5.4 analisou outros aspectos que poderiam ter sido enfocados na arquitetura, apresentando uma breve discussão sobre estes aspectos e como estes poderiam ser investigados em trabalhos adicionais.

O modelo e a arquitetura propostos são concebidos para o gerenciamento das redes atuais num contexto amplo, incluindo os **contextos modernos de rede** que possuem requisitos de gerenciamento não atendidos de modo apropriados em modelos de gerenciamento tradicionais, assim como as **redes atuais tradicionais** cujo gerenciamento por modelos baseados nos paradigmas tradicionais possui limitações de escalabilidade, tolerância a falhas e flexibilidade, entre outras. Tal modelo e arquitetura visam, inclusive, possibilitar o gerenciamento das redes atuais existentes em diversas organizações em que há a **presença de um enorme número de equipamentos heterogêneos** que necessitam ser gerenciados, porém possuem um suporte nativo ao gerenciamento rígido e limitado. Assim, a abordagem proposta não exige a implantação de *peers* em todos os nodos da rede: o modelo e arquitetura foram concebidos para fazer uso de entidades que podem ser empregadas para estender o gerenciamento destes equipamentos, através das *entidades para controle dos recursos gerenciados*.

A arquitetura proposta neste capítulo abordou a estrutura do ambiente de gerenciamento, discutindo as categorias presentes no ambiente e sua organização em serviços e aplicações. Esta arquitetura enfoca a estrutura do ambiente de gerenciamento, sem especificar como os serviços estruturais ou as funcionalidades de gerenciamento serão desenvolvidos sobre tal ambiente. Tal estrutura objetiva proporcionar a separação

entre a arquitetura do ambiente de gerenciamento global e a arquitetura de seus serviços e funcionalidades em particular, permitindo que serviços estruturais com diferentes características sejam providos, assim como que novas funcionalidades de gerenciamento possam ser desenvolvidas ou alteradas de modo independente.

A definição dos serviços estruturais, por sua vez, deve ser realizada considerando a infra-estrutura P2P sobre o qual o ambiente foi implementado e os requisitos para o serviço em um ambiente de gerenciamento de redes como o proposto. As características do serviço estrutural de envio de notificações no ambiente são discutidas como exemplo no capítulo 6.

Por fim, o modo como as funcionalidades de gerenciamento são executadas no ambiente é definido através de arquiteturas para suas atividades, que irão determinar como a funcionalidade é projetada, assim como quais serviços são empregados para que esta seja realizada e suas composições, se existirem. A arquitetura para a atividade de *polling* distribuído, empregada para duas funcionalidades de gerenciamento, é abordada como estudo de caso no capítulo 7.

6 SERVIÇO ESTRUTURAL: ENVIO DE NOTIFICAÇÕES

O capítulo anterior apresentou a arquitetura para um ambiente de gerenciamento distribuído baseado em P2P. Como visto, a arquitetura é estruturada em categorias de serviços. A categoria de serviços e aplicações de gerenciamento compreende as funcionalidades para o gerenciamento propriamente dito. Tais funcionalidades podem fazer uso de facilidades na categoria de serviços estruturais do ambiente P2P, que contém serviços que podem ser úteis para qualquer ambiente distribuído. Os serviços estruturais do ambiente P2P são proporcionados pela infra-estrutura P2P básica sobre a qual o ambiente está estruturado.

Um dos principais serviços estruturais de um ambiente distribuído para gerenciamento de redes compreende o mecanismo para envio de notificações. Este capítulo discute as características deste serviço para um ambiente de gerenciamento de redes como o proposto. A seção a seguir introduz o serviço de envio de notificações e apresenta o paradigma *publish-subscribe*, seguido por tal serviço. As seções posteriores discutem as características do serviço para um ambiente de gerenciamento como o proposto.

6.1 Serviço de Envio de Notificações *Publish-Subscribe*

O mecanismo para envio de notificações é utilizado por diversas atividades de gerenciamento de redes, sendo empregado para a retransmissão de notificações de eventos geradas pelos equipamentos gerenciados, para o envio de alarmes indicando situações críticas detectadas através de *polling*, para o envio de eventos reportando novas versões de imagens de software, etc. No ambiente de gerenciamento distribuído baseado em P2P proposto, este mecanismo deve ser oferecido através de um serviço de envio de notificações que segue o paradigma *publish-subscribe* e é baseado na infra-estrutura P2P utilizada pelo ambiente.

No paradigma *publish-subscribe* (EUGSTER et al, 2003) (MAHAMBRE; KUMAR; BELLUR, 2007) (BEHNEL; FIEGE; MÜHL, 2006) (HUANG; GARCIA-MOLINA, 2004), *subscribers* (**assinantes**) comunicam seu interesse no recebimento de certos eventos através de uma *subscription* (**subscrição**) e são notificados da ocorrência destes quando estes são publicados por *publishers* (**publicadores**) através de *notificações de eventos*. Uma infra-estrutura para envio de notificações media a comunicação entre publicadores e assinantes, provendo o gerenciamento das subscrições e a entrega eficiente das notificações publicadas. A figura 6.1 esquematiza o paradigma.

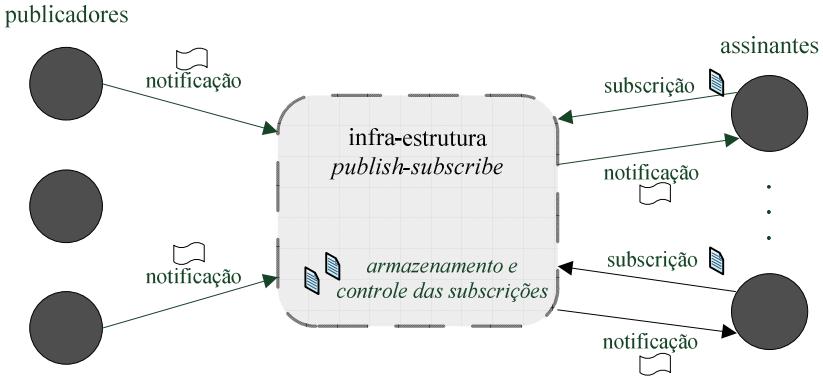


Figura 6.1: Esquema do paradigma *publish-subscribe*

Uma das principais vantagens da utilização do paradigma *publish-subscribe* para um serviço de envio de notificações é o desacoplamento de espaço, de tempo e de sincronização proporcionado (EUGSTER et al, 2003), que aumenta a escalabilidade dos sistemas. Assinantes e publicadores não precisam conhecer-se uns aos outros. Na ocorrência de um evento, publicadores divulgam este evento através do mecanismo de envio de notificações, sem preocupar-se com os assinantes interessados. Além disso, assinantes e publicadores não necessitam participar ativamente da comunicação. Conforme a qualidade do serviço oferecida pela infra-estrutura *publish-subscribe*, publicadores podem publicar eventos enquanto assinantes estão desconectados e estes, ao se reconectarem, receberão os eventos anteriores. Por fim, quando um publicador publica uma notificação, este não necessita ficar bloqueado enquanto os assinantes interessados recebem a mensagem. A entrega da notificação é feita assincronamente, pois a publicação do evento pelo publicador e o recebimento do evento pelos assinantes não ocorre no fluxo de controle principal. O desacoplamento de tais sistemas permite ainda que publicadores e assinantes não tenham conhecimento da organização ou tamanho da infra-estrutura *publish-subscribe*: esta pode ser formada por um único *broker* ou por um conjunto destes, organizados em diferentes arquiteturas.

A estrutura de infra-estruturas *publish-subscribe* tem sido descrita de diversas formas, não havendo uma definição unificada sobre como organizá-la. Adotando uma organização que se baseia e combina as apresentadas em (BEHNEL; FIEGE; MÜHL, 2006), (EUGSTER et al, 2003) e (MAHAMBRE; KUMAR; BELLUR, 2007), uma infra-estrutura *publish-subscribe* pode ser compreendida como formada por duas camadas. A primeira camada compreende características funcionais obrigatórias que formam o *core* (núcleo) da infra-estrutura, tais como sua arquitetura e o modo como a disseminação das mensagens é feita. A segunda camada compreende um conjunto de serviços opcionais que provêem garantias de qualidade de serviço (QoS).

A utilização de uma infra-estrutura *publish-subscribe* no ambiente de gerenciamento de redes distribuído baseado em P2P deve permitir a transmissão de notificações de acordo com as características e as garantias de QoS requeridas por tal ambiente. Em simultâneo, deve considerar as características da rede P2P sobre a qual o ambiente está estruturado.

As seções a seguir discutem as características de uma infra-estrutura *publish-subscribe* no ambiente de gerenciamento proposto. Seguindo a estrutura composta por duas camadas, a seção inicial discute as características do núcleo da infra-estrutura *publish-subscribe* para um ambiente de gerenciamento de redes distribuído baseado em

P2P. A seção posterior aborda os requisitos de QoS da infra-estrutura requeridos por tal ambiente.

6.2 Características do Núcleo da Infra-Estrutura *Publish-Subscribe* no Ambiente Proposto

O núcleo de uma infra-estrutura *publish-subscribe* (MAHAMBRE; KUMAR; BELLUR, 2007) (EUGSTER et al, 2003) (HUANG; GARCIA-MOLINA, 2004) (BEHNEL; FIEGE; MÜHL, 2006) compreende quatro características: o modelo de eventos, o esquema de subscrições, a arquitetura e o modo de disseminação das notificações.

O **modelo de eventos** define como e por quais parâmetros os eventos são identificados na infra-estrutura. Faz uso de três tipos de mensagens: anúncios, subscrições e notificações. As mensagens de **anúncio** são utilizadas pelos publicadores para estes informarem à infra-estrutura sobre as notificações que eles possuem capacidade de publicar e suas propriedades. Este tipo de mensagem não é suportado por todas as infra-estruturas *publish-subscribe*. As mensagens de **subscrição** são utilizadas pelos assinantes para estes informarem os eventos que desejam receber, cuja ocorrência é reportada através de mensagens de **notificação**. Os eventos podem ser organizados hierarquicamente através de seu tipo, de modo que a subscrição para um tipo de evento englobe a subscrição para todos os eventos inferiores a este tipo na hierarquia.

No ambiente de gerenciamento proposto, a infra-estrutura *publish-subscribe* a ser empregada deve suportar, quando possível, não apenas as mensagens de subscrição e de notificação, mas também a mensagem de anúncio. Esta mensagem pode ser utilizada, por exemplo, na atividade de monitoração da rede, para que as *entidades para controle dos recursos gerenciados* informem antecipadamente quais as notificações que os recursos gerenciados por elas possuem capacidade de enviar (*e.g.*, alarmes que cada recurso gerenciado gera). Como nas redes atuais novos equipamentos são inseridos freqüentemente, as mensagens de anúncio podem ser utilizadas para que as aplicações e os serviços de gerenciamento interessados no recebimento de notificações possam tomar conhecimento dos novos eventos e façam subscrições para estes. Na atividade de monitoração, as subscrições são enviadas, tipicamente, por *entidades para interface com o administrador da rede* e por *entidades para serviços de gerenciamento*, enquanto as notificações são enviadas pelas *entidades para controle dos recursos gerenciados*.

A subscrição de assinantes para um ou mais eventos pode ser feita de diversos modos, o que define o **esquema de subscrição** utilizado. Diversos esquemas de subscrição têm sido utilizados em infra-estruturas *publish-subscribe* (EUGSTER et al, 2003) (HUANG; GARCIA-MOLINA, 2004) (MAHAMBRE; KUMAR; BELLUR, 2007) (COURTENAGE; WILLIAMS, 2006). No esquema baseado em grupos, um conjunto de grupos é definido para o sistema. Os assinantes se inscrevem para receber eventos de um ou mais grupos, e cada evento é publicado em um grupo específico pelo publicador. No esquema baseado em tópicos, um assunto é designado para descrever o conteúdo do evento. A subscrição é realizada para um ou mais tópicos, e hierarquias para organizar os tópicos podem ser suportadas, nas quais a subscrição para um tópico superior na hierarquia significa a subscrição para todos os tópicos inferiores a este. Por fim, o esquema baseado em conteúdo pode ser visto como uma melhoria do esquema baseado em tópicos nos quais a subscrição se baseia no conteúdo real dos eventos (suas propriedades), ao invés dos eventos serem classificados de acordo com um critério

externo pré-definido como o nome do tópico. A subscrição é realizada utilizando filtros que definem condições, usualmente na forma de pares *nome-valor* comparando propriedades dos eventos através de operadores como igualdade, maior, menor e suas combinações. Alguns sistemas permitem até mesmo subscrições para eventos correlacionados, com os quais assinantes somente são notificados na ocorrência do conjunto de eventos. Este esquema de subscrição oferece uma flexibilidade muito maior que os esquemas citados anteriormente, porém traz também uma complexidade muito maior no projeto e na implementação.

No ambiente de gerenciamento proposto, nenhum esquema de subscrições específico é requerido na infra-estrutura, porém este necessita ser flexível para permitir o tratamento de novos eventos de gerenciamento, já que, como anteriormente discutido, o gerenciamento da rede evolui constantemente e novos eventos são inseridos na rede ao longo do tempo. Deste modo, através de uma combinação das mensagens de anúncio (se suportadas) e do esquema de subscrição empregado, devem haver meios para que os assinantes façam subscrições para novos eventos da rede: isto pode ser realizado através de novas subscrições ou através de subscrições que suportem esta flexibilidade. O esquema necessita, ainda, ser flexível para suportar notificações de eventos com características variáveis, já que a rede gerenciada pode possuir uma grande heterogeneidade de recursos que resulta em diferentes tipos de eventos, originados a partir de diversos protocolos, com diferentes atributos.

Em relação à **arquitetura** de uma infra-estrutura *publish-subscribe*, esta pode ser representada através de três tipos (EUGSTER et al, 2003). Na arquitetura centralizada, publicadores enviam os eventos para uma entidade central que os armazena e os repassa aos assinantes interessados. Na arquitetura distribuída, primitivas de comunicação inteligentes que implementam mecanismos de armazenamento e envio são implementadas nos processos dos assinantes e publicadores de modo que a comunicação seja vista como assíncrona e anônima, sem a necessidade de uma entidade intermediária. Na arquitetura intermediária, o serviço de notificações de eventos é implementado como uma rede distribuída de servidores, que pode utilizar diferentes topologias.

No ambiente proposto, a arquitetura da infra-estrutura *publish-subscribe* intermediária se mostra a mais adequada. Uma arquitetura centralizada, implementada por um único *broker*, não é viável para este modelo por possuir um único ponto de falha, acarretar alto tráfego nos enlaces próximos ao *broker* e demandar alto poder de processamento em um único equipamento.

A **disseminação das notificações** publicadas na infra-estrutura para os assinantes interessados varia conforme as demais características da infra-estrutura, especialmente sua arquitetura e seu esquema de subscrições. A disseminação pode ser feita de diferentes modos, incluindo comunicação ponto-a-ponto, comunicação *multicast* ou fazendo uso de uma rede *overlay* de roteamento.

No ambiente proposto, a disseminação de notificações publicadas deve ser realizada observando as diversas características do ambiente de gerenciamento. A escalabilidade necessita ser avaliada, pois uma rede de computadores pode possuir um grande número de recursos gerenciados. Além disto, em situações de falha em um recurso, é comum a geração de um grande número de eventos em um curto período de tempo, emitidos não apenas pelo próprio recurso com a falha, como também pelos demais recursos afetados por esta. Este requisito se torna ainda mais severo em situações nas quais a falha resulta

na redução da largura de banda disponível nos enlaces da rede, pois um grande número de notificações é gerado em um ambiente no qual a largura de banda já se encontra reduzida. Requisitos de tolerância a falhas devem também ser considerados no modo utilizado para a disseminação das notificações, a fim de que eventos importantes nunca sejam perdidos na rede de gerenciamento.

O suporte produzido por redes P2P tem sido freqüentemente utilizado para a disseminação de notificações de sistemas *publish-subscribe* (CHOI; PARK, 2005) (COURTENAGE; WILLIAMS, 2006) (GUPTA et al, 2004) (KOUBARAKIS et al, 2003). No ambiente proposto, esta utilização se torna facilitada em virtude da infra-estrutura P2P integrar a arquitetura do ambiente. Esta infra-estrutura P2P pode ser utilizada de diferentes modos, para diferentes mecanismos. O mecanismo de envio de notificações pode, por exemplo, localizar as subscrições (e, assim, identificar os assinantes) usando uma *distributed hash table* (DHT) (CHOI; PARK, 2005) (GUPTA et al, 2004) ou através de *super-peers* (KOUBARAKIS et al, 2003). Mecanismos híbridos podem também ser empregados, tal como o proposto em (COURTENAGE; WILLIAMS, 2006), que utiliza uma DHT para definir o armazenamento das subscrições e o *framework* JXTA para efetuar o roteamento e a disseminação de eventos. Funcionalidades da rede P2P que possibilitam a consciência da topologia física podem também ser utilizadas e são úteis para na disseminação dos eventos, ao levar em conta características da rede real como largura de banda, tolerância a falhas dos nodos e enlaces envolvidos, distância física entre os nodos, domínio administrativo a que o nodo pertence, entre outros.

6.3 Garantias de QoS da Infra-Estrutura *Publish-Subscribe* no Ambiente Proposto

Diversas garantias de QoS podem ser oferecidas por uma infra-estrutura *publish-subscribe* (BEHNEL; FIEGE; MÜHL, 2006) (MAHAMBRE; KUMAR; BELLUR, 2007) (EUGSTER et al, 2003), que podem ser agrupadas em dois grandes grupos: *garantias do nível da infra-estrutura global* e *garantias do nível de subscrições e notificações*. Estas garantias são discutidas a seguir.

6.3.1 Garantias de QoS do Nível da Infra-Estrutura Global

As garantias de QoS do nível da infra-estrutura global compreendem as propriedades de baixo nível da infra-estrutura do serviço de notificação de eventos, incluindo largura de banda, garantias de entrega e persistência de mensagens (BEHNEL; FIEGE; MÜHL, 2006) (MAHAMBRE; KUMAR; BELLUR, 2007) (EUGSTER et al, 2003). Em ambientes que utilizam o suporte P2P para a disseminação das notificações, estas garantias estão profundamente relacionadas às providas pela infra-estrutura P2P utilizada.

No ambiente de gerenciamento proposto, a adoção do paradigma *publish-subscribe* demanda a observância cuidadosa de certas garantias de QoS, tais como, por exemplo, largura de banda e garantias de entrega. As principais garantias deste grupo serão discutidas a seguir.

A **largura de banda** consumida pela infra-estrutura *publish-subscribe* está relacionada à arquitetura e ao modo de disseminação de notificações utilizados na infra-estrutura. No ambiente proposto, a utilização de largura de banda para a execução da infra-estrutura *publish-subscribe* é uma característica importante, pois o gerenciamento

deve causar o menor impacto possível na rede física real. Em virtude disso, é desejável que publicadores possam controlar e divulgar em seus anúncios qual o limite máximo de tráfego que seus eventos geram. Além disto, é desejável permitir que subscrições delimitem a largura de banda máxima que a infra-estrutura pode utilizar para enviar as notificações subscritas. A necessidade de controle de largura de banda é ainda mais importante se houver a presença de entidades de gerenciamento em nodos móveis, já que estes possuem limitações mais severas de recursos e um tráfego maior pode provocar um consumo de energia não suportado (BEHNEL; FIEGE; MÜHL, 2006) (HUANG; GARCIA-MOLINA, 2004).

A *composição de eventos pela infra-estrutura publish-subscribe* pode ser uma alternativa para reduzir a largura de banda, já que, com este mecanismo, uma única mensagem é gerada e entregue pela infra-estrutura *publish-subscribe* em substituição a diversas mensagens publicadas originalmente que seguem uma determinada ordem ou padrão, de modo que a mensagem gerada represente as diversas mensagens originais. Esta composição pode se dar no nível de subscrições, como proposto em (COURTENAGE; WILLIAMS, 2006). O suporte à composição de eventos, entretanto, eleva o grau de complexidade de outros aspectos da infra-estrutura, tais como o esquema de subscrições, a arquitetura e a disseminação de eventos. A proximidade de conceitos entre a composição de eventos pela infra-estrutura *publish-subscribe* e a correlação de eventos em gerenciamento de redes — tópico amplamente discutido na área de gerenciamento de redes (COMER, 2006) — sugere uma análise unificada de ambas as técnicas de modo a oportunizar a integração da correlação de eventos em gerenciamento de redes na própria infra-estrutura *publish-subscribe* do ambiente.

As **garantias de entrega** de infra-estruturas *publish-subscribe* estão relacionadas à confiabilidade na entrega das mensagens, garantindo que não haverá perda de mensagens ou duplicação. Quatro níveis de garantias podem ser oferecidos: melhor esforço, no qual não há garantia de confiabilidade e notificações são enviadas sem garantia de entrega e com possibilidade de duplicação; no máximo um, no qual é garantido que o assinante não receberá notificações duplicadas; no mínimo um, no qual é garantido que o assinante receberá ao menos uma mensagem da notificação; e exatamente um, no qual é garantido que o assinante receberá todas as notificações enviadas e sem duplicações. Em infra-estruturas em que todas as garantias forem suportadas, a definição das garantias exigidas para cada notificação pode ser feita através das subscrições dos assinantes, definindo que notificações estes precisam receber, que notificações podem ser perdidas e que notificações não podem ser recebidas duplicadamente. Além disso, publicadores podem também definir, através dos anúncios e das notificações, quais notificações precisam ser transmitidas aos assinantes (BEHNEL; FIEGE; MÜHL, 2006) (MAHAMBRE; KUMAR; BELLUR, 2007).

No ambiente proposto, as garantias de entrega demandadas estão relacionadas às atividades sendo desempenhadas, às características dos eventos gerados e à sua severidade. Na monitoração da rede, por exemplo, considerando uma análise geral, é exigida a transmissão das notificações para os assinantes interessados, já que serão através destas notificações que as *entidades para controle dos recursos gerenciados* informarão as demais entidades do ambiente sobre a ocorrência de falhas nos recursos gerenciados, que podem ter sido detectadas através do recebimento de notificações dos próprios recursos gerenciados ou através do *polling* destes. Em virtude da arquitetura fortemente distribuída do ambiente, com distribuição das atividades de gerenciamento por toda a rede, esta necessidade ganha ainda maior importância, já que a monitoração

dos recursos será realizada por múltiplas entidades, que necessitam informar as demais entidades do ambiente sobre os eventos detectados.

A entrega duplicada de uma notificação pode causar dificuldades em alguns assinantes do ambiente de gerenciamento, de acordo com os objetivos das aplicações utilizadas por estes. Em aplicações cujo propósito é apenas mostrar o último estado dos recursos, a duplicação de uma mensagem de notificação não causa problema: apenas um maior processamento terá sido exigido, porém a aplicação continuará produzindo resultados consistentes. Entretanto, em aplicações que objetivam apresentar a lista de eventos da rede, a presença de mensagens duplicadas pode causar interpretações incorretas se não houver algum tratamento para eliminá-las. O mesmo ocorre para a correlação de eventos, já que a ocorrência de eventos idênticos seqüenciais pode provocar a geração de determinado evento relacionado.

Outro aspecto relativo às garantias de entrega é a **persistência de mensagens**, que diz respeito à garantia de entrega de mensagens para assinantes que temporariamente não podem ser acessados através da rede (*e.g.*, por falhas nos enlaces intermediários ou por desconexão temporária de assinantes em ambientes móveis). Nestas situações, pode ser necessário que a infra-estrutura *publish-subscribe* ofereça persistência das mensagens, armazenando a notificação até que os assinantes possam ser novamente acessados.

No ambiente de gerenciamento proposto, esta garantia varia de acordo com os objetivos do assinante. Por exemplo, aplicações em nodos móveis que necessitam mostrar o último estado dos recursos podem substituir a persistência por um mecanismo de atualização quando o nodo for novamente conectado à rede. Ao analisar a necessidade de persistência para cada assinante, deve ser considerado por qual período as notificações permanecerão válidas. Em uma análise geral, o suporte à persistência de notificações revela-se importante, pois uma falha em um enlace da rede física pode gerar interrupção nos canais da rede P2P, bloqueando o envio de eventos até mesmo daqueles recursos não envolvidos na falha.

Como visto, diversas garantias de QoS variam no ambiente proposto de acordo com a atividade sendo desempenhada, os objetivos dos assinantes e as características dos eventos. Desde modo, na infra-estrutura *publish-subscribe* integrada a este ambiente, é conveniente que as subscrições possam indicar as garantias requeridas pelos assinantes. Esta indicação pode ser utilizada também em anúncios e notificações: ao publicador seria permitido indicar requisitos *default* para a notificação, requisitos estes que poderiam ser sobrepostos pelos assinantes. A possibilidade de publicadores indicarem as garantias requeridas é importante para permitir o tratamento de novos eventos sem a necessidade de configurar as aplicações assinantes.

6.3.2 Garantias de QoS do Nível de Subscrições e Notificações

O segundo grupo de garantias de QoS em infra-estruturas *publish-subscribe* está relacionado à semântica de subscrições e notificações (BEHNEL; FIEGE; MÜHL, 2006) (MAHAMBRE; KUMAR; BELLUR, 2007) (EUGSTER et al, 2003). As principais garantias deste grupo são discutidas a seguir.

A garantia de **ordenação das notificações** entregues aos assinantes no ambiente proposto pode ser relevante para alguns tipos de notificações e alguns assinantes, pois algumas vezes a ocorrência de um evento após outro é uma informação importante para identificar a origem da falha. Como esta garantia não é requerida por todos os

assinantes, é conveniente que sua necessidade possa ser configurada pelas notificações e subscrições se não puder ser sempre oferecida, ou possuir custo elevado para disponibização.

O **período de validade de uma notificação** indica até quando uma notificação permanece válida, o que pode ser indicado por uma unidade de tempo ou através da recepção de uma notificação mais recente. Este requisito está relacionado às garantias de ordenação e entrega, especialmente em situações em que a validade da notificação é identificada pela recepção de outra notificação mais recente. O uso de **fontes redundante** para um mesmo evento, utilizado em algumas infra-estruturas para aumentar a tolerância a falhas da entrega das notificações, não é relevante para ambientes de gerenciamento de redes, já que acaba por gerar maior volume de tráfego sem prover garantias reais da entrega da mensagem.

A **entrega periódica ou esporádica** indica se a notificação deve ser recebida periodicamente pelos assinantes, refletindo o estado da informação no momento, ou esporadicamente, reportando apenas mudanças no estado da informação, com base na comparação entre o valor corrente com o valor anterior da informação, podendo fazer uso de limiares pré-configurados para ponderar a diferença entre tais valores. Esta garantia não é necessária em uma infra-estrutura *publish-subscribe* básica aplicada para o gerenciamento de redes, já que, tradicionalmente, controles semelhantes para entrega esporádica têm sido implementados pelas próprias aplicações de gerenciamento de redes e podem ser transpostos, no ambiente baseado em P2P proposto, para as aplicações e os serviços de gerenciamento. Por exemplo, para a monitoração de recursos, tais controles podem ser realizados pelas *entidades para controle dos recursos gerenciados*, sendo estas responsáveis por não publicar notificações se não houverem mudanças consideradas significativas no estado da informação. Contudo, esta garantia pode ser utilizada em uma infra-estrutura mais elaborada e traz benefícios para diversas tarefas de gerenciamento, liberando as aplicações e serviços deste controle. Como exemplo, pode ser utilizada para proporcionar a filtragem de alarmes duplicados, isto é, alarmes idênticos que são gerados repetidamente para indicar uma mesma situação de falha. Pode, ainda, ser estendida para eliminar também alarmes oscilantes, isto é, alarmes quando uma mesma situação de falha causa repetidas seqüências similares de alarmes.

Por fim, a **seletividade das subscrições** está relacionada ao grau de complexidade da linguagem utilizada para expressar as subscrições em relação ao mecanismo de casamento destas com as notificações publicadas, falsos positivos na entrega, etc. De modo geral, linguagens mais complexas permitem que as subscrições sejam feitas de modo mais preciso, diminuindo o número de falsos positivos. Contudo, tais linguagens tendem a dificultar o uso de otimizações nos filtros e no casamento distribuído.

No ambiente proposto, a infra-estrutura *publish-subscribe* deve permitir que a subscrição defina características de eventos tais como o tipo de recurso gerenciado, o recurso origem do evento, o tipo de informação, o conteúdo da informação no evento, entre outras. Em virtude do grande número de recursos gerenciados em uma rede e dos requisitos de desempenho usualmente presentes em tais ambientes, o esquema de casamento entre as notificações publicadas e as subscrições cadastradas pelos assinantes deve possibilitar apenas um pequeno número de falsos positivos e deve ser feito, sempre que possível, próximo aos publicadores, evitando o tráfego desnecessário na rede.

6.4 Serviço de Envio de Notificações *Publish-Subscribe* no Ambiente de Gerenciamento Proposto

A implantação de um serviço de notificações baseado no paradigma *publish-subscribe* em um ambiente de gerenciamento de redes resulta em benefícios para diversos serviços e aplicações do ambiente, que podem agora fazer uso de um mecanismo escalável, eficiente e flexível para o envio de notificações de qualquer tipo. A utilização de uma rede P2P para a infra-estrutura *publish-subscribe* tem sido estudada, como discutido previamente, em diversos sistemas (CHOI; PARK, 2005) (COURTENAGE; WILLIAMS, 2006) (GUPTA et al, 2004) (KOUBARAKIS et al, 2003). Tais sistemas fazem uso da rede P2P para localizar as subscrições e rotear notificações para os assinantes interessados através dos mecanismos de comunicação e busca providos pela rede.

No ambiente apresentado, a execução do serviço de notificação é realizada utilizando os próprios *peers* do ambiente, tipicamente incluindo todos os *peers* para a infra-estrutura *publish-subscribe*. Entre estes, *peers para interface com o administrador da rede* (IA), *peers para controle dos recursos gerenciados* (CRG) e *peers para serviços de gerenciamento* (SG) podem assumir o papel de assinantes. Tipicamente, o papel de publicador é assumido por *peers CRG* e *peers SG*. Contudo, *peers para interface com o administrador da rede* também podem publicar notificações (*e.g.*, para indicar uma ação de um usuário em uma aplicação, tal como a inclusão de um equipamento em um mapa que controla os recursos sendo monitorados). O mecanismo de envio das notificações propriamente dito (incluindo o armazenamento das subscrições e o roteamento de notificações) é implementado tipicamente por todos os *peers* que compõem o ambiente de modo conjunto, fazendo uso da infra-estrutura P2P para a comunicação entre assinantes e publicadores.

Em um ambiente de gerenciamento de redes, a atividade de monitoração dos recursos gerenciados por aplicações e serviços de gerenciamento afigura-se como uma das maiores consumidoras deste mecanismo. Tal atividade inclui funcionalidades para a retransmissão de mensagens recebidas dos recursos gerenciados (*e.g.*, traps SNMP) e funcionalidades para o envio de notificações geradas pelas próprias *entidades CRG* para estas reportarem situações identificadas através de operações de *polling* nos equipamentos (*e.g.*, reportando o estado indevido de um recurso, ou limiares excedidos na coleta de dados de desempenho). Outras atividades, porém, também podem fazer uso deste serviço estrutural, tal como o serviço para instalação de novas versões de software.

A figura 6.2 exemplifica o uso do serviço de envio de notificações por algumas funcionalidades de monitoração de redes. Na porção esquerda e central do nível superior, dois *grupos de peers CRG* são responsáveis pela recepção de alarmes e pelo *polling* de recursos da rede: estes *peers* assumem o papel de publicadores. Na porção direita do nível superior, um *peer IA* executa uma aplicação para visualização de alarmes em tempo real: este *peer* assume o papel de assinante.

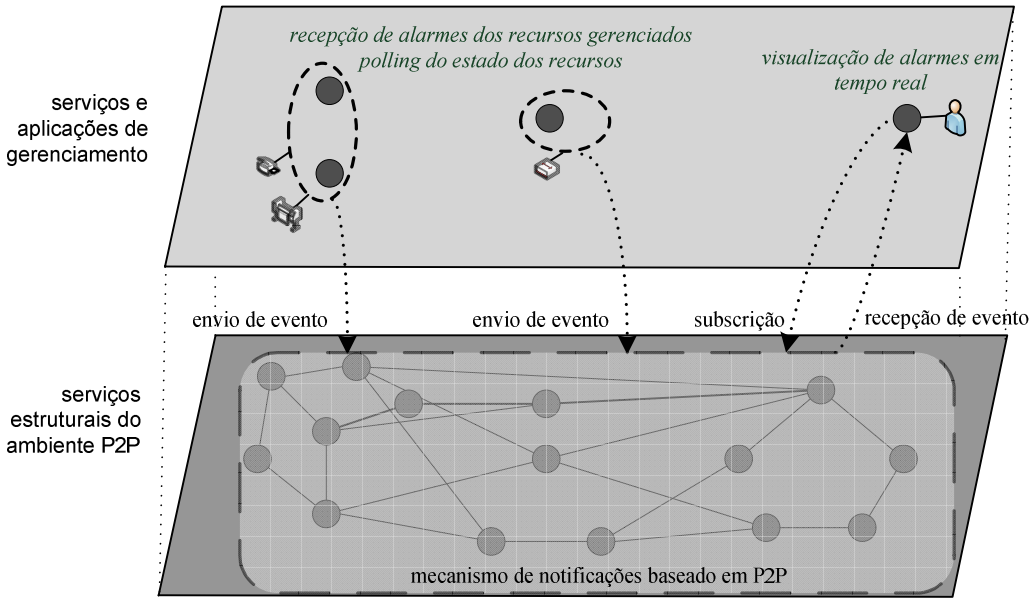


Figura 6.2: Exemplo de uso do serviço de envio de notificações

As seções 6.2 e 6.3 discutiram, em um plano teórico e amplo, as características e os requisitos de QoS necessários ou desejáveis para um serviço de envio de notificações *publish-subscribe* em um ambiente de gerenciamento como o proposto. Este serviço, contudo, não necessita ser desenvolvido de modo específico para o ambiente proposto: o desenvolvimento e a implantação deste serviço no ambiente proposto podem ser realizados fazendo uso de abordagens *publish-subscribe* baseadas em P2P já propostas na literatura, que podem ser investigadas para serem integradas ao novo ambiente. Esta integração pode requerer alterações na abordagem para fazer uso da infra-estrutura P2P suportada no ambiente de gerenciamento e alterações na infra-estrutura P2P do ambiente para suporte à abordagem, conforme as características da abordagem e da infra-estrutura P2P empregada no ambiente de gerenciamento. Além disto, muitas características ou requisitos de QoS desejáveis ao serviço de envio de notificações no ambiente podem não ser suportadas pela abordagem sendo integrada: estes aspectos devem também ser analisados ao investigar quais as abordagens mais adequadas às características do ambiente de gerenciamento específico.

A seguir, algumas abordagens para envio de notificações *publish-subscribe* baseadas em P2P propostas na literatura são brevemente apresentadas como exemplo, representando três modos distintos de uso da rede P2P. Cabe destacar, entretanto, que estas abordagens representam apenas exemplos entre as existentes: outras abordagens devem também ser investigadas ao buscar a abordagem mais adequada para um ambiente de gerenciamento específico, o que está relacionado, de modo especial, com a infra-estrutura P2P utilizada no ambiente.

6.4.1 Abordagem proposta por Chirita e Outros

O sistema proposto em (CHIRITA et al, 2004) é exemplo de uma abordagem que pode ser investigada para ser integrada ao ambiente de gerenciamento. Tal sistema, concebido a partir da experiência obtida com o sistema P2P-DIET (KOUBARAKIS et al, 2003), representa uma implementação de um sistema *publish-subscribe* em uma rede P2P baseada em *super-peers*. O sistema foi concebido para que um usuário possa

submeter uma *query* contínua acerca de recursos disponíveis na rede e este receba notificações quando ocorram eventos relativos a estes novos recursos, tais como um novo arquivo ser disponibilizado no sistema de compartilhamento de arquivos ou um novo livro ser oferecido em uma biblioteca digital. O sistema suporta três tipos mensagens: anúncios, subscrições e notificações. As subscrições são armazenadas próximas aos *peers* que publicam as notificações relacionadas à subscrição. Quando uma notificação é gerada, esta é propagada para todos os *peers* cujas subscrições casam com a notificação emitida. Os anúncios são utilizados para os *peers* informarem em alto nível as notificações que irão publicar. Os *super-peers* são organizados no sistema em um topologia *HyperCub*, que permite a difusão das *querys* de modo eficiente e não redundante (CHIRITA et al, 2004).

O primeiro passo no sistema ocorre quando um *peer* envia anúncios para seu *super-peer* indicando as notificações que irá oferecer no futuro. O *super-peer* difunde o anúncio para os demais *super-peers* da rede e utiliza o anúncio para a atualização de seu *índice de roteamento de anúncios,* que será utilizado ao processar subscrições.

Quando um *peer* assinante submete uma subscrição para seu *super-peer*, esta subscrição é armazenada em uma *estrutura de subscrições* no *super-peer* e este define se ela deve ser re-encaminhada para os demais *super-peers* da rede P2P. A *estrutura de subscrições* emprega uma hierarquia de subscrições que faz uso de generalizações. Esta hierarquia de subscrições é utilizada para minimizar o tráfego na rede, de modo que *super-peers* não repassem subscrições que já foram submetidas em subscrições anteriores mais genéricas ou idênticas, ou que não possuam anúncios relacionados. Se o *super-peer* decide enviar a subscrição adiante, ele inicia um procedimento de difusão seletiva baseada no protocolo *HyperCub*. As subscrições recebidas por um *super-peer* são casadas com os *índices de roteamento de anúncios* a fim de definir se a subscrição deve ser enviada para cada *super-peer* vizinho.

Quando uma notificação é enviada para um *super-peer*, este faz o casamento da notificação com as subscrições raízes em sua *estrutura de subscrições*. Se a notificação casa com uma subscrição raiz, esta é casada com as subscrições filhas (que representam refinamentos da subscrição raiz). A cada subscrição em que a notificação realiza um casamento positivo, a notificação é enviada para os *peers* e *super-peers* que originaram a subscrição.

Este sistema *publish-subscribe* pode ser investigado para ser integrado ao ambiente de gerenciamento distribuído proposto e ser empregado para prover o serviço de envio de notificações *publish-subscribe*. Por fazer uso de redes P2P baseadas em *super-peers*, este sistema se mostra mais adequado de ser integrado ao ambiente de gerenciamento se este fizer uso de uma infra-estrutura P2P também baseada em *super-peers*. Além disto, esta integração deve considerar ainda alguns aspectos que diferenciam o ambiente de gerenciamento do ambiente para o qual o sistema foi inicialmente proposto. No ambiente de gerenciamento, em virtude do crescimento e da evolução das redes, é freqüente a inclusão de novos equipamentos gerenciados em *grupos de entidades CRG* já existentes, assim como a inclusão de novos *grupos de entidades CRG*. Nestas situações, os anúncios emitidos por tais *grupos de entidades CRG* devem ser relacionados pela infra-estrutura *publish-subscribe* com as subscrições submetidas em período anterior aos anúncios serem emitidos. Considerações sobre este aspecto não são abordadas no sistema proposto em (CHIRITA et al, 2004). Assim, ao empregar tal sistema no ambiente de gerenciamento, o posicionamento das subscrições na rede P2P precisa ser analisado com respeito a esta temporalidade, a fim de que as notificações

sejam propagadas para as entidades assinantes interessadas mesmo se o anúncio acerca destas notificações foi emitido após a subscrição correspondente. Um mecanismo que pode ser investigado é a realização da análise de subscrições já armazenadas no ambiente quando um novo anúncio for emitido. Outro aspecto que pode ser considerado diz respeito ao fato de que, no ambiente de gerenciamento, tipicamente o número de subscrições não é elevado, sendo este muito inferior ao número de notificações emitidas. Assim, o mecanismo que minimiza a difusão das subscrições no sistema para redução de tráfego poderia ser analisado para ser simplificado sem causar detrimento significativo do tráfego na rede no ambiente de gerenciamento.

A abordagem proposta em (CHIRITA et al, 2004) oferece ainda um tratamento para persistência de notificações para *peers* assinantes que estão desconectados da rede quando uma notificação relacionada é gerada. Tal mecanismo é útil no ambiente de gerenciamento proposto para o recebimento de notificações por aplicações de gerenciamento em nodos móveis ou para situações em que houver particionamento temporário da rede por falhas nos enlaces de comunicação.

6.4.2 Abordagem proposta por Gupta e Outros

O sistema Meghdoot, proposto em (GUPTA et al, 2004), consiste em um sistema *publish-subscribe* que faz uso de uma rede P2P estruturada baseada em DHT para determinar onde as subscrições devem ser armazenadas e definir como as notificações de eventos são roteadas para as subscrições relacionadas. A estrutura DHT utilizada é baseada no CAN (RATNASAMY et al, 2001) e o sistema suporta a utilização de subscrições com múltiplos atributos.

A estrutura do sistema faz uso de um espaço cartesiano lógico com 2^n dimensões, sendo *n* o número de atributos definido para o sistema. Este espaço lógico é particionado entre os *peers* pertencentes ao sistema e cada *peer* é responsável por uma das partições, que são denominadas *zonas*. Cada *peer* mantém informações sobre as coordenadas de sua zona e informações das zonas vizinhas, assim como o endereço IP dos *peers* responsáveis por estas zonas.

As subscrições são armazenadas em *peers* da rede. Cada subscrição submetida ao sistema é mapeada para um ponto correspondente no espaço lógico com 2^n dimensões e é roteada para o *peer* responsável pela zona deste ponto, sendo armazenada neste *peer*.

Quando uma notificação de evento é publicada no sistema, esta deve ser casada com todas as subscrições relacionadas. Para isto, a notificação é mapeada para um ponto no espaço lógico e roteada para o *peer* cuja zona contém este ponto, utilizando múltiplos *peers* para realizar este roteamento. Atingindo este *peer*, a notificação é então propagada para todos os outros *peers* que pertencem a região do espaço lógico afetada pelo evento em questão. Um algoritmo para fazer o casamento das subscrições é ativado em cada um destes *peers*, e a notificação é enviada para os assinantes cujas subscrições casarem com a notificação publicada. O sistema oferece ainda um esquema de replicação das subscrições, a fim de evitar perda de subscrições em caso de *peers* que deixam a rede por falha, sem realizar a migração das subscrições anteriormente.

Uma importante característica desta abordagem para o uso de um ambiente de gerenciamento de redes é o suporte a múltiplos atributos, que podem ser trabalhados não apenas com valores fixos, mas também através de valores em intervalos. Em um ambiente de gerenciamento de redes como o proposto, esta característica traz grande flexibilidade aos serviços e às aplicações que farão uso do recebimento de notificações,

permitindo que o ambiente proporcione subscrições baseadas no tipo do evento, no equipamento origem, no tipo do equipamento origem, no conteúdo das informações de estado e desempenho reportadas através dos eventos, etc.

Por ser baseada em uma rede P2P estruturada que faz uso do CAN, esta abordagem se mostra particularmente adequada para ser analisada para uso em ambientes de gerenciamento que façam uso de uma infra-estrutura P2P também com estas características. Por outro lado, a utilização da abordagem em um ambiente de gerenciamento com infra-estrutura P2P baseada em outros mecanismos (tal como o emprego *super-peers* ou outras estruturas DHT) necessita ser investigada com maior detalhamento com o intuito de avaliar o *overhead* a ser introduzido para a manutenção da estrutura empregada por esta abordagem.

6.4.3 Abordagem proposta por Courtenage e Williams

O sistema proposto em (COURTENAGE; WILLIAMS, 2006) consiste em um sistema para envio de notificações de eventos baseado no paradigma *publish-subscribe* que utiliza uma rede P2P baseada em DHT para configurar as subscrições recebidas e o *framework* JXTA (GONG, 2001) (TRAVERSAT et al, 2003) para o roteamento das notificações de eventos publicadas. Uma importante característica deste sistema é o suporte à subscrição para eventos compostos, além de eventos primitivos.

As subscrições do sistema são baseadas no tipo de evento e predicados sobre estes. Para cada tipo de evento, é calculado seu *hash*, que é utilizado para identificar (através da arquitetura Chord) o *peer* que será responsável por fazer o casamento das subscrições e notificações. Este *peer* é denominado no sistema como *event detector*. Quando um assinante submete uma subscrição, esta é enviada para cada *peer* que representa o *event detector* correspondente aos tipos de eventos sendo subscritos. Neste *peer*, se ainda não existir, é criado um *event detector* para o tipo de evento correspondente. Em subscrições para eventos compostos, este processo é repetido recursivamente até que os *event detectors* de cada tipo de evento primitivo sejam encontrados ou criados. Quando um *event detector* é criado, o *peer* hospedeiro cria uma *output pipe* JXTA que será utilizada para publicar as notificações de eventos tratadas por aquele *event detector*. Após a criação da *pipe*, o *event detector* envia uma mensagem *ack* para o *peer* que enviou a subscrição (que pode ser o *peer* assinante original, ou um *event detector* para um evento composto). Ao receber o *ack*, o *peer* faz *bind* para a *output pipe* JXTA correspondente para que as notificações enviadas por esta *pipe* sejam recebidas por ele. A localização da *pipe* é realizada por este *peer* através do serviço de descoberta JXTA. Com este mecanismo, se um *event detector* é migrado para outro nodo, o roteamento dos eventos através deste *event detector* não é afetado.

O uso desta abordagem para a infra-estrutura *publish-subscribe* do ambiente de gerenciamento de redes proposto tem como benefício a possibilidade de incorporar à infra-estrutura do ambiente a composição de eventos suportada na abordagem. Como discutido na seção 6.3.1, a composição de eventos na infra-estrutura *publish-subscribe* pode ser investigada para a integração da correlação de eventos de gerenciamento de redes na própria infra-estrutura de envio de notificações.

Um aspecto a ser analisado ao utilizar a abordagem no ambiente proposto diz respeito ao uso do tipo de evento como chave para o posicionamento das subscrições e local para armazenamento destas. Em um ambiente de gerenciamento, seria adequado que as subscrições pudessem ser realizadas não apenas pelo tipo de evento, mas também

por outras características, tal como o equipamento gerenciado onde o evento ocorreu. Seria o caso, por exemplo, de uma aplicação ou de um serviço que tivesse interesse em receber todos os eventos relativos a um equipamento, independente do tipo de evento. Nestas situações, a subscrição para cada tipo de evento emitido pelo equipamento seria dispendiosa e complexa para a aplicação ou o serviço assinante, que pode não ter conhecimento de todos os tipos de eventos suportados: uma subscrição através do identificador do equipamento (*e.g.*, seu número IP) seria mais adequada. A implementação de mecanismos de subscrição baseados em outros aspectos além do tipo de evento, assim, deve ser analisada para a integração da abordagem ao ambiente proposto. Uma possibilidade que pode ser analisada seria empregar um nível superior para o armazenamento de subscrições baseadas em outras chaves (*e.g.*, número IP), combinada com o uso de anúncios dos *grupos de peers CRG* reportando os tipos de eventos suportados por cada tipo de equipamento. Neste caso, os anúncios emitidos por cada *grupo CRG*, para cada equipamento gerenciado, seriam direcionados ao *peer* correspondente ao *hash* do número IP do equipamento. Este *peer* seria também utilizado para o direcionamento das subscrições baseadas no número IP de equipamentos. Ao receber uma subscrição, este *peer* seria responsável por traduzir a subscrição baseada no número IP para subscrições baseadas nos tipos de eventos reportados através de anúncios para o dado equipamento. Como o procedimento de subscrições é realizado poucas vezes, o *overhead* causado por este mecanismo pode ser aceitável frente ao benefício proporcionado por subscrições a partir de outros fatores que não apenas o tipo de evento. Estes aspectos devem ser avaliados ao investigar a integração da abordagem no ambiente de gerenciamento.

6.5 Considerações Finais

Este capítulo discutiu o serviço estrutural de envio de notificações no ambiente de gerenciamento proposto. O capítulo inicialmente apresentou o paradigma *publish-subscribe*, seguido pela discussão das principais características e requisitos de QoS necessários e ou desejáveis ao serviço de envio de notificações em um ambiente de gerenciamento de redes distribuído como o proposto. Por fim, a seção 6.4 discutiu o serviço no ambiente de gerenciamento proposto e apresentou, como exemplo, algumas abordagens *publish-subscribe* baseadas em P2P existentes na literatura que podem ser investigadas para serem integradas ao ambiente.

Como discutido ao longo deste capítulo, este serviço baseia-se na infra-estrutura P2P utilizada no ambiente de gerenciamento. Deste modo, suas características estão relacionadas de modo fundamental às características da rede P2P empregada para o ambiente.

7 ESTUDO DE CASO: *POLLING* DISTRIBUÍDO

O capítulo 5 apresentou um ambiente para gerenciamento distribuído baseado em P2P, discutindo a arquitetura para este ambiente. Como visto, as funcionalidades de gerenciamento são realizadas no ambiente através de aplicações e de serviços de gerenciamento. Tais serviços fazem uso da infra-estrutura P2P e dos serviços estruturais fornecidos pelo ambiente, podendo utilizar composições de serviços.

Este capítulo apresenta um estudo de caso para uma atividade de gerenciamento baseada na arquitetura do ambiente proposto. O estudo aborda a realização de *polling* distribuído, atividade que é utilizada para as funcionalidades de monitoração do estado dos recursos na rede e de coleta periódica de dados de desempenho (discutidas anteriormente nas seções 5.3.2.2 e 5.3.2.3).

A atividade de *polling* foi selecionada como estudo de caso em virtude de sua importância, seu amplo uso e de suas limitações se realizada a partir de modelos tradicionais (tal como discutido nas seções 5.3.2.2 e 5.3.2.3). Esta atividade é realizada de forma periódica e freqüente no gerenciamento de redes, tipicamente para consulta de um número elevado de recursos gerenciados. Em virtude destas características, o tráfego de gerenciamento da atividade pode gerar sobrecarga nos enlaces de comunicação e limitações de escalabilidade na rede se a atividade for realizada a partir de arquiteturas centralizadas ou fracamente distribuídas, que concentram o tráfego de gerenciamento para um número restrito de entidades. As características da atividade acarretam, ainda, limitações de tolerância a falhas se realizada a partir de arquiteturas tradicionais, tal como a interrupção da consulta de um número elevado de recursos gerenciados em caso de particionamento da rede que isole a entidade responsável pela atividade.

A atividade de *polling* é utilizada para uma das funcionalidades de gerenciamento mais fundamentais — a monitoração da rede —, necessária para a identificação de falhas ou de situações adversas ocorrendo na rede, o que destaca a importância da atividade de ser executada de modo apropriado e permanente. Adicionalmente, a atividade é necessária no gerenciamento da quase totalidade de redes existentes, desde redes tradicionais até redes com características modernas, tais como as analisadas no capítulo 4.

A seção a seguir discorre sobre as características da atividade de *polling* e das funcionalidades de monitoração da rede e de coleta periódica de dados de desempenho. A seção posterior apresenta a arquitetura de *polling* distribuído, seguida pelas seções 7.3, 7.4, 7.5 e 7.6 que abordam, respectivamente, um cenário exemplo da atividade, o protótipo desenvolvido, os experimentos realizados com este e considerações acerca da arquitetura proposta. Por fim, a seção 7.6 apresenta as considerações finais.

7.1 *Polling* Distribuído de Recursos Gerenciados

A monitoração do estado e a coleta periódica de dados de desempenho dos recursos gerenciados representam importantes funcionalidades de gerenciamento de redes. Estas duas funcionalidades são realizadas através da coleta periódica de informações dos recursos, em uma operação denominada *polling*. Quando utilizada para *monitorar informações* de estado e de desempenho dos recursos gerenciados, a operação de *polling* deve ser realizada de modo a oferecer baixo tempo de resposta e pode ser associada à geração de notificações reportando eventos, que indicam alterações nos estados monitorados ou limiares de desempenho atingidos. Por outro lado, quando utilizada para a *coleta de dados de desempenho com fins estatísticos*, esta operação é associada ao armazenamento das informações de desempenho coletadas. Ambas as funcionalidades podem ser, ainda, combinadas: isto ocorre, por exemplo, quando uma informação de desempenho (*e.g.*, taxa de utilização de uma interface) é monitorada com o intuito de detectar em tempo real situações críticas na rede e, simultaneamente, tal informação é armazenada para avaliação de tendências.

Como detalhado em capítulo anterior (seções 5.3.2.2 e 5.3.2.3), as operações de *polling* possuem importantes limitações de escalabilidade e tolerância a falhas quando executadas através dos modelos de gerenciamento tradicionais. No ambiente de gerenciamento distribuído baseado em P2P proposto, contudo, a arquitetura de *polling* pode ser remodelada para fazer uso das potencialidades proporcionadas pelo novo ambiente, possibilitando grande distribuição das ações de *polling* e utilizando os serviços providos pelo ambiente.

Uma arquitetura para *polling* no ambiente de gerenciamento distribuído baseado em P2P é apresentada na seção a seguir. Como será visto, a arquitetura de *polling* proposta permite distribuir as ações de *polling* para um grande número de entidades de gerenciamento, numa abordagem na qual as operações de coleta de dados periódica são desempenhadas por um grande número de *entidades para controle dos recursos gerenciados* (CRG). Em situações em que a geração de notificações de eventos seja requerida, esta é realizada utilizando o *serviço de envio de notificações publish-subscribe baseado em P2P*. Por fim, se o armazenamento das informações coletadas for desejado, este é realizado fazendo uso do *serviço de armazenamento baseado em P2P* do ambiente de gerenciamento. Tais requisitos são controlados através de parâmetros de configuração do *polling*, permitindo utilizar a abordagem para ambas as funcionalidades.

7.2 Arquitetura do *Polling* Distribuído

A arquitetura de *polling* proposta divide as ações de *polling* em duas atividades principais, a fim de tratar de modo específico cada uma das duas etapas requeridas para o *polling*. Tais atividades compreendem a etapa que realiza a ***configuração do polling*** nas diversas *entidades CRG* e a etapa que realiza a ***execução periódica do polling***, desempenhada por *entidades CRG* que interagem com os recursos sendo monitorados. Ambas as atividades são executadas através de serviços de *grupos de peers* e composições destes serviços. Alguns serviços utilizados nestas composições são específicos para a funcionalidade de *polling*; outros serviços executam funções gerais e são também utilizados em outras atividades de gerenciamento.

A atividade de ***configuração do polling*** é realizada para que o *polling* dos recursos gerenciados desejados seja configurado no ambiente. Esta atividade pode ser realizada

antes de iniciar a *execução periódica do polling* ou ser realizada após o início da execução para alterar as informações e os recursos a serem monitorados, assim como para finalizar a monitoração de um ou mais recursos.

A *configuração do polling* pode ser requisitada, por exemplo, por uma *entidade para interface com o administrador da rede* (IA), na qual o administrador humano configura os parâmetros do *polling*, tais como equipamentos e informações a serem monitorados, freqüência de monitoração, geração ou não de eventos, armazenamento ou não no ambiente, início da monitoração, duração da monitoração, etc. Esta entidade interage com um *serviço de grupo* oferecido por *entidades para serviços de gerenciamento* (SG) e informa os parâmetros de *polling* definidos pelo administrador. O *serviço de grupo* das *entidades SG* identifica o *grupo de entidades para controle dos recursos gerenciados* (CRG) que é responsável por controlar cada recurso configurado no *polling* e interage com o serviço de *polling* destes grupos indicando a configuração de *polling* que eles devem executar. Cada serviço de *polling* dos *grupos de entidades CRG* executa as atividades para configuração em sua entidade. Por fim, se a entidade IA desejar receber eventos relacionados ao *polling* configurado, esta subscreve-se como assinante para tais eventos junto ao *serviço de envio de notificações* do ambiente, assim como outras aplicações e outros serviços interessados em tais eventos podem fazê-lo.

A atividade de *configuração do polling* é realizada através de uma composição de serviços, apresentada na figura 7.1. A notação utilizada nesta figura é derivada da notação proposta em (OBJECT MANAGEMENT GROUP, 2008): o diagrama de colaboração (representado pela elipse) representa uma composição de serviços e cada serviço é representado através de sua interface (esquematizado por um retângulo). O tipo da entidade que desempenha o serviço é indicado dentro da diretiva (simbolizada por << >>), assim como o suporte para invocação como serviço de grupo. Serviços que são desempenhados por todos os tipos de entidades (tal com o serviço de notificação) não possuem o tipo da entidade indicado.

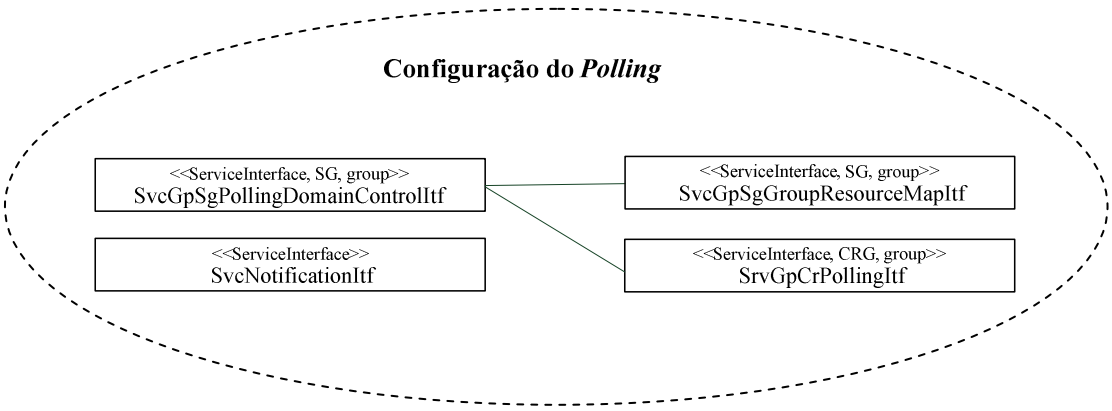


Figura 7.1: Composição de serviços para *configuração do polling*

A atividade de configuração é realizada para que todas as *entidades CRG* responsáveis pela monitoração dos recursos selecionados para *polling* sejam devidamente configuradas. Cada *entidade CRG*, por sua vez, será responsável por realizar o *polling* propriamente dito dos recursos controlados por ela, *polling* este que pode ser iniciado imediatamente após a configuração ou em um período definido durante a configuração.

A atividade de ***execução periódica do polling*** é, deste modo, realizada por cada *grupo de entidades CRG* responsável pelo *polling* de um ou mais recursos da rede. Esta atividade envolve requisitar periodicamente a informação dos equipamentos gerenciados de acordo com os intervalos configurados, comparar os valores recebidos com limiares pré-definidos, gerar ações quando estes limiares forem ultrapassados (se isto estiver configurado nos parâmetros do *polling*), assim como armazenar estes valores (se isto estiver configurado nos parâmetros do *polling*).

A figura 7.2 esquematiza a composição de serviços realizada pela *execução periódica do polling*. Seguindo a mesma notação da figura anterior, esta figura contém ainda a diretiva `<<local>>`, que representa os serviços com *dependência local*: estes serviços, mesmo que suportem a execução através de *grupos de peers*, serão, nesta composição, invocados localmente pelo serviço consumidor, como definido na seção 5.2.5. Embora invocados com *dependência local*, a definição dos serviços *SvGpCrMapping* e *SvGpCrSnmp* como serviços individuais foi projetada para permitir a reutilização destes serviços para outras atividades de gerenciamento, assim como para permitir flexibilidade aos serviços consumidores: o serviço *SvGpCrSnmp*, por exemplo, só é empregado quando o recurso for gerenciado através do protocolo SNMP, e um serviço diferente deve ser invocado quando outros protocolos estiverem sendo utilizados.

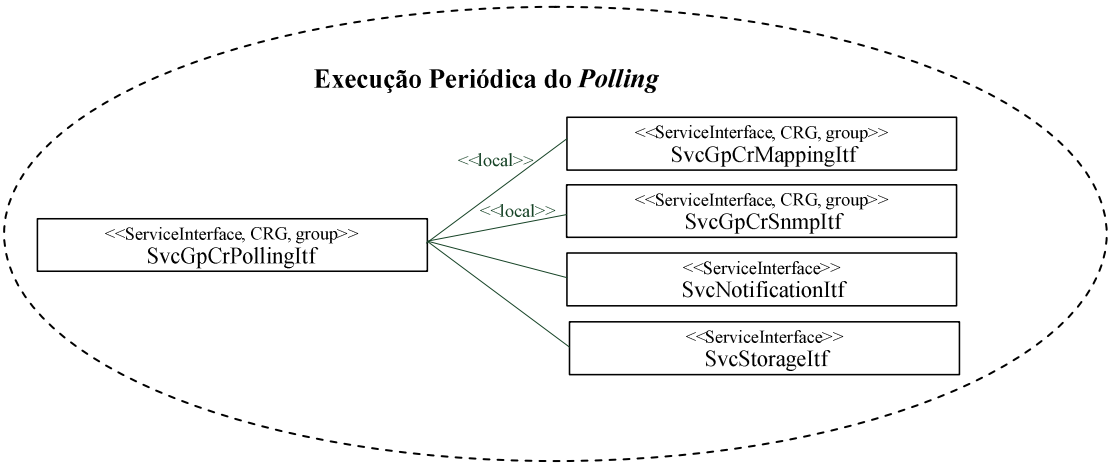


Figura 7.2: Composição de serviços para a *execução periódica do polling*

Os serviços participantes das composições são:

- *SvGpSgGroupResourceMap*: executado por *grupos de peers SG*, pertence à categoria de serviços e aplicações de gerenciamento. Este serviço é responsável por informar o *grupo de peers CRG* encarregado de controlar cada recurso gerenciado específico. O modo como esta informação é obtida não é definido na composição: a interface do serviço apenas especifica que este serviço será responsável por fornecer esta informação ao serviço invocador. De acordo com a infra-estrutura P2P utilizada e a abordagem utilizada pelo ambiente para controle dos recursos gerenciados, esta informação pode ser projetada de diferentes modos. Estes incluem o uso de serviços de busca de recursos disponibilizados pela infra-estrutura P2P (numa abordagem na qual os equipamentos controlados por cada *entidade CRG* são reportados por esta como sendo recursos que ela possui) e o uso de serviços de armazenamento (numa abordagem na qual cada *entidade CRG*

armazena no ambiente P2P os equipamentos que controla e tais informações são compartilhadas com o serviço de mapeamento). Mecanismos para *cache* destas informações junto às entidades responsáveis pelo serviço de mapeamento também podem ser empregados, sendo estes complementados com a publicação de eventos por *entidades CRG* reportando alterações na lista de recursos controlados por elas. O serviço de mapeamento dos recursos não é específico para a funcionalidade de *polling*, sendo utilizado também para as demais funcionalidades que necessitam interagir diretamente com os equipamentos gerenciados (*e.g.*, configuração dos equipamentos, execução de testes nos equipamentos, etc.).

- *SvGpSgPollingDommainControl*: executado por *grupos de peers SG*, pertence à categoria de serviços e aplicações de gerenciamento. Este serviço é responsável por (*i*) interagir com o serviço *SvGpSgGroupResourceMap* a fim de obter os *grupos de peers CRG* encarregados dos recursos configurados para *polling*; (*ii*) interagir com os serviços de tais *grupos de peers* informando os parâmetros configurados para *polling*. Este serviço é específico para a funcionalidade de *polling*.

- *SvGpCrMapping*: executado por *grupos de peers CRG*, pertence à categoria de serviços e aplicações de gerenciamento. Este serviço é responsável pelo mapeamento do objeto expresso de acordo com o modelo de informação utilizado no ambiente de gerenciamento para o objeto no modelo de informação seguido pelo protocolo de gerenciamento suportado pelo recurso sendo gerenciado. Este serviço não é específico para a funcionalidade de *polling*, sendo também utilizado pelas outras funcionalidades que interagem diretamente com os equipamentos gerenciados.

- *SvGpCrPolling*: executado por *grupos de peers CRG*, pertence à categoria de serviços e aplicações de gerenciamento. Este serviço é responsável por executar periodicamente o *polling* dos recursos a partir dos parâmetros recebidos e do mapeamento obtido com a invocação do serviço *SvGpCrMapping*, incluindo: (*i*) consultar o valor do objeto do recurso gerenciado através do serviço correspondente (*e.g.*, serviço *SvGpCrSnmp*); *(ii*) comparar o valor do objeto recebido com os limiares estabelecidos para ele, enviando notificações através do serviço *SvNotification* quando os limiares forem ultrapassados (se esta opção estiver habilitada nos parâmetros recebidos para o *polling*); (*iii*) armazenar o valor no ambiente de gerenciamento através do serviço *SvStorage* (se esta opção estiver habilitada nos parâmetros recebidos para o *polling*). Este serviço é específico para a funcionalidade de *polling*.

- *SvGpCrSnmp*: executado por *grupos de peers CRG*, pertence à categoria de serviços e aplicações de gerenciamento. Este serviço é responsável por requisitar os valores de objetos nos recursos gerenciados utilizando o protocolo SNMP. Este serviço somente será utilizado se o recurso gerenciado utilizar este protocolo de gerenciamento. Este serviço não é específico para a funcionalidade de *polling* e será utilizado por outras funcionalidades que interagem com equipamentos gerenciados através do protocolo SNMP.

- *SvNotification*: pertence à categoria de serviços estruturais do ambiente. Este serviço é responsável por enviar notificações de eventos, seguindo o mecanismo de envio de eventos *publish-subscribe* baseado em P2P descrito no capítulo 6.
- *SvStorage*: pertence à categoria de serviços estruturais do ambiente. Este serviço é responsável por armazenar as informações no ambiente de gerenciamento.

As interações entre os elementos envolvidos na ***configuração do polling*** para um cenário exemplo são apresentadas na figura 7.3. Neste cenário, as instâncias de serviços *SvGpCrPolling* são resultado dos *grupos de peers CRG* obtidos na interação com o serviço *SvGpSgGroupResourceMap*: neste exemplo, duas instâncias deste serviço, correspondentes aos *grupos GCR001 e GCR002*. Além disso, no exemplo, a aplicação que requisita o *polling* subscreve-se como assinante junto ao serviço *SvNotification* para recebimento de notificações de eventos relacionados.

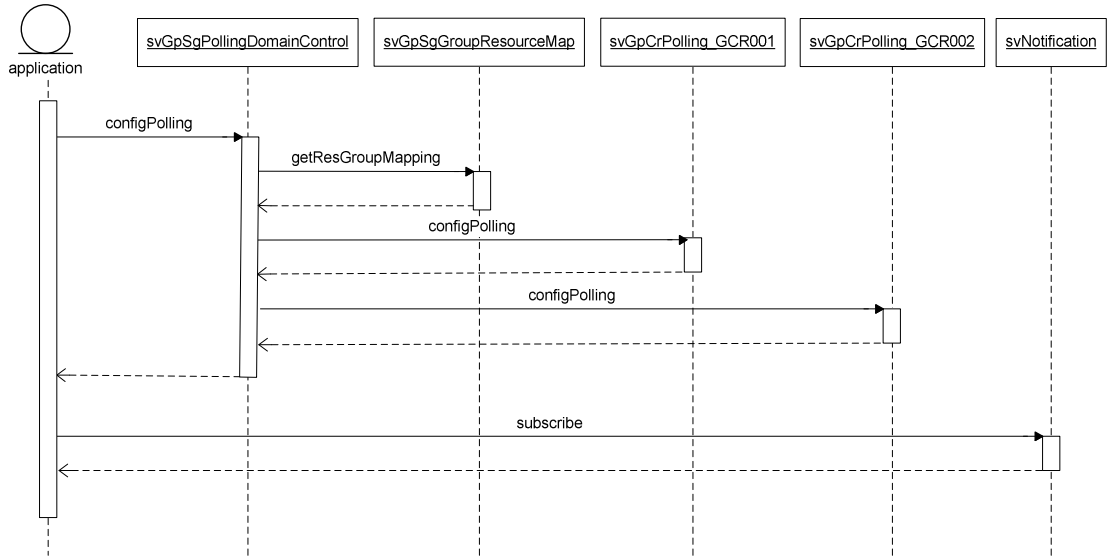


Figura 7.3: Interações para a configuração do *polling*

Dando seqüência ao cenário exemplo da figura acima, após os serviços *SvGpCrPolling* dos *grupos GCR001 e GCR002* terem sido configurados para *polling*, eles iniciarão, imediatamente ou em período definido, a monitoração dos recursos selecionados. A figura 7.4 apresenta as interações realizadas periodicamente para a ***execução do polling***. Estas interações são realizadas por cada *grupo de peers CRG* configurado para *polling* na etapa de configuração: nesta figura, são apresentadas as interações do *grupo GCR001*.

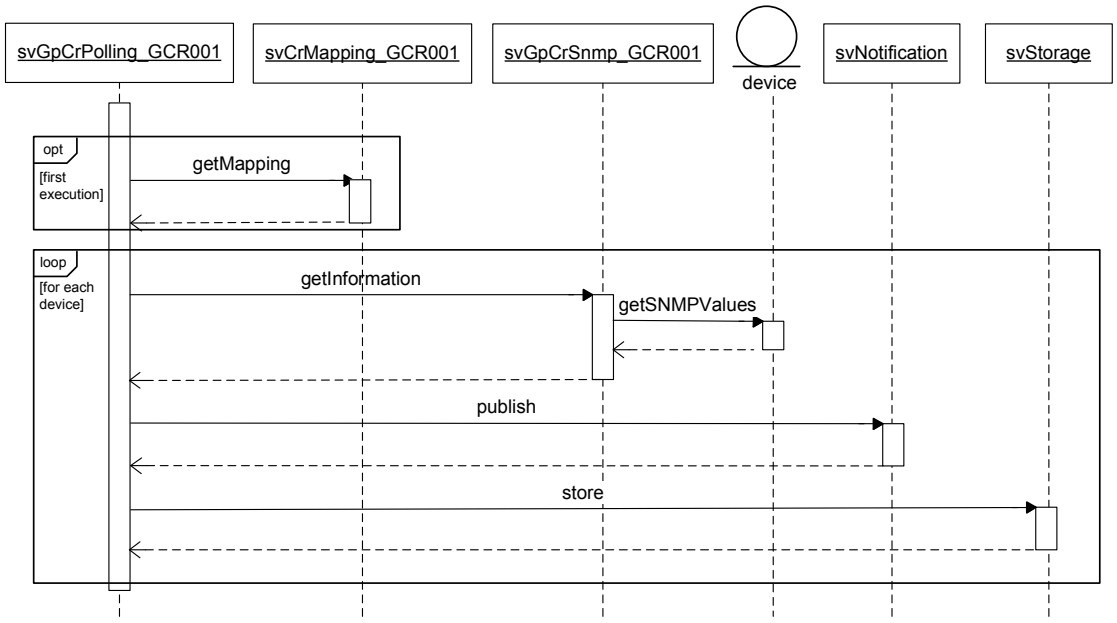


Figura 7.4: Interações na execução periódica do *polling*

A arquitetura de *polling* foi projetada para permitir distribuir as ações envolvidas no *polling* periódico para um grande número de entidades de gerenciamento. Com a abordagem, um elevado número de *entidades CRG* pode ser empregado para as atividades periódicas, diferindo, deste modo, de ambientes de gerenciamento centralizados ou fracamente distribuídos, nos quais uma única ou poucas entidades são responsáveis por monitorar um elevado número de recursos. A distribuição proporcionada nesta abordagem permite que a entidade de gerenciamento encarregada da consulta periódica às informações seja posicionada mais próxima aos recursos gerenciados. Estas características permitem restringir o tráfego de gerenciamento aos enlaces próximos aos recursos sendo monitorados, sem concentrar o tráfego de gerenciamento em nenhum ponto da rede.

Cada atividade de *configuração do polling*, individualmente, possui uma estrutura parcialmente hierárquica segundo o modo como as ações são realizadas, já que um único serviço é responsável por invocar parte dos demais para que a configuração seja concluída. Considerando o ambiente completo, por outro lado, podem ocorrer múltiplas configurações, invocadas por diferentes entidades, sem a existência de uma entidade gerente única responsável pelo gerenciamento. Deste modo, múltiplos serviços e aplicações podem configurar o *polling* para recursos, inclusive serviços e aplicações em entidades pertencentes a diferentes domínios administrativos. Cada *grupo CRG* responsável pelo *polling* de recursos, por sua vez, combina as solicitações de *polling* recebidas para a mesma informação de cada recurso, de modo que, sempre que possível, uma única consulta será realizada atendendo às múltiplas configurações recebidas.

A *execução do polling periódico* propriamente dito, por sua vez, é realizada em paralelo pelos múltiplos *grupos de peers CRG* dispostos no ambiente. Tais *peers*, ao identificarem a ocorrência de situações que representam eventos nas informações monitoradas (*e.g.*, uma mudança no estado de uma informação ou um limiar ultrapassado), publicam uma notificação no *serviço de envio de notificações* (se isto estiver sido configurado), e estas são repassadas para todas as entidades que se

subscreveram para seu recebimento, que podem incluir não apenas as entidades que invocaram a configuração, como também entidades adicionais.

7.3 Cenário Exemplo

Um cenário exemplo de como a atividade de *polling* pode ser realizada de acordo com a arquitetura proposta é apresentado na figura 7.5. Este cenário é composto por redes pertencentes a dois departamentos (D1 e D2), nas quais diversos serviços e aplicações de gerenciamento estão sendo executados, incluindo um serviço para controle do estado e da topologia da rede, um serviço para avaliar o desempenho da rede, um serviço para gerenciamento da infra-estrutura de rede para uma grade computacional e uma aplicação *dashboard* para visualização de eventos. Cada rede possui vários equipamentos, alguns contendo *peers* do ambiente de gerenciamento, outros não. Diversos *grupos de peers* estão presentes no ambiente. Os *grupos GCR* são utilizados para representar os *grupos de peers CRG*, responsáveis pelo controle de recursos na rede, que foram assim configurados (organizados conforme as áreas hachuradas)*: grupo GCR001*, responsável pelo controle do roteador RA, do switch SA e dos demais dispositivos na rede 1; *grupo GCR002*, responsável pelo controle do switch SB e dos servidores presentes na rede 2; *grupo GCR003*, responsável pelo controle do roteador RB, do switch SC e dos demais servidores da rede 3; *grupo GCR004*, responsável pelo controle do switch SD e dos demais servidores na rede 4; *grupo GCR005*, responsável pelo controle do roteador RC, do switch SE e dos demais equipamentos na rede 6.

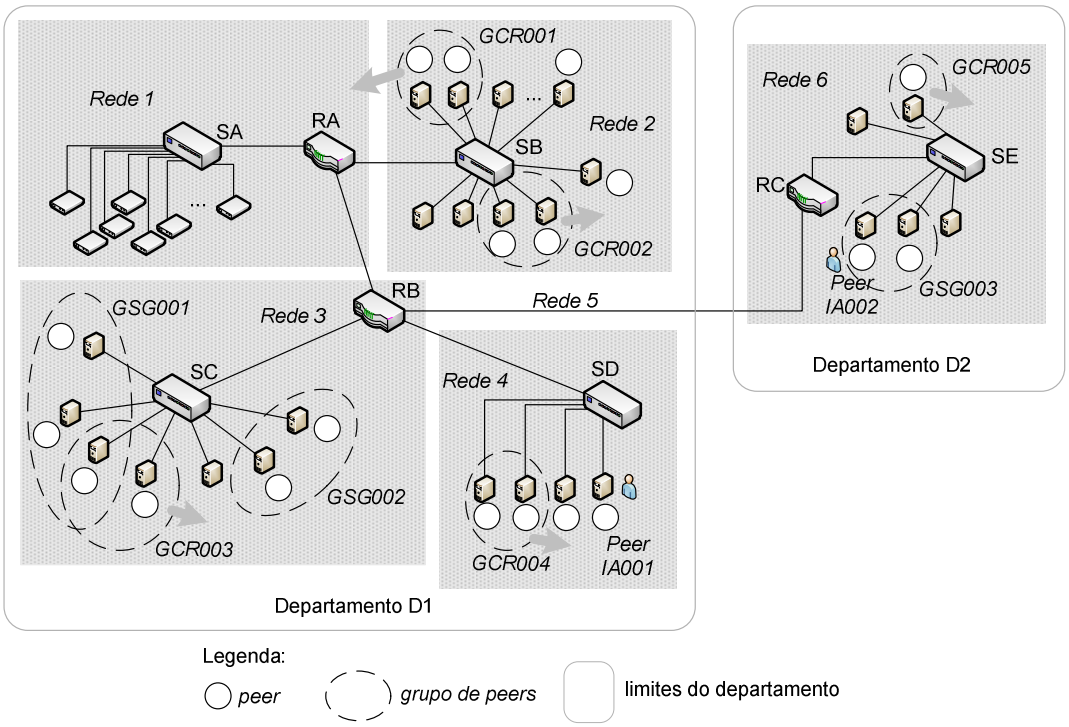


Figura 7.5: Cenário exemplo de *polling* segundo a arquitetura proposta

Na figura, alguns *grupos de peers SG* foram também dispostos como exemplo. O *grupo GSG001* executa um serviço para controle do estado e da topologia da rede, responsável por controlar mapas que apresentam o estado atualizado dos recursos, que são armazenados no serviço de armazenamento do ambiente para serem utilizados por

outros serviços e por aplicações. Assim, este serviço requisita a *configuração de polling* para os recursos da rede 1, rede 2, rede 3 e rede 4, informando nos parâmetros de *polling* a monitoração de determinadas informações de gerenciamento e a publicação de notificações sempre que alterações no estado destas informações em algum dos recursos forem detectadas. Este serviço subscreveu-se ainda no *serviço de envio de notificações* como assinante para tais eventos. Deste modo, após sua *configuração de polling* ter sido solicitada e devidamente configurada no ambiente, os *grupos GCR001, GCR002, GCR003 e GCR004* passam a *executar o polling periódico* de cada um dos recursos controlados por eles. Ao detectar uma mudança de estado, um evento é publicado pelo *grupo GCR* correspondente, e o *serviço de envio de notificações* transmite tal notificação para o serviço do *grupo GSG001* (assinante de tais notificações).

O *grupo GSG002*, por sua vez, executa um serviço para avaliar o desempenho e as tendências nos dispositivos na rede 1. Assim, este serviço requisita ao ambiente de gerenciamento a *configuração do polling* para os dispositivos da rede 1, configurando nos parâmetros de *polling* a monitoração de algumas informações e o armazenamento das informações coletadas. Deste modo, após esta configuração ter sido solicitada e devidamente configurada no ambiente, o *grupo GCR001*, responsável pelo controle destes recursos, passa a incluir em seu *polling periódico* a coleta das novas informações solicitadas (se estas não forem coincidentes com as já requisitadas pelo *grupo GSG001* para tais recursos), armazenando as informações coletadas no *serviço de armazenamento* do ambiente. O *serviço GSG002*, quando desejar obter as informações coletadas, as obtém diretamente do *serviço de armazenamento* do ambiente.

O *grupo GSG003*, por sua vez, executa um serviço que necessita identificar alterações críticas no estado ou no desempenho de certos enlaces e servidores do departamento D1, assim como informações de recursos de sua rede (rede 6, departamento D2). Estas informações são utilizadas por serviços de uma grade computacional localizados na rede 6, que necessitam destas informações para suspender, se necessário, o escalonamento de *jobs* em certos servidores da rede 2. Assim, o serviço no *grupo GSG003* requisita ao ambiente de gerenciamento a *configuração do polling* para os switch SE e SB, os roteadores RC, RB e RA, e alguns servidores na rede 2 que podem ser utilizados para a execução de *jobs* da grade computacional. Os parâmetros de *polling* indicam algumas informações para serem monitoradas e a publicação de notificações sempre que alterações no estado destas informações forem detectadas. Este serviço subscreveu-se ainda no *serviço de envio de notificações* como assinante para tais eventos. Deste modo, após a configuração ter sido solicitada e devidamente configurada no ambiente, o *grupo GCR005* passa a *executar o polling periódico* dos recursos SE e RC, e os *grupos GCR001, GCR002 e GCR003* incluem em seu *polling periódico* a coleta das novas informações solicitadas (se não forem coincidentes com as já requisitadas anteriormente). Ao detectar uma mudança de estado, o evento é publicado pelo *grupo GCR* correspondente, e o *serviço de envio de notificações* transmite tal notificação para o serviço do *grupo GSG003* (assinante de tais notificações), assim como para outros serviços assinantes.

Por fim, o *peer IA001* executa uma aplicação *dashboard* que fornece a visualização dos eventos das redes do departamento D1 associados a alterações de estado e topologia da rede. Este *peer*, assim, subscreve-se como assinante no *serviço de envio de notificações* para recebimento de tais eventos. Deste modo, quando tais eventos forem publicados pelos serviços de *polling periódico* nos *grupos GCR001, GCR002, GCR003 e GCR004*, além do serviço do *grupo GSG001*, também o *peer IA001* irá recebê-los.

7.4 Protótipo Implementado

Um protótipo da arquitetura de *polling* proposta foi implementado para avaliar o mecanismo. Este protótipo foi implementado utilizando a infra-estrutura JXTA (GONG, 2001) (TRAVERSAT et al, 2003) (ARNEDO-MORENO; HERRERA-JOANCOMARTI) e fazendo uso do o *framework* ManP2P (PANISSON, 2007) (PANISSON; ROSA; MELCHIORS; GRANVILLE; ALMEIDA; TAROUCO, 2006).

A infra-estrutura JXTA é uma infra-estrutura P2P de propósito geral que se tornou um dos principais ambientes de testes para aplicações P2P (ARNEDO-MORENO; HERRERA-JOANCOMARTI, 2009), tendo como importantes características: ser uma infra-estrutura com código aberto e que faz uso de um conjunto de protocolos abertos; não ser dependente de plataforma específica; e ter sido projetada para poder ser implementada em qualquer equipamento (incluindo equipamentos heterogêneos tais como sensores, computadores desktop, servidores de *datacenter*, sistemas de armazenamento e roteadores de rede) (GONG, 2001), o que aumenta a possibilidade de *peers* poderem ser adicionados diretamente em um maior número de equipamentos de rede. Além disto, a utilização desta infra-estrutura para o desenvolvimento deste protótipo tem como benefícios esta infra-estrutura ser utilizada por outros trabalhos do grupo de pesquisa, incluindo (PANISSON, 2007), (ROSA, 2007), (SANTOS, 2008), (MARQUEZAN et al, 2008), e o fato desta infra-estrutura já estar integrada a um *framework* desenvolvido em pesquisa dentro do grupo (ManP2P) (PANISSON, 2007) (PANISSON; ROSA; MELCHIORS; GRANVILLE; ALMEIDA; TAROUCO, 2006), já empregado em outras pesquisas do grupo (SANTOS, 2008) (MARQUEZAN et al, 2008).

O *framework* ManP2P utiliza a linguagem Java e, como visto, a infra-estrutura JXTA, e segue uma arquitetura baseada em componentes. O *framework* ManP2P provê componentes de software denominados *Componentes de Gerenciamento* para que funcionalidades de gerenciamento sejam projetadas e implementadas em *peers*. Estes componentes são utilizados para desenvolver serviços de *peers* ou de *grupos de peers*, e são herdados para o desenvolvimento de componentes específicos. Os *Componentes de Gerenciamento* são controlados através de um *Container*.

Como visto, os serviços representados nas composições de *polling* pertencem à categoria dos serviços e aplicações de gerenciamento e à categoria de serviços estruturais do ambiente. Cada serviço pertencente à primeira categoria, tais como os serviços *SvGpSgPollingDommainControl*, *SvGpSgGroupResourceMap* e *SvGpCrPolling*, foi implementado através de um *Componente de Gerenciamento*, que foi herdado e estendido para a implementação das funcionalidades específicas do serviço. Os serviços pertencentes à segunda categoria, por sua vez, representam uma funcionalidade do ambiente de gerenciamento, estando tipicamente distribuídos em todos os *peers* do ambiente. Na atual versão do protótipo, o foco concentrou-se na execução do *polling* através de uma abordagem fortemente distribuída, incluindo a arquitetura seguida para execução desta funcionalidade, os serviços e suas interações. Em virtude disto, o serviço de notificação foi implementado através de um mecanismo *publish-subscribe* básico, implementado através de um *Componente de Gerenciamento*, em que um serviço é iniciado para cada *grupo de peers CRG*, servido por um único *peer*. O serviço de armazenamento, por sua vez, foi implementado fazendo uso do sistema de armazenamento de arquivos do próprio *peer*, também implementado através de um *Componente de Gerenciamento*, em que também um serviço é iniciado para

servir cada *grupo de peers CRG*. Por fim, o serviço *SvGpSgGroupResourceMap* foi implementado armazenando as informações de mapeamento de modo fixo diretamente no *peer* com tal serviço.

A arquitetura baseada em componentes e serviços do ambiente de gerenciamento torna possível que cada serviço seja aprimorado de modo independente e transparente para os demais serviços da composição, desde que a interface do serviço seja respeitada. No protótipo desenvolvido, cada serviço foi implementado atribuindo um único *peer* para cada grupo. Funcionalidades de distribuição de carga e de tolerância a falhas entre membros do grupo não foram consideradas. A identificação de objetos empregada no SNMP foi utilizada para expressar os objetos no modelo de informação do ambiente: em versões futuras, esta identificação pode ser substituída alterando o serviço *SvGpCrMapping*.

Os componentes implementados e suas interações são descritos na figura 7.6, que também segue uma notação derivada da proposta em (OBJECT MANAGEMENT GROUP, 2008).

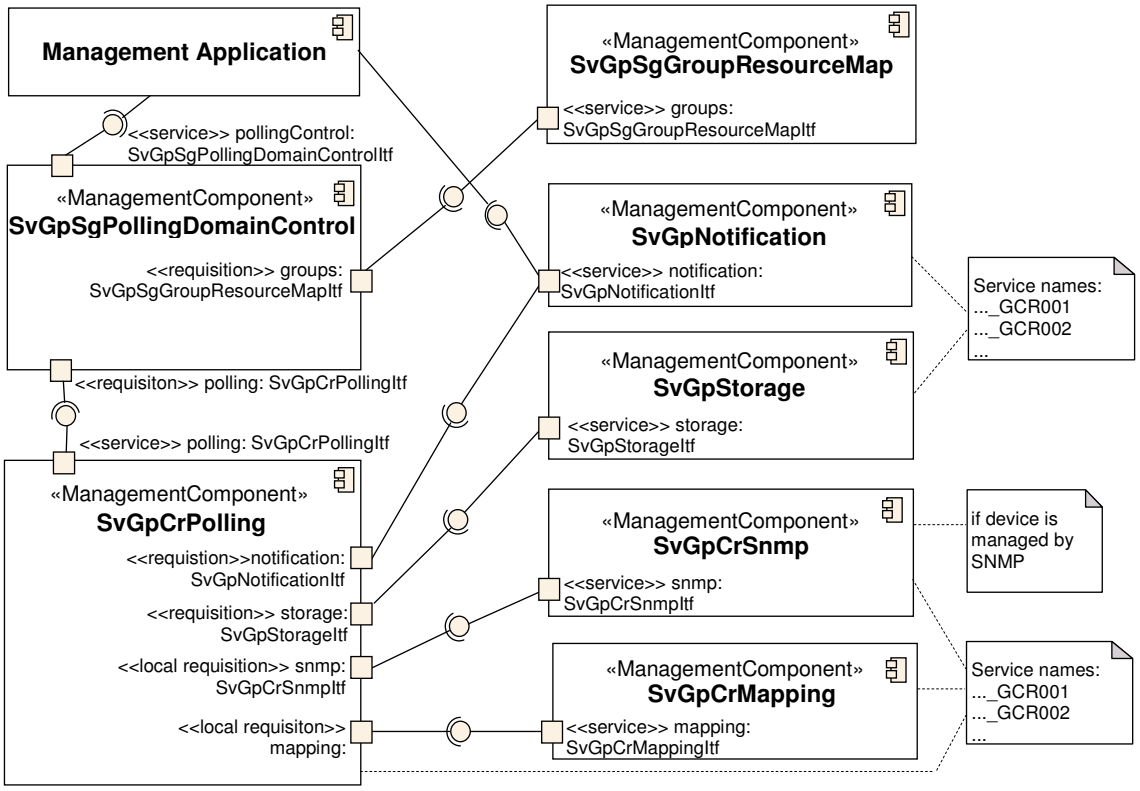


Figura 7.6: Componentes utilizados no *polling*

7.5 Experimentos Realizados

Esta seção discute os experimentos realizados para avaliar a arquitetura de *polling* proposta segundo alguns parâmetros de desempenho. Dois conjuntos de experimentos foram realizados, cada qual enfocando uma das atividades envolvidas no *polling*.

O **primeiro conjunto de experimentos** analisou a atividade de ***configuração do polling***. Esta avaliação foi realizada utilizando onze máquinas virtuais (*VM*), cada uma com 128 Mb de RAM. As onze VMs foram executadas em um computador Core2 com

2,4 GHz. Cada VMs hospedou um *peer*, da seguinte forma: uma VM com um *peer* com um serviço de autenticação (disponibilizado pelo *framework* ManP2P), uma VM com um *peer* com o serviço *SvGpSgPollingDomainControl*, uma VM com um *peer* com o serviço *SvGpSgGroupResourceMap* e oito VMs, cada qual com um *peer* com os serviços *SvGpCrPolling*, *SvGpCrSnmp* e *SvGpCrMapping* para um *grupo CRG* correspondente (*e.g.*, *grupos GCR001, GCR002*, ...), além dos serviços *SvNotification* e *SvStorage*. Como visto, os serviços do *polling* são disponibilizados através de *serviços de grupo*, porém, nesta avaliação, apenas um *peer* foi designado para representar cada grupo. As *configurações de polling* foram invocadas por uma aplicação em um *peer* separado, sendo executado em um computador Pentium IV com Windows XP.

Este primeiro conjunto de experimentos objetivou analisar a escalabilidade da atividade de configuração do *polling*, variando o número de *peers*/*grupos CRG* sendo configurados pela atividade (1, 2, 4 e 8 *grupos CRG*). Cada *grupo CRG* foi configurado para realizar o *polling* de 64 agentes SNMP, resultando em 512 agentes SNMP sendo configurados para *polling* quando 8 *grupos CRG* foram utilizados. Dois parâmetros de desempenho foram medidos: o **tempo de resposta para configurar o *polling* para o conjunto completo de agentes SNMP em todos os *peers CRG* correspondentes** (medido na aplicação que requisitou a *configuração do polling*) e o **tráfego médio gerado para a configuração de todos os *peers* envolvidos** (medido utilizando a ferramenta *tcpdump* (TCPDUMP, 2009)). O tempo de resposta foi avaliado nos experimentos em virtude da importância de verificar-se se o período transcorrido para configurar o *polling* como uma atividade fortemente distribuída é viável e apropriado para ser utilizado em operações de gerenciamento de redes, como discutido abaixo. O tráfego de rede gerado, por sua vez, necessita ser verificado uma vez que, se um alto volume de tráfego é gerado para configurar a atividade de forma distribuída, este pode gerar limitações para a utilização da arquitetura.

As figuras 7.7 e 7.8 apresentam, respectivamente, o tempo de resposta médio e o tráfego de rede gerado médio resultante de 30 amostras executadas para cada número de *grupos CRG* (1, 2, 4 e 8).

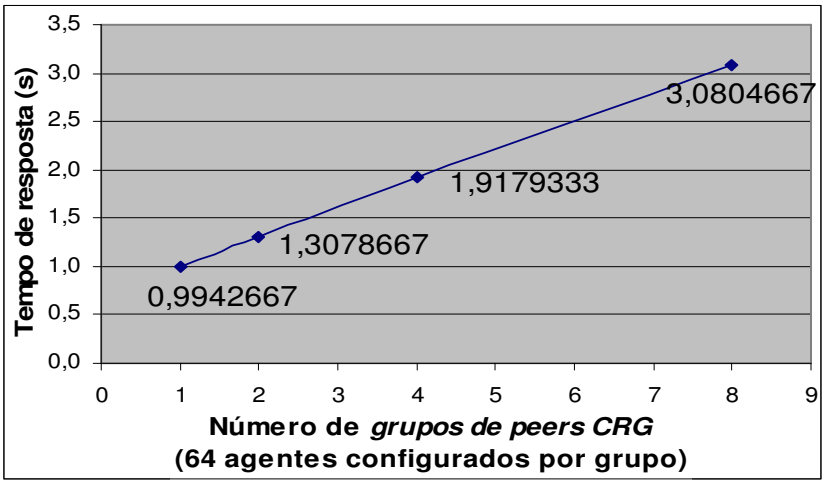


Figura 7.7: Tempo de resposta médio na configuração do *polling*

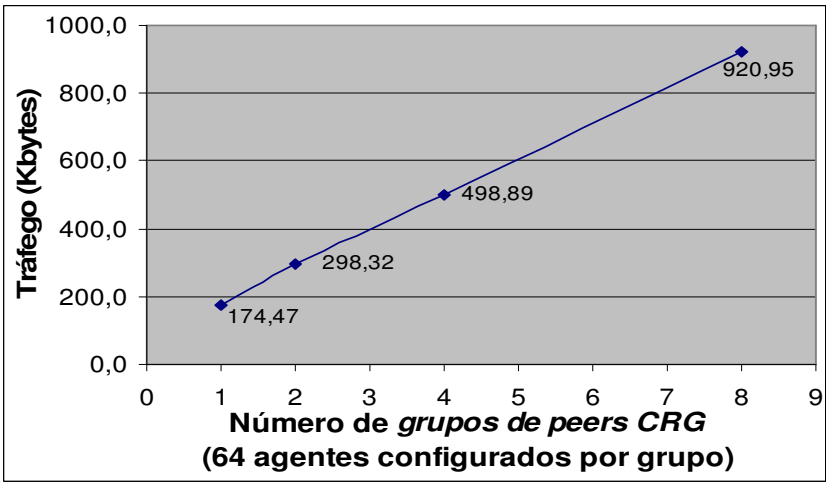


Figura 7.8: Volume médio de tráfego na configuração do *polling*

Como pode ser visto nas figuras acima, ambos os resultados são funções lineares do número de *grupos CRG* sendo configurados. A atividade de *configuração do polling* em um ambiente de gerenciamento é tipicamente realizada poucas vezes. Contudo, uma rápida *configuração do polling* para novos equipamentos e objetos de gerenciamento é importante para permitir que os administradores sejam capazes de analisar novas informações da rede em situações especiais ou críticas. Tal requisito pode se tornar uma limitação para uma arquitetura de *polling* fortemente distribuída como a proposta, quando comparada com arquiteturas centralizadas ou fracamente distribuídas. Os experimentos, contudo, mostram que a arquitetura proposta suporta tal rápida configuração, como requerido, resultando em aproximadamente 3,08s para a configuração do polling de 512 equipamentos, monitorados através de 8 *grupos CRG*. Além disto, *grupos CRG* são configurados seqüencialmente pelo algoritmo implementado no serviço *SvGpSgPollingDomainControl*: deste modo, em situações onde uma configuração ainda mais rápida for necessária, tal algoritmo pode ser aprimorado com a paralelização das interações com os *grupos CRG*. Esta paralelização pode resultar, por exemplo, com a utilização de mecanismo para 4 *grupos CRG* serem configurados em simultâneo, em 512 equipamentos sendo configurados para *polling* em aproximadamente 1,3s, ou, com a paralelização de 8 *grupos CRG*, em aproximadamente 1s para o mesmo número de equipamentos.

Em relação ao volume de tráfego gerado, os valores obtidos estão relacionados com o uso da infra-estrutura JXTA, que usa mensagens em formato texto e contém um *overhead* para o tráfego de controle JXTA (HALEPOVIC; DETERS, 2003). Embora tenha sido encontrado um alto volume de tráfego para a configuração de um único *grupo CRG* (*polling* de 64 agentes), o tráfego de rede apresenta um crescimento menor com a inclusão de mais *grupos CRG*. Como previamente discutido, a atividade de *configuração do polling* é realizada somente poucas vezes, e, assim, o volume de tráfego gerado causa um impacto limitado nos enlaces da rede. Em análises futuras, tais parâmetros podem ser avaliados utilizando compactação das mensagens XML JXTA. Adicionalmente, a arquitetura de *polling* pode ser avaliada utilizando outras infra-estruturas P2P além do JXTA, a fim de investigar infra-estruturas P2P que consomem menor largura de banda.

O **segundo conjunto de experimentos** analisou a *execução do polling periódico* realizada por um *grupo de peers CRG*. A avaliação foi realizada utilizando 4 VMs, cada

qual com 128 Mb de RAM, instaladas em um computador Core2 com 2,33 GHz. Cada VM hospedou um *peer*: uma VM com um *peer* com um serviço de autenticação, uma VM com um *peer* com o serviço *SvGpSgPollingDomainCtrl*, uma VM com um *peer* com o serviço *SvGpSgGroupResourceMap* e uma VM com um *peer* responsável pela execução do *polling* periódico propriamente dito, contendo o serviço *SvGpCrPolling* que invoca diretamente os serviços *SvGpCrMapping e SvGpCrSnmp*, além dos serviços *SvGpNotification* e *SvGpStorage* iniciados para tal *grupo CRG*.

Este conjunto de experimentos testou a escalabilidade da *execução de polling periódico* como uma função do número de equipamentos consultados por um *grupo CRG*. Dois parâmetros de desempenho foram medidos. O primeiro analisou o **tempo de resposta para executar o *polling* do conjunto completo de equipamentos**, utilizando uma única *thread* Java (todos os agentes consultados seqüencialmente). O segundo analisou o **volume de tráfego gerado nos enlaces da rede** para recuperar a informação do equipamento utilizando SNMP. O tráfego do serviço de armazenamento não foi considerado, já que esta implementação enfocou os serviços de *polling* e o *serviço de armazenamento* estava disponível para ser invocado diretamente. Notificações não foram geradas e, deste modo, o tráfego destas não foi incluído.

As figuras 7.9 e 7.10 apresentam os resultados de tais experimentos, requisitando os objetos SNMP *ifInOctects* e *IfOutOctects* de uma interface de cada agente.

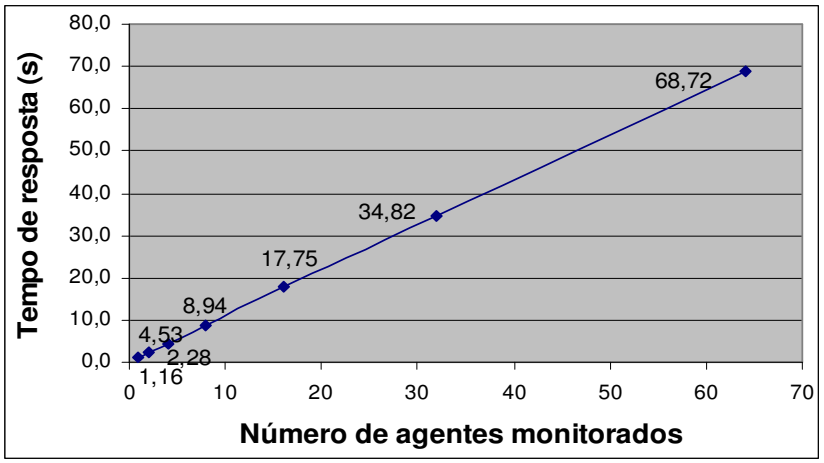


Figura 7.9: Tempo de resposta médio na execução do *polling* periódico

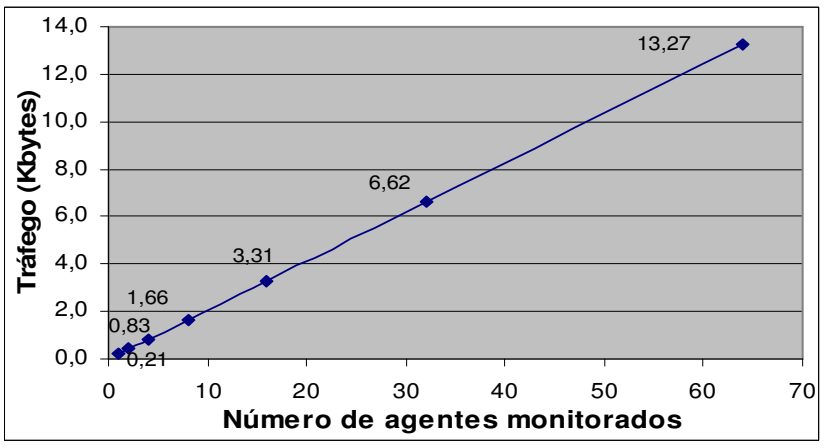


Figura 7.10: Volume médio de tráfego na execução do *polling* periódico

Como *um único peer/grupo CRG* foi utilizado no experimento, o tempo de resposta e o tráfego gerado são funções lineares do número de agentes monitorados. A inclusão de novos agentes SNMP para monitoração através de *grupos CRG adicionais* resultará na *paralelização do tempo de resposta*, já que cada *grupo CRG* irá executar o *polling* apenas dos agentes pelos quais é responsável. Assim, mesmo com a inclusão de um grande número de *grupos CRG*, como suportado e esperado na arquitetura proposta, o tempo de resposta para a monitoração de um número elevado de agentes não será afetado, independente do número de *grupos CRG* incluídos, já que o polling é executado em paralelo para cada grupo. Em relação ao volume de tráfego gerado por *grupos CRG adicionais*, o posicionamento dos *grupos de peers CRG* e o *mapeamento recurso gerenciado-grupo CRG* (reportado pelo *serviço de grupo SvGpSgGroupResourceMap*) de acordo com a topologia da rede pode permitir que o tráfego gerado pelo *polling* periódico seja *restrito aos enlaces próximos aos recursos gerenciados*. Além disto, conforme a disposição dos *grupos CRG* empregada, possivelmente o tráfego de *polling* em cada enlace da rede conterá apenas o tráfego de um único *grupo CRG*, *eliminando a concentração do tráfego existente em arquiteturas centralizadas ou fracamente distribuídas e reduzindo o tráfego gerado nos enlaces da rede*.

Neste conjunto de experimentos, uma avaliação adicional foi realizada a fim de identificar os gargalos do tempo de resposta para consulta aos agentes SNMP. Esta avaliação demonstrou que a operação de fechamento do *socket* levou um tempo médio de 1.002 milisegundos versus o tempo médio total de 1.074 milisegundos para manusear todo o processamento de *polling* de um agente. Assim, a fim de aprimorar o tempo de resposta, uma análise mais aprofundada deste tópico pode ser realizada. Além disto, o tempo de resposta pode ser reduzido aumentando o *pool de threads* Java no serviço *SvGpCrPolling*. Experimentos iniciais executados para consultar 64 agentes com 5 *threads* Java resultaram num tempo de resposta médio de 14.594 milisegundos (30 amostras), versus 68.720 milisegundos para apenas uma *thread*. O número de *threads* no *pool* pode ser ajustado de modo independente em cada *peer*, de acordo com os recursos disponíveis no *peer*. Análises futuras podem também enfocar os serviços estruturais do ambiente, integrando e avaliando os serviços de armazenamento e envio de notificações, assim como o serviço de mapeamento.

7.6 Considerações Acerca da Arquitetura Proposta

A arquitetura de *polling* proposta possibilita uma forte distribuição das ações periódicas de coleta de dados de equipamentos gerenciados, que são realizadas na arquitetura através de *grupos de peers CRG*. A abordagem permite ainda que a topologia da rede seja explorada para que *grupos de peers CRG* e mapeamentos *equipamento gerenciado-grupo CRG* sejam definidos de modo que os recursos gerenciados sejam consultados periodicamente por entidades muito mais próximas do que aquelas empregadas em abordagens centralizadas ou fracamente distribuídas. Como conseqüência, o processamento e o tráfego gerado nos enlaces de comunicação rede podem ser reduzidos.

A arquitetura de *polling* proposta tem como importante característica permitir organizar a monitoração de cada recurso da rede em mesmo *grupo de entidades CRG*, concentrando neste grupo o *polling* requisitado por diferentes serviços de rede e eliminando a realização de múltiplas consultas para um mesmo recurso: a consulta periódica das informações é realizada uma única vez pelas *entidades CRG* localizadas

próximas aos equipamentos e responsáveis pelo gerenciamento destes. Um exemplo é a monitoração de informações de rede exemplificada na seção 7.3. Em tal exemplo, diferentes serviços (*i.e.*, o serviço para controle do estado e da topologia da rede executado pelo *grupo GSG001* e serviços de uma grade computacional executados pelo *grupo GSG003*) requisitam a monitoração de equipamentos da rede 2. Estes equipamentos são monitorados unicamente pelas *entidades do grupo GCR002*, através do serviço *SvcGpCrPolling* executado por estas, e todos os serviços requisitantes fazem uso destas informações. Tal organização ocorre, igualmente, para requisições de monitoração de entidades presentes em outros domínios administrativos. A arquitetura empregada permite ainda concentrar nas *entidades CRG* uma elevada inteligência de gerenciamento, incluindo as funcionalidades para gerenciamento dos equipamentos pelos quais é responsável e os mecanismos de controle requeridos (para uso, por exemplo, por múltiplos domínios administrativos, como abordado posteriormente).

Outra importante característica da arquitetura diz respeito a sua aplicação para redes em que há a presença de um grande número de equipamentos heterogêneos que, embora necessitem ser gerenciados a partir de informações e de protocolos variados, possuem um suporte nativo a gerenciamento rígido e limitado. Neste contexto, a arquitetura proposta pode ser vista como se estendesse as rígidas funcionalidades de gerenciamento do equipamento gerenciado através das *entidades CRG* localizadas em outros nodos da rede. O emprego destas entidades para as atividades periódicas de *polling* permite que a consulta às informações de gerenciamento seja realizada com a flexibilidade de operações de *polling* tradicionais (*e.g.*, permitindo a monitoração de qualquer informação disponibilizada pelo agente em equipamentos heterogêneos, através de diferentes protocolos, com o controle de limiares e a geração de notificações de eventos), porém sem causar as limitações de escalabilidade e de tolerância a falhas que ocorrem nas abordagens tradicionais, em virtude do grande número de *entidades CRG* possibilitado pela abordagem proposta e de sua estrutura (como será discutido no capítulo 8).

A arquitetura possibilita também sua aplicação para atividades de monitoração de redes que envolvam um único ou múltiplos domínios administrativos. Na presença de múltiplos domínios, se não houver hierarquia administrativa entre estes, os serviços da arquitetura devem fazer uso de mecanismos para controle e segurança integrados ao ambiente (como discutido na seção 5.4.1) para que as entidades possam avaliar e tomar decisões quanto à execução, ou não, de um serviço solicitado. Na arquitetura de *polling* distribuída baseada em P2P, este controle pode ser concentrado nas *entidades CRG* ao receberem a solicitação de configuração de *polling* (na invocação do serviço *SvcGpCrPolling*). Tais entidades podem, assim, utilizar os mecanismos do ambiente para definir se irão ou não realizar a configuração de *polling* requerida e, no caso de optarem por não realizar o *polling* requisitado, os parâmetros para sua configuração são descartados e atividade de *polling* periódico não é ativada.

A existência de equipamentos com suporte ao gerenciamento limitado, discutida anteriormente, causa algumas necessidades adicionais à arquitetura, tal como a exigência de um esquema de mapeamento entre os *grupos CRG* e cada equipamento gerenciado. A arquitetura pode, contudo, quando pertinente, ser simplificada para explorar as características de redes nas quais os equipamentos suportem a execução de *peers* nos próprios equipamentos (nodos). Nestas situações, uma abordagem que pode ser investigada é a criação de *grupos de entidades CRG* para cada nodo da rede, grupos estes que contenham o *peer* localizado no próprio nodo gerenciado e um ou mais *peers*

adicionais para detecção de falhas neste nodo (fazendo uso de mecanismos de tolerância a falhas entre os membros do grupo, como discutido na seção 5.2.3). Neste contexto, o *serviço de mapeamento recurso gerenciado-grupo CRG* (*SvGpSgGroupResourceMap*) pode ser eliminado e o *serviço de controle do polling* (*SvGpSgPollingDommainControl*) pode ser adaptado para não mais requerer este mapeamento, passando a fazer uso apenas dos mecanismos providos pela infra-estrutura P2P para que seja feita a divulgação das solicitações de configurações de *polling*.

Adicionalmente, em redes com natureza tipicamente distribuída, tal como, por exemplo, em algumas ocorrências de redes *mesh*, mecanismos podem ser investigados para que os *grupos de entidades CRG* possam ser organizados para possuírem como membros os nodos vizinhos na própria rede, explorando a topologia da rede física para o posicionamento das entidades responsáveis pela monitoração destes.

7.7 Considerações Finais

Este capítulo apresentou uma arquitetura para a atividade de *polling*, empregada nas funcionalidades de gerenciamento de monitoração da rede e de coleta periódica de dados de desempenho. O capítulo apresentou a arquitetura de *polling* distribuída e seus serviços, discorreu sobre um cenário exemplo de sua aplicação, apresentou o protótipo desenvolvido, discutiu os experimentos realizados com este e teceu considerações sobre a arquitetura proposta.

A arquitetura apresentada demonstra um exemplo de como realizar no ambiente proposto uma atividade de modo fortemente distribuído, incluindo sua separação em duas etapas, uma que configura as entidades envolvidas; outra que executa as ações de gerenciamento propriamente ditas, já executada de forma totalmente distribuída por diversas *entidades CRG*. A arquitetura apresentada possibilita, ainda, demonstrar como uma arquitetura para uma atividade de gerenciamento pode fazer uso da composição de serviços provida pelo ambiente e como coordenar os serviços relacionados para a realização da atividade completa. Por fim, a arquitetura possibilita mostrar como fazer uso de serviços estruturais do ambiente proposto.

O capítulo a seguir apresenta uma análise do modelo e da arquitetura de gerenciamento distribuído baseado em P2P, discutindo, quando pertinente, a arquitetura de *polling* proposta como exemplo.

8 ANÁLISE DO MODELO E DA ARQUITETURA DE GERENCIAMENTO BASEADO EM P2P

O capítulo 5 apresentou um modelo e uma arquitetura para um ambiente de gerenciamento distribuído baseado em P2P. Tais discussões foram seguidas pelo detalhamento das principais características de um serviço estrutural (*serviço de envio de notificações*) no ambiente proposto (capítulo 6) e pela discussão de um estudo de caso de uma atividade de gerenciamento (*polling* distribuído) baseada em tal modelo e em tal arquitetura (capítulo 7).

Neste capítulo, serão abordados aspectos adicionais do modelo e da arquitetura propostos, com o objetivo de fornecer uma discussão que permita avaliar suas características e funcionalidades, assim como discutir seu emprego para o gerenciamento das redes atuais. A seção 8.1 apresenta uma análise comparativa entre a abordagem baseada em P2P e duas outras importantes abordagens de gerenciamento distribuídas, comparando nove características entre estas. A seção 8.2 apresenta considerações sobre a análise realizada. A seção 8.3 discute o emprego da abordagem baseada em P2P para o gerenciamento de diferentes redes atuais, incluindo redes tradicionais e redes com características modernas. Por fim, a seção 8.4 apresenta as considerações finais do capítulo.

8.1 Análise Comparativa

Uma análise comparativa do modelo e da arquitetura do ambiente de gerenciamento baseados em P2P propostos foi realizada, confrontando-os com duas outras abordagens de gerenciamento distribuídas. Para a elaboração desta análise, foi escolhido como exemplo de atividade de gerenciamento, na comparação realizada, a atividade de *polling*, fazendo uso, para a abordagem baseada em P2P, da arquitetura discutida como estudo de caso no capítulo 7. A análise discutiu ainda, quando pertinente, correlações existentes entre as abordagens e o gerenciamento dos contextos modernos selecionados como estudo de caso no capítulo 4.

Para a análise, optou-se pela realização de uma comparação entre as abordagens baseada em critérios qualitativos. A opção por uma avaliação baseada em tal sorte de critérios, incluindo características, requisitos funcionais e/ou capacidades, é adotada por alguns autores ao analisar e comparar abordagens de gerenciamento distribuídas, tal como utilizado por Quittek e Brunner ao avaliar tecnologias de gerenciamento distribuído (QUITTEK; BRUNNER, 2003) e por Martinez e outros ao avaliar diferentes modos de implementação de uma arquitetura para gerenciamento de políticas baseada na Script MIB (MARTINEZ et al, 2002).

Na presente pesquisa, optou-se por também adotar uma avaliação seguindo tal sorte de critérios, baseada em características e funcionalidades, sendo esta avaliação qualitativa escolhida frente a uma avaliação quantitativa em virtude de dois motivos principais: tal sorte de comparação permite discutir mais aspectos das abordagens; e a escalabilidade e outros parâmetros de desempenho das abordagens estão intrinsecamente relacionados com o paradigma de distribuição empregado por estas. Além disto, uma comparação quantitativa não possibilitaria considerar outros importantes aspectos funcionais, não quantitativos, que deveriam ser comparados entre as abordagens, tais como a tolerância a falhas suportada, o nível de controle requerido entre as entidades da abordagem, o suporte oferecido à comunicação entre as entidades, a flexibilidade proporcionada, a facilidade para o projeto e a implementação de novas funcionalidades, a complexidade da abordagem, etc.

A abordagem proposta foi comparada com duas outras abordagens de gerenciamento distribuído: a adotada por plataformas de gerenciamento de redes tradicionais comerciais largamente utilizadas, e a Script MIB (LEVI; SCHÖNWÄLDER, 2001) (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000). Estas abordagens foram selecionadas por representarem diferentes e representativos modelos de gerenciamento. O modelo e a arquitetura seguidos pelas plataformas de gerenciamento de redes comerciais são compostos por uma estação de gerenciamento principal e algumas estações coletoras que recuperam as informações de gerenciamento dos equipamentos da rede. Este modelo e esta arquitetura são, ainda hoje, largamente utilizados no gerenciamento de redes reais e representam uma das abordagens de gerenciamento mais tradicionais. A Script MIB, por sua vez, como apresentado na seção A.2.3, define uma MIB SNMP projetada para que funções de gerenciamento possam ser delegadas para gerentes distribuídos. Esta abordagem representa uma das abordagens de gerenciamento fortemente distribuídas mais pesquisadas e discutidas na literatura, tendo sido debatida através de um grupo de trabalho do IETF (IETF, 2010) e padronizada através de uma RFC (LEVI; SCHÖNWÄLDER, 2001).

As abordagens foram comparadas segundo nove características, selecionadas com o objetivo de diferenciar características funcionais importantes nas abordagens de gerenciamento distribuídas, com o intuito de distinguir estrutura, aspectos de operação, requisitos de gerenciamento, benefícios e limitações em cada abordagem. Quando pertinente, as características foram também utilizadas para comparar a arquitetura da atividade de *polling* nas abordagens. Por fim, algumas características permitiram também comparar as abordagens em relação aos requisitos de gerenciamento dos estudos de caso de contextos modernos analisados no capítulo 4, que compreendem o gerenciamento de redes *mesh* sem fio (seção 4.3.1), os mecanismos para detecção e reação a ataques DDoS que necessitam ser realizados em redes intermediárias (seção 4.3.2) e o gerenciamento da infra-estrutura de redes requerido por grades computacionais (seção 4.3.3).

Na análise, a fim de facilitar a comparação entre as diferentes abordagens, foi adotada uma nomenclatura que considera a estrutura formada nas interações entre as entidades para a realização de funcionalidades de gerenciamento. Assim, a entidade que requisita uma funcionalidade de gerenciamento (*e.g.*, *polling*) será referida como *top-level manager* (TLM), ou *gerente de nível superior.* As outras entidades que executam ações para que a funcionalidade requisitada seja realizada serão referidas como *mid-level managers* (MLM), ou *gerentes de nível intermediário*. Entre estas, considerando a funcionalidade de *polling* analisada como exemplo, as entidades que especificamente

realizam as requisições de *polling* periódicas (interagindo com os recursos monitorados) serão aqui denominadas *collector mid-level managers* (CMLM), ou *gerentes de nível intermediário coletores*. Cabe destacar que esta terminologia comum foi adotada para facilitar a comparação entre as diferentes abordagens. Tal terminologia, entretanto, enfoca a estrutura de cada atividade individualmente (*e.g.*, cada configuração de *polling* realizada), e não as operações completas no ambiente, já que, no ambiente proposto, tais papéis não são fixos: ao contrário, são papéis dinâmicos, que certas entidades assumem numa determinada atividade, e que podem ser alterados em outras atividades sendo realizadas em paralelo ou posteriormente. Além disto, tal nomenclatura não indica uma hierarquia administrativa de uma entidade sobre a outra: ela representa apenas a estrutura hierárquica para a realização de uma atividade, a fim de nomear as entidades de acordo com o modo como estas estão estruturadas e como a interação é realizada entre elas.

As tabelas 8.1, 8.2 e 8.3 sintetizam os resultados da análise realizada para cada uma das características. Estes resultados são discutidos nas seções a seguir.

Tabela 8.1: Comparação entre abordagens de gerenciamento — 1

Característica	**Abordagem de Gerenciamento**		
	Plataformas Tradicionais	**Script MIB**	**Baseada em P2P**
1. Nível de distribuição	Fracamente distribuído	Fortemente distribuído	Fortemente distribuído
2. Monitoração	Realizada pela estação de gerenciamento principal (TLM) e por estações de gerenciamento secundárias (CMLMs).	*Scripts* delegados para MLMs podem executar funções de *polling*.	Serviços implementam funções de *polling*, incluindo um serviço que executa o *polling* periódico em *entidades CRG (*CMLMs).
3. Controle de entidades MLMs pela entidade TLM: funções disponibilizadas para entidade TLM controlar entidades MLMs; nível de controle da entidade TLM requerido pelas entidades MLMs para a operação destas	Tipicamente, as estações secundárias (MLMs) realizam ações de gerenciamento com elevada autonomia. Muitas funções de controle podem não ser disponibilizadas para a estação principal (TLM).	Funções para controle dos MLMs pelo TLM são disponibilizadas através de objetos da Script MIB. O TLM tipicamente precisa realizar operações de controle sobre os MLMs, tais como transferir ou requisitar a transferência do *script*, iniciar sua execução, obter resultados sobre sua execução, etc.	Funções para controlar os MLMs podem ser implementadas através de operações que são disponibilizadas pela interface do serviço requisitado. O TLM envia as informações através dos parâmetros das operações de serviços. Cada serviço invocado tipicamente executa sua operação sem a necessidade de controle da entidade que o invocou.

Tabela 8.2: Comparação entre abordagens de gerenciamento — 2

Característica	Abordagem de Gerenciamento		
	Plataformas Tradicionais	**Script MIB**	**Baseada em P2P**
4. Comunicação entre entidades de gerenciamento	Tipicamente, através de mensagens SNMPv2 Inform-Request e de mensagens específicas da plataforma.	Através do protocolo SNMP e dos objetos da Script MIB, possuindo limitações de flexibilidade (interação baseada em objetos SNMP se torna custosa e possui as limitações do modelo de informação).	Através de mensagens do ambiente, dos serviços estruturais do ambiente e de invocação das operações dos serviços de gerenciamento, proporcionando maior flexibilidade.
5. Localização das entidades MLMs	Distância média dos recursos gerenciados.	Podem ser dispostas próximas aos recursos gerenciados.	Podem ser dispostas próximas aos recursos gerenciados.
6. Escalabilidade	Média Processamento de gerenciamento ainda concentrado em poucas estações.	Mais elevada Forte distribuição das ações de gerenciamento (emprego de elevado número de entidades MLMs, proximidade entre estas e recursos gerenciados, com redução da concentração do tráfego de gerenciamento e processamento).	Mais elevada Forte distribuição das ações de gerenciamento (emprego de elevado número de entidades MLMs, proximidade entre estas e recursos gerenciados, com redução da concentração do tráfego de gerenciamento e processamento). Aprimorada pelo TLM não necessitar realizar operações de controle sobre MLMs. Aprimorada pelo suporte a serviços de *grupos de peers* e distribuição de carga entre seus membros.
7. Tolerância a falhas	Limitada Considerando cenário de atividade de *polling* como estudo de caso: - Falha da estação principal: continuidade das operações das estações secundárias; monitoração dos equipamentos realizada pela estação principal interrompida. - Falha de estação secundária: como nas demais abordagens, há continuidade das operações das demais estações secundárias.	Média Considerando cenário de atividade de *polling* como estudo de caso: - Falha do TLM: algumas funções dos CMLMs podem ser interrompidas. - Falha de CMLM: como nas demais abordagens, há continuidade das operações dos demais CMLMs. Aprimorada pelo emprego de grande número de entidades CMLMs.	Alta Considerando cenário de atividade de *polling* como estudo de caso: - Falha do TLM: não afeta a operação das *entidades CRG*. - Falha de *entidade CRG*: como nas demais abordagens, há continuidade das operações das demais *entidades CRG*. Aprimorada pelo emprego de grande número de *entidades CRG*. Aprimorada pelo suporte a serviços de *grupos de peers* e possibilidade de outro *peer* do grupo assumir as funções do *peer* em falha.

Tabela 8.3: Comparação entre abordagens de gerenciamento — 3

Característica	Abordagem de Gerenciamento		
	Plataformas Tradicionais	**Script MIB**	**Baseada em P2P**
8. Facilidade e flexibilidade para projeto e implementação de funcionalidades	De acordo com a estrutura e a API fornecida pela plataforma.	Média Algumas características contribuem para a redução da facilidade e/ou da flexibilidade. Outras contribuem para aumento da facilidade. Entre outros: - Redução de simplicidade se comparada a abordagens fracamente distribuídas: funcionalidades necessitam ser concebidas de modo a distribuir as ações para um elevado número de entidades. - Facilidade aprimorada por: não possuir restrições de linguagem para o *script*; ser designada integrada ao *framework* SNMP (padronizado, amplamente utilizado). - Redução de flexibilidade por: invocação dos *scripts* ser limitada aos recursos providos pela Script MIB.	Mais elevada Algumas características contribuem para a redução da facilidade. Outras contribuem para aumento da facilidade e/ou da flexibilidade. Entre outros: - Redução de simplicidade se comparada a abordagens fracamente distribuídas: funcionalidades necessitam ser concebidas de modo a distribuir as ações para um elevado número de entidades. - Facilidade aprimorada por: arquitetura baseada em serviços e composições destes, permitindo reuso de serviços no desenvolvimento de novas funcionalidades. - Facilidade aprimorada por: serviços desenvolvidos podem fazer uso dos serviços da infra-estrutura P2P e dos serviços estruturais. - Flexibilidade aprimorada por: não ser restrita aos modelos de informação e de comunicação do *framework* SNMP. - Facilidade aprimorada por: suporte provido ao desenvolvimento de serviços que aprimorem a implantação e a manutenção do próprio ambiente.
9. Complexidade da abordagem	Reduzida Pequeno número de estações secundárias com elevada inteligência e autonomia. Estações secundárias podem ser configuradas diretamente pelo administrador. Entidades possuem papéis pré-definidos, com estrutura fixa e permanente.	Elevada Ações distribuídas para elevado número de entidades requerem mecanismos para interação entre estas, coordenação das ações, acesso às informações distribuídas, etc. Na implantação do ambiente, seleção de entidades e seus papéis na hierarquia envolve elevado número de entidades.	Elevada Ações fortemente distribuídas. Eliminação da necessidade de entidades assumirem papéis fixos na estrutura demanda entidades e atividades com estruturas distintas. Na implantação do ambiente, é requerida a configuração de parâmetros para sua operação. Mecanismos de segurança requeridos para uso em múltiplos domínios administrativos. Necessidade de oferecer e manter a infra-estrutura P2P.

8.1.1 Nível de Distribuição

A arquitetura seguida pelas plataformas tradicionais representa um típico exemplo de arquitetura fracamente distribuída. A abordagem emprega, para a atividade de *polling*, analisada como estudo de caso, também uma arquitetura fracamente distribuída. Por sua vez, a arquitetura adotada pela Script MIB pode ser empregada de forma fracamente e fortemente distribuída (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000). Pode, assim, ser empregada para arquiteturas de *polling* fracamente e fortemente distribuídas. Por fim, a arquitetura baseada em P2P representa uma abordagem fortemente distribuída. A arquitetura da atividade de *polling* apresentada no capítulo 7 é também projetada com forte distribuição. Ambas as arquiteturas do ambiente baseado em P2P e a arquitetura de *polling* propostas, contudo, podem ainda ser empregadas de modo fracamente distribuído, se desejado. Na análise realizada neste capítulo, será dado enfoque às abordagens baseada na Script MIB e baseada em P2P que adotam forte distribuição. Deste modo, ao menos quando explicitamente referido, este nível de distribuição será o considerado na análise dos itens a seguir.

Considerando o nível de distribuição suportado pelas abordagens em relação ao gerenciamento dos três contextos modernos analisados como estudos de caso no capítulo 4, algumas observações adicionais podem ser apresentadas. Acerca do contexto moderno de redes *mesh* sem fio, os resultados da análise apresentada em referido capítulo (seção 4.3.1) permitem concluir que o gerenciamento destas redes através da arquitetura seguida pelas plataformas tradicionais não seria indicado, em virtude desta arquitetura empregar um paradigma fracamente distribuído. Tal restrição não ocorre com o uso da arquitetura baseada na Script MIB ou da arquitetura baseada em P2P, já que ambas suportam o emprego de paradigmas fortemente distribuídos, mais indicados para o gerenciamento destas redes.

Acerca dos mecanismos de detecção e reação a ataques DDoS, os resultados da análise (seção 4.3.2) também destacam a importância do emprego de paradigmas fortemente distribuídos para o tratamento de vários tipos de ataques. Deste modo, também para este contexto de rede, conclui-se que o gerenciamento a partir de plataformas tradicionais não se mostraria adequado.

Por fim, considerando o gerenciamento das grades computacionais, a análise observou (seção 4.3.3) que, em contextos nos quais a grade não possuir escala excessivamente ampla e não exigir o gerenciamento das redes que provêem a interconexão entre os domínios administrativos, seriam indicadas, quanto ao grau de distribuição, tanto arquiteturas baseadas no paradigma fracamente distribuído como baseadas no paradigma fortemente distribuído. Assim, quanto ao aspecto discutido no presente item da comparação, que avalia o nível de distribuição isoladamente, sem considerar a existência de relações de hierarquia administrativa na arquitetura, tais condições se encaixariam em qualquer uma das três abordagens.

8.1.2 Monitoração

As três abordagens comparadas podem ser empregadas para a monitoração das redes através de *polling*. Na arquitetura seguida pelas plataformas tradicionais, a monitoração dos equipamentos gerenciados na rede é realizada pela estação de gerenciamento principal (TLM) e por um pequeno número de estações de gerenciamento secundárias coletoras (CMLMs). Tais papéis são assumidos permanentemente pelas entidades. Na arquitetura da Script MIB, *scripts* delegados para agentes da Script MIB (MLMs) por

um gerente SNMP (TLM) podem implementar funções de *polling*, tornando-se CMLMs. Por fim, na arquitetura proposta no capítulo 7, a funcionalidade de *polling* é realizada através de serviços que implementam tais funções, incluindo um serviço que realiza a execução do *polling* periódico propriamente dito em *entidades para controle dos recursos gerenciados* (*entidades CRG*), que representam o papel de CMLMs naquele dado *polling*.

Tais estruturas podem também ser seguidas na monitoração dos contextos modernos analisados como estudo de caso. Adicionalmente, para a abordagem que segue o modelo e a arquitetura baseados em P2P, em contextos com natureza tipicamente distribuída, tais como em redes *mesh* sem fio e em ataques DDoS, adaptações e simplificações poderiam ser realizadas na arquitetura de monitoração de modo a explorar as características do contexto e da abordagem de modo conjunto, tal como discutido na seção 7.6.

Considerando as limitações e os requisitos de gerenciamento dos contextos modernos, conclui-se que a monitoração de redes *mesh* não se mostraria adequada de ser realizada através da arquitetura adotada pelas plataformas tradicionais, em virtude do pequeno nível de distribuição das ações de monitoração empregado, que utiliza um pequeno número de entidades CMLMs. Por outro lado, a arquitetura baseada na Script MIB e a arquitetura baseada em P2P não possuem tais restrições, já que empregam alta distribuição das ações de gerenciamento, o que permitiria o aperfeiçoamento das funcionalidades de monitoração pela possibilidade de coleta de informações de modo simultâneo ao longo de toda a rede, além de trazer benefícios que incluem maior tolerância a falhas e escalabilidade, como será discutido em itens posteriores. Comparando, por fim, ambas as abordagens fortemente distribuídas, conclui-se que a abordagem baseada em P2P possui alguns benefícios para a monitoração de redes *mesh* sem fio em virtude do maior suporte que a abordagem pode proporcionar para lidar com redes dinâmicas, decorrente de características da abordagem, tais como: capacidade de auto-organização provida pela infra-estrutura P2P; não exigência de papéis estanques para as entidades, que podem assumir diferentes tipos de entidade (por exemplo, assumindo o papel de *entidade SG* e de *entidade CRG*); suporte a *grupos de peers*, de modo que um serviço possa ser executado por qualquer *peer* do grupo, etc. Tais benefícios são considerados importantes para o gerenciamento de redes *mesh* sem fio uma vez que poderiam proporcionar maior suporte para lidar com alterações da topologia da rede, que podem ocorrer com freqüência em tais redes.

A necessidade do emprego de uma abordagem fortemente distribuída ocorre também, como visto no item anterior, para os mecanismos de tratamento a ataques DDoS executados em redes intermediárias. Em tal contexto, a monitoração da rede representa uma atividade auxiliar para o mecanismo de tratamento aos ataques, fornecendo informações que permitem a detecção destes. A monitoração deveria, tipicamente, permitir obter informações dos roteadores da rede dispersos ao longo de vários domínios administrativos, fazendo uso de um grande número de entidades CMLMs. Assim, o emprego da arquitetura seguida pelas plataformas tradicionais não se mostraria adequado para a monitoração deste contexto, sendo requerido o emprego de arquiteturas que ofereçam suporte para que as ações de monitoração sejam realizadas de modo fortemente distribuído, tais como nas abordagens baseada na Script MIB e baseada em P2P.

Por fim, considerando o gerenciamento de infra-estruturas de rede requerido por grades computacionais que não sejam excessivamente amplas e não requeiram o

gerenciamento das redes intermediárias, a monitoração poderia ser realizada através de abordagens fracamente ou fortemente distribuídas.

Em adição ao nível de distribuição suportado, aspectos adicionais devem ser analisados para os três contextos modernos quando a rede gerenciada envolver mais de um domínio administrativo, sem hierarquia entre eles. Nestes contextos, a abordagem de gerenciamento empregada deveria suportar ou poder ser estendida para prover mecanismos para controlar as informações de monitoração fornecidas para outros domínios administrativos.

8.1.3 Controle de Entidades MLMs pela entidade TLM

O controle de entidades MLMs aqui discutido envolve dois aspectos: as funções disponibilizadas para a entidade TLM controlar as entidades MLMs, e o nível de controle da entidade TLM requerido pelas entidades MLMs para a operação destas.

Em plataformas tradicionais, tipicamente as estações de gerenciamento secundárias (MLMs) realizam ações de elevada complexidade e com autonomia, sem requererem que a entidade principal (TLM) execute muitas funções de controle para a execução da funcionalidade. Muitas vezes, as estações secundárias são configuradas diretamente pelo administrador da rede, sem o auxílio ou a interferência da estação de gerenciamento principal. Além disto, muitas funções para controle das entidades MLMs podem não ser disponibilizadas. Isto também ocorre para a atividade de *polling*, na qual funções para a estação principal alterar a execução da atividade nas estações secundárias coletoras (CMLMs) podem não ser providas: apenas funções para controle dos resultados são oferecidas.

Na arquitetura da Script MIB, as entidades MLMs (entidades com agentes da Script MIB) provêm diversas funções para que a entidade TLM controle a execução do *script*. Tais funções são disponibilizadas através de objetos da Script MIB, que são invocados pela entidade TLM através de operações SNMP. Por outro lado, a entidade TLM necessita realizar um grande controle sobre a execução do *script* no MLM para a realização das funcionalidades de gerenciamento: tipicamente, a entidade TLM terá que verificar se o MLM já possui o módulo do *script* que executa a funcionalidade; terá que transferir ou requisitar a transferência do *script* em caso contrário; terá que controlar a execução do *script*; terá que obter os resultados sobre a execução deste, etc. Este mecanismo ocorre para as diversas funcionalidades de gerenciamento a serem executadas pelas MLMs, incluindo a funcionalidade de *polling*.

Por fim, na arquitetura baseada em P2P proposta, funções para controlar a execução dos serviços do ambiente são providas através de operações destes definidas pelas interfaces dos serviços. Não há restrições sobre tais operações, de modo que, se requerido, podem ser implementadas operações de serviços que disponibilizem funções de controle específicas para que as entidades TLM controlem a execução de tais serviços. Tipicamente, contudo, a arquitetura requer um nível de controle muito baixo do TLM (possivelmente, apenas a informação dos parâmetros da funcionalidade a ser invocada, *e.g.*, parâmetros de configuração do *polling*). Isto ocorre porque os MLMs do ambiente (incluindo os CMLMs na funcionalidade de *polling*) são concebidos para possuir independência e autonomia de outras entidades, possuindo eles mesmos controle sobre como executar suas próprias funções. No caso da arquitetura de *polling* proposta, por exemplo, o serviço ou a aplicação requisitando a atividade (representando o papel de TLM naquela dada configuração de *polling*) apenas precisa informar os parâmetros

desejados para o *polling* (*e.g.*, informações a serem monitoradas, início imediato ou posterior da monitoração, freqüência de monitoração, etc.): a operação do serviço é controlada pelo próprio serviço nas *entidades CRG* (que representam entidades CMLMs). Comparando, assim, a abordagem proposta com a abordagem da Script MIB, esta última requer que o TLM realize muito mais controle sobre os MLMs: a abordagem baseada em P2P provê maior independência e autonomia para os MLMs.

Acerca dos contextos modernos analisados como exemplo, cabe destacar que, no gerenciamento de redes *mesh* sem fio, o emprego de uma abordagem que exija um elevado nível de controle das entidades MLMs não se mostraria apropriado em virtude da dinamicidade estas redes, que podem apresentar freqüentes alterações de topologia e particionamentos da rede. Deste modo, o isolamento entre as entidades MLMs e a entidade TLM poderia causar limitações importantes de gerenciamento se um elevado controle for requerido pelas entidades MLMs para a operação destas. Assim, considerando as abordagens analisadas, o maior nível de controle requerido da abordagem baseada na Script MIB se mostraria menos adequado para o gerenciamento das redes *mesh* sem fio.

Considerações similares podem ser apresentadas para os mecanismos de tratamento a ataques DDoS que necessitam ser realizados em redes intermediárias. Em redes sob um ataque em curso, é usual a ocorrência de um volume excessivo de tráfego, que pode gerar dificuldades de acesso entre as redes. Assim, a exigência de um elevado nível de controle da entidade TLM sobre as entidades MLMs nos mecanismos de tratamento não é considerada apropriada, já que tais entidades seriam acessadas através das próprias redes que sofrem o ataque.

Por fim, para qualquer um dos três contextos modernos analisados, é importante destacar que, na presença de diversos domínios administrativos no ambiente gerenciado, o controle requerido entre as entidades da abordagem, se houver, deve ser integrado a mecanismos das entidades MLMs que permitam a estas ter autonomia para a tomada de decisão quanto à opção ou não por executar as operações indicadas pela entidade TLM. Tal autonomia, contudo, não se mostraria natural em abordagens em que um elevado controle for requerido da entidade TLM.

8.1.4 Comunicação entre Entidades de Gerenciamento

Em plataformas tradicionais, a comunicação entre as entidade de gerenciamento (estações) é tipicamente realizada através de mensagens específicas da plataforma. Mensagens SNMPv2 Inform-Request também são empregadas para reportarem eventos de estações de gerenciamento secundárias (MLMs) para a estação de gerenciamento principal (TLM), tal como, por exemplo, para reportarem eventos detectados na monitoração.

Na Script MIB, a comunicação entre o TLM e os MLMs é realizada através do protocolo SNMP e dos objetos da Script MIB. Os resultados do *script* são também coletados através de objetos da Script MIB. Tais aspectos, embora possuam os benefícios de utilizar um protocolo padrão *de facto*, possuem limitações de flexibilidade já que a interação através de objetos SNMP se torna custosa e possui as limitações impostas pelo modelo de informação utilizado. Entre as limitações existentes, incluem-se as apontadas em (QUITTEK, BRUNNER, 2003), que compreendem: resultados das funções delegadas (executadas através dos *scripts*) retornados em *strings*, sendo suportada apenas uma *string* por função, e esta *string* sobrescrita cada vez que a função

produz novo resultado. Além disto, tais autores destacam ainda a limitação da comunicação entre TLMs e MLMs através de notificações, observando que um número muito restrito de notificações é provido pela abordagem para esta forma de comunicação. Em adição ao pequeno número de notificações suportadas, cabe destacar que estas são ainda limitadas ao esquema de envio de notificações provido pelo *framework* SNMP, que não oferece mecanismos mais flexíveis e elaborados tal como o envio de notificações *publish-subscribe*.

Por outro lado, na arquitetura baseada em P2P, a comunicação entre as entidades é realizada através de mensagens do ambiente de gerenciamento e de invocações de operações dos serviços envolvidos na funcionalidade sendo realizada (*e.g.*, *polling*), que podem ser desenvolvidos de forma flexível. Resultados de ações de gerenciamento específicas podem também ser obtidos através de operações dos serviços. Adicionalmente, na arquitetura proposta, o armazenamento das informações produzidas na atividade e o envio de notificações são realizados fazendo uso das potencialidades do ambiente de gerenciamento baseado em P2P. Deste modo, por exemplo, a consulta às informações de gerenciamento coletadas por um *grupo CRG* é realizada por outras entidades fazendo uso do serviço de armazenamento baseado em P2P do ambiente, e o envio de notificações reportando eventos é realizado através do serviço de envio de notificações *publish-subscribe* baseado em P2P do ambiente. Tais recursos proporcionam uma flexibilidade muito maior para a interação entre as entidades e para a execução das atividades.

Acerca dos contextos modernos analisados como exemplo, cabe destacar que a arquitetura baseada em P2P proposta tem como benefício adicional o suporte à difusão de mensagens para grupos ou para todas as entidades da rede de gerenciamento, provido pela infra-estrutura P2P empregada, o que poderia ser explorado para aprimorar a comunicação entre as entidades no gerenciamento de contextos com natureza tipicamente fortemente distribuída tais como as redes *mesh* sem fio e os mecanismos de tratamento a ataques DDoS. Assim, a execução de operações tais como a solicitação de execução de uma ação de monitoração ou a solicitação de configuração de um dado tipo de recurso poderia ser realizada, nestes contextos, fazendo uso deste mecanismo de difusão, diferente do empregado, por exemplo, em abordagens baseadas na Script MIB, em que cada entidade MLM necessita ser identificada e endereçada individualmente.

8.1.5 Localização dos MLMs

Na arquitetura seguida pelas plataformas tradicionais, as estações de gerenciamento secundárias são dispostas a uma distância média ou longa dos recursos gerenciados, já que um pequeno número de entidades secundárias é empregado. Esta disposição se aplica, assim, também para a atividade de *polling*, na qual tais estações representam as entidades CMLMs.

Com uma estrutura distinta, ambas as arquiteturas baseada na Script MIB e baseada em P2P permitem que as entidades MLMs sejam dispostas próximas aos recursos gerenciados: é requerido apenas que os MLMs sejam equipados com um agente SNMP com suporte para a Script MIB ou equipados com um *peer* do ambiente, respectivamente. Deste modo, também na funcionalidade de *polling* as entidades CMLMs podem estar dispostas próximas aos recursos.

Considerando os contextos modernos analisados como estudos de caso, é possível concluir-se que, no gerenciamento de redes *mesh* sem fio, tipicamente a melhor

disposição para as entidades MLMs envolveria a introdução de uma entidade MLM em um elevado número de nodos da rede, a fim de minimizar situações em que as alterações de topologia e particionamento da rede deixem parte desta sem entidades que possam realizar seu gerenciamento. Configuração similar poderia ser indicada para o tratamento de ataques DDoS.

Além disto, acerca destes contextos, é possível concluir-se a importância de avaliar a presença dos diversos domínios administrativos no contexto sendo gerenciado. Em tais situações, as entidades MLMs tipicamente deveriam ser posicionadas de modo que a entidade MLM responsável pelo gerenciamento de um dado equipamento da rede faça parte daquele mesmo domínio e possa executar mecanismos para controle das operações requisitadas por outras entidades. Este requisito pode ser considerado relevante para qualquer uma das abordagens distribuídas analisadas.

8.1.6 Escalabilidade

Quando comparadas às abordagens centralizadas ou fracamente distribuídas (incluindo as plataformas tradicionais), ambas as abordagens baseada na Script MIB e baseada em P2P são aprimoradas por suportarem um grande número de entidades MLMs e pelo posicionamento destas próximas aos recursos gerenciados. Isto possibilita que o processamento de gerenciamento seja distribuído para um grande número de nodos e que o tráfego de gerenciamento seja distribuído ao longo da rede, não mais existindo um elevado volume de tráfego concentrado nos enlaces próximos a um pequeno número de entidades. Considerando a funcionalidade de *polling*, tais características adquirem ainda maior relevância, já que o *polling* representa uma atividade realizada periodicamente e para um grande número de recursos. Assim, o posicionamento das entidades CMLMs próximas aos recursos gerenciados contribui por diminuir o tráfego periódico de monitoração nos enlaces das redes, que passa a ser restrito aos enlaces entre cada entidade coletora e os recursos monitorados por esta.

Por fim, em comparação com a Script MIB, a escalabilidade da arquitetura baseada em P2P é aprimorada em virtude do TLM não necessitar realizar operações de controle sobre os MLMs, reduzindo ainda mais o processamento e o tráfego nesta entidade. Além disto, o suporte para serviços de grupo proporcionado pela arquitetura baseada em P2P aprimora a escalabilidade através dos métodos de distribuição de carga que podem ser utilizados entre os membros do grupo, como discutido na seção 5.2.3. Considerando a funcionalidade de *polling*, mais uma vez estes fatores adquirem ainda maior relevância, em virtude desta ser uma atividade periódica e que envolve tipicamente um grande número de recursos monitorados.

Considerando o gerenciamento do contexto moderno de redes *mesh* sem fio, a redução da concentração do processamento e do volume de tráfego de gerenciamento representa uma característica bastante relevante da abordagem de gerenciamento empregada, uma vez que estas redes possuem, freqüentemente, largura de banda e recursos reduzidos. Considerações similares podem ser tecidas para os mecanismos de tratamento a ataques DDoS analisados, já que, durante um ataque em curso, as redes envolvidas podem sofrer degradação dos serviços de rede em virtude de alto volume de tráfego do ataque, assim como os nodos envolvidos no ataque podem sofrer limitações de processamento, memória, etc. Acerca do gerenciamento da infra-estrutura de rede para grades computacionais, tipicamente a rede gerenciada possui características de redes tradicionais, existindo, assim, as mesmas restrições que as já discutidas para estas redes, sem requisitos adicionais.

8.1.7 Tolerância a Falhas

A análise da tolerância a falhas nas abordagens necessita ser realizada considerando-se os diferentes cenários de falha que podem ocorrer nas atividades de gerenciamento de redes. Considerando a atividade de *polling* como estudo de caso, tais falhas incluem situações como quando a entidade TLM falha, quando uma entidade CMLM falha, e quando falhas ocorrem nos canais de comunicação.

Nas situações em que a entidade TLM falha, em plataformas tradicionais comerciais, tipicamente a operação de *polling* é mantida nas demais estações (CMLMs) que realizam coleta de informações. Entretanto, se alguns equipamentos são monitorados pela própria estação TLM, a monitoração destes equipamentos é interrompida. Por sua vez, na abordagem baseada na Script MIB, de acordo com a implementação do *script*, as entidades CMLMs podem ter algumas funções interrompidas, já que diversas operações de controle são requeridas da entidade TLM para a operação das entidades CMLMs, como visto anteriormente (seção 8.1.3). Por fim, na arquitetura baseada em P2P, uma falha na entidade TLM não afeta a operação de *polling* periódica de nenhuma das entidades CMLMs, já que o *polling* periódico é executado apenas por tais entidades coletoras (*grupos de entidades CRG*) e tais entidades são autônomas e não requerem nenhum controle da entidade TLM para o serviço periódico. Adicionalmente, mesmo na atividade de configuração do *polling*, a abordagem é totalmente independente de uma entidade TLM específica: a arquitetura é concebida considerando que qualquer *peer* pode assumir o papel de TLM e requisitar a configuração de *polling*. Deste modo, mesmo os parâmetros configurados para *polling* podem ser alterados durante uma falha na entidade TLM que anteriormente requisitou um dado *polling* agora em execução.

Considerando, por sua vez, um cenário em que a entidade TLM está operando adequadamente e uma entidade CMLM falha, a operação de *polling* é mantida nas outras estações CMLMs em quaisquer das três abordagens. Nestes cenários, as plataformas tradicionais podem prover meios para que a estação de gerenciamento principal inicie o *polling* de algumas informações dos equipamentos que eram monitorados pela estação em falha (usualmente, um grande número de equipamentos, em função do pequeno número de entidades CMLMs). Entretanto, tal *polling* possivelmente suporta a coleta de apenas algumas informações básicas, limitando o gerenciamento destes equipamentos. Por outro lado, tanto nas arquiteturas baseada na Script MIB como na baseada em P2P, em virtude da forte distribuição proporcionada e do grande número de entidades coletoras empregado, a tolerância a falhas é aprimorada já que somente um pequeno número de equipamentos é afetado pela falha em uma entidade coletora, reduzindo seu dano. Em adição a estes benefícios proporcionados pela forte distribuição, comparando a arquitetura baseada na Script MIB com a arquitetura baseada em P2P, o suporte provido para serviços de *grupos de peers* nesta última traz benefícios para a tolerância a falhas uma vez que, se um dos *peers* do serviço de grupo falha, outros *peers* do grupo podem assumir as funções de *polling* do *peer* em falha, proporcionando a continuidade das operações da entidade coletora.

Por fim, considerando as situações em que falhas ocorrem nos canais de comunicação das redes causando a interrupção da conectividade em alguns pontos, as arquiteturas fortemente distribuídas (baseada na Script MIB e baseada em P2P) possuem tolerância a falhas aprimorada, uma vez que a forte distribuição permite que as entidades coletoras sejam posicionadas mais próximas aos recursos gerenciados, reduzindo as situações em que a comunicação é interrompida nos enlaces entre a

entidade CMLM e cada equipamento que esta gerencia. Em adição, na arquitetura baseada em P2P, o suporte provido para serviços de *grupos de peers* aumenta a tolerância a falhas já que, muitas vezes, a interrupção na comunicação da rede não afeta todos os membros do *grupo de peers CRG* e, assim, outro *peer* do grupo pode assumir as funções do *peer* que não mais possui conectividade para os equipamentos gerenciados.

Considerando os contextos modernos analisados como exemplo, cabe destacar que, acerca do gerenciamento de redes *mesh* sem fio, a tolerância a falhas suportada pela abordagem é uma característica extremamente relevante, já que tais redes possuem grande dinamicidade, com interconexões intermitentes e freqüentes alterações na topologia da rede, que podem levar ao particionamento desta e causar o isolamento tanto entre a entidade TLM e as entidades MLMs, como entre a entidade MLM e os equipamentos gerenciados por estas. Considerando a funcionalidade de monitoração através de *polling*, como esta é uma funcionalidade que deve ser realizada de modo contínuo e, no caso de redes *mesh* sem fio, deve ainda ser realizada ao longo de toda a rede e de modo freqüente (em virtude de sua dinamicidade e de suas outras características), a tolerância a falhas suportada pela atividade se mostra ainda mais relevante. Assim, observa-se que o gerenciamento destas redes através da arquitetura baseada na Script MIB e da arquitetura baseada em P2P se mostrariam mais adequados e, dentre estas, a arquitetura baseada em P2P se mostraria mais indicada em virtude de, adicionalmente às características das abordagens fortemente distribuídas em geral, possuir características que aumentam a tolerância a falhas suportada, como discutido acima.

8.1.8 Facilidade e Flexibilidade para Projeto e Implementação de Funcionalidades

A facilidade e a flexibilidade para o projeto e a implementação de novas funcionalidades de gerenciamento são importantes características da abordagem utilizada, em virtude da alta taxa de mudanças e evolução existentes nas redes atuais. Em plataformas tradicionais, tais características estão relacionadas à estrutura de desenvolvimento empregada e à API de desenvolvimento provida. Isto ocorre, do mesmo modo, para a implementação de novas funcionalidades para *polling*. Em virtude disto, tais características desta abordagem não podem ser comparadas de modo particular com as outras abordagens analisadas, já que dependem da plataforma específica empregada. Contudo, com relação ao nível de distribuição utilizado e à estrutura resultante deste, comparando as plataformas tradicionais com as abordagens fortemente distribuídas analisadas, observa-se uma diminuição de simplicidade no projeto e na implementação de funcionalidades nestas últimas. Isto ocorre em virtude das funcionalidades necessitarem agora ser concebidas de modo a distribuir as ações de gerenciamento para um número elevado de entidades, o que exige o emprego de uma arquitetura que considere esta distribuição e que faça uso de mecanismos para a coordenação de tais ações e para o acesso às informações de gerenciamento agora distribuídas.

Comparando ambas as abordagens fortemente distribuídas, outras características também interferem na facilidade e na flexibilidade para o projeto e a implementação de funcionalidades. Na Script MIB, conforme definido em sua especificação, não há restrições sobre a linguagem de programação a ser empregada, o que traz facilidade para o projeto e a implementação de *scripts*. Além disto, a abordagem possui como aspecto

relevante ter sido designada integrada ao *framework* SNMP, *framework* padronizado e amplamente utilizado no gerenciamento de redes. Por outro lado, considerando a flexibilidade para o projeto e a implementação de funcionalidades, a abordagem possui limitações pela invocação das funções (*scripts*) ser realizada através da Script MIB, tornando a flexibilidade para a invocação dos *scripts* limitada aos recursos providos pela Script MIB, assim como ao restrito suporte à comunicação provido, discutidos em item anterior.

Por fim, na abordagem baseada em P2P, o emprego de uma arquitetura baseada em serviços que permite a composição destes traz facilidade para o projeto e a implementação de novos serviços quando comparada à abordagem baseada na Script MIB, uma vez que todos os serviços do ambiente de gerenciamento P2P podem ser reutilizados através da composição de serviços e do suporte à invocação destes, sejam individuais ou de grupo. Além disto, os serviços a serem desenvolvidos podem fazer uso dos serviços providos pela infra-estrutura P2P e dos serviços estruturais do ambiente de gerenciamento P2P, também trazendo facilidade para o projeto e o desenvolvimento de funcionalidades.

Em adição a estes aspectos, na abordagem baseada em P2P, não há exigência de uso dos modelos de informação e de comunicação do *framework* SNMP, o que aumenta sua flexibilidade quando comparada à abordagem baseada na Script MIB, restrita a estes modelos. Por fim, outro importante aspecto que contribui para a facilidade e a flexibilidade da abordagem baseada em P2P diz respeito ao suporte provido pela infra-estrutura P2P para o desenvolvimento de serviços do ambiente que aprimorem a implantação e a manutenção do próprio ambiente. Tais serviços podem ser concebidos para permitir, por exemplo, a instalação e a atualização facilitada de novos componentes de software em um *peer* ou no próprio ambiente de gerenciamento completo, como discutido na seção 5.4.3, trazendo facilidade para a implantação de novas funcionalidades e para suas atualizações.

Acerca dos contextos modernos analisados como estudos de caso, em virtude de suas características modernas, surgidas recentemente, é esperado que, com a evolução destas redes, serviços adicionais de gerenciamento sejam necessários com freqüência significativa. Tais serviços poderiam representar, por exemplo, necessidades adicionais de monitoração, necessidade de configurar serviços ao longo de vários domínios administrativos, necessidade de interações específicas entre entidades, etc. Assim, em tais contextos, a facilidade e a flexibilidade para o projeto e a implementação de novas funcionalidades oferecidas pela abordagem empregada se tornaria uma característica ainda mais relevante, permitindo que o gerenciamento do contexto atenda às novas necessidades.

8.1.9 Complexidade da Abordagem

O emprego de maior distribuição das ações de gerenciamento em uma abordagem traz associado um aumento da complexidade de sua arquitetura, que envolve o projeto do ambiente e de suas atividades, a instalação e a operação deste, etc. Outros fatores influenciam, ainda, a complexidade da arquitetura, tal como o controle requerido pelas entidades MLMs, os procedimentos para implantação e atualizações requeridos na abordagem, a existência ou não de hierarquia administrativa no ambiente gerenciado, as facilidades e os mecanismos requeridos do ambiente de gerenciamento, etc.

Na arquitetura seguida pelas plataformas tradicionais, o emprego de um pequeno número de entidades de gerenciamento (estações), cada qual concentrando um significativo conjunto de atividades de grande complexidade, torna a operação do ambiente e de suas atividades mais simples quando comparada às abordagens fortemente distribuídas. Nas plataformas tradicionais, cada estação de gerenciamento secundária realiza suas operações de modo independente das demais estações secundárias e a estação principal, embora necessite interagir com as estações secundárias para a operação da abordagem, necessita comunicar-se com apenas um pequeno número de estações. Além disto, tais estações possuem, cada qual, elevada inteligência de gerenciamento e significativa autonomia para realização de suas atividades, o que reduz o controle requerido da estação principal.

Adicionalmente, muitas vezes, as estações secundárias são configuradas diretamente pelo administrador da rede, sem o auxílio ou a interferência da estação principal. Tal aspecto, por um lado, aumenta a complexidade de implantação da abordagem pelo administrador humano, uma vez que exige a configuração de cada estação diretamente, enquanto, por outro lado, diminui a complexidade da arquitetura da abordagem propriamente dita, já que a definição das atividades e do escopo de gerenciamento de cada estação é realizada diretamente pelo administrador humano.

Por fim, as entidades nesta abordagem possuem papéis pré-definidos pelos administradores humanos, com estrutura hierárquica fixa e permanente, inclusive quanto à hierarquia administrativa entre as estações, o que simplifica sua arquitetura e sua operação.

Considerando, agora, ambas as abordagens fortemente distribuídas, incluindo a baseada na Script MIB e a baseada em P2P, estas apresentam uma maior complexidade em sua arquitetura e na arquitetura de suas atividades de gerenciamento, envolvendo o projeto, o desenvolvimento e a operação destas. Isto ocorre em virtude das atividades de gerenciamento serem agora realizadas através de ações distribuídas em um elevado número de entidades, requerendo mecanismos para a interação entre as entidades, para a coordenação de tais ações e para acesso às informações de gerenciamento distribuídas.

A respeito da abordagem baseada na Script MIB, em adição ao elevado número de entidades agora presentes, o controle requerido da entidade TLM pelas entidades MLMs traz um aumento de complexidade às funções desempenhadas pelas entidades TLMs. Além disto, uma elevada complexidade está presente na implantação da abordagem, já que, tipicamente, a seleção das entidades e seus papéis na hierarquia administrativa envolve um número elevado de entidades. Com uma seleção estática destes papéis, como tipicamente é esperado na abordagem baseada na Script MIB, há um aumento da complexidade para a implantação da abordagem, porém uma diminuição da complexidade da arquitetura no que tange a sua operação em relação à ausência de necessidade de lidar com papéis hierárquicos dinâmicos. Tal estrutura estática para os papéis e para a hierarquia administrativa, contudo, pode inviabilizar seu emprego para o gerenciamento de múltiplos domínios administrativos sem hierarquia entre si, conforme houver sido concebido na solução empregada.

Considerando, por fim, a abordagem baseada em P2P e comparando-a com a abordagem baseada na Script MIB, o menor controle agora requerido das entidades TLMs diminui a complexidade das ações desempenhadas por estas em seus serviços ou aplicações. Eleva, contudo, a complexidade de projeto das entidades MLMs, exigindo maior autonomia e inteligência nos serviços de tais entidades. Um aumento de

complexidade é também causado no ambiente e em suas entidades pela flexibilidade provida pela abordagem com a não exigência de papéis fixos (permanentes) serem assumidos pelas entidades: uma entidade pode assumir diferentes papéis na estrutura das interações, de acordo com a atividade em curso, assumindo, por exemplo, em uma dada atividade, papel de TLM; em outra, papel de MLM. Esta flexibilidade exige o desenvolvimento de entidades e atividades com estruturas distintas das empregadas tradicionalmente, aumentando sua complexidade. Tal flexibilidade, contudo, traz em contrapartida a possibilidade de gerenciar múltiplos domínios administrativos que não possuem hierarquia administrativa entre si, o que não seria apropriado com o emprego de uma estrutura hierárquica de operação com papéis fixos e permanentes, como ocorre na arquitetura de plataformas tradicionais. Adicionalmente, o uso de uma arquitetura baseada em componentes e serviços, que oferece a possibilidade de modelar e de projetar as atividades de gerenciamento de modo mais estruturado através de pequenos módulos, cada qual visando atingir um determinado objetivo, contribui para reduzir a complexidade do projeto das atividades de gerenciamento.

Um aumento na complexidade da implantação do ambiente baseado em P2P é também identificado em virtude da existência de forte distribuição e de outras características de sua arquitetura, que exigem a configuração de parâmetros para sua operação, tais como a definição dos *grupos de peers CRG* no ambiente, a definição dos recursos gerenciados por cada grupo, etc. Por outro lado, o aumento da complexidade decorrente destes aspectos pode ser minimizado com a investigação de arquiteturas que visem aprimorar os mecanismos de implantação e de manutenção do ambiente. Tais mecanismos podem fazer uso das potencialidades oferecidas pela infra-estrutura P2P e, como discutido na seção 5.4.3, prover facilidades que visem, por exemplo, a implantação inicial do ambiente, a auto-instalação e a atualização do software de gerenciamento nas entidades do ambiente, e a manutenção da operação das entidades e dos grupos do ambiente.

Existe ainda, na abordagem baseada em P2P, uma maior complexidade relativa aos mecanismos de controle e de segurança a serem suportados quando esta for aplicada para o gerenciamento de diversos domínios administrativos, como discutido na seção 5.4.1. Estes mecanismos devem permitir o controle do ambiente para que as atividades de gerenciamento sejam realizadas de modo apropriado pelos diversos usuários pertencentes a domínios administrativos distintos, inclusive considerando a existência de diferentes níveis de acesso. Tais mecanismos são necessários em qualquer ambiente que objetive o gerenciamento de diferentes domínios administrativos sem hierarquia entre si e com a realização de operações que envolvam múltiplos domínios simultaneamente.

Por fim, a abordagem proposta, por ser baseada numa infra-estrutura P2P, apresenta maior complexidade em virtude da necessidade de oferecer e manter a própria infra-estrutura P2P, incluindo seus serviços básicos e seus serviços estruturais. Com relação a este aspecto, uma vez que abordagens P2P têm sido utilizadas com sucesso amplamente nas redes atuais em outras áreas de aplicação, discute-se que a experiência já obtida nestas outras abordagens P2P pode ser empregada para o desenvolvimento da camada de infra-estrutura P2P requerida pela arquitetura proposta.

8.2 Considerações Acerca da Análise Comparativa

A partir da análise realizada nas seções anteriores, algumas considerações podem ser tecidas acerca dos benefícios e das limitações da abordagem P2P proposta. Observa-se que a abordagem baseada em P2P compartilha com a abordagem baseada na Script MIB os benefícios resultantes por serem baseadas em um paradigma fortemente distribuído. Entre estes, cumpre destacar a maior escalabilidade resultante, em virtude da redução da concentração do processamento e do tráfego de gerenciamento antes existente em abordagens centralizadas ou fracamente distribuídas; e a maior tolerância a falhas proporcionada, resultante do emprego de um grande número de entidades para a realização das operações e da possibilidade de posicionar as entidades mais próximas aos recursos gerenciados. Ambos os benefícios são também identificados na análise da atividade de *polling* realizada em tais abordagens, sendo a importância destes benefícios ainda mais relevante em virtude desta atividade ser realizada de modo periódico e envolvendo um grande número de equipamentos gerenciados.

Quando comparada à abordagem baseada na Script MIB, a abordagem baseada em P2P proporciona alguns benefícios adicionais, como discutido a seguir. Na abordagem baseada em P2P, na execução de uma atividade de gerenciamento, um menor controle é requerido da entidade TLM, uma vez que as entidades são concebidas para possuir independência e autonomia de outras entidades, possuindo elas mesmas controle sobre como executar (ou solicitar a invocação) das ações distribuídas requisitadas. Este aspecto, combinado com a maior autonomia proporcionada para as entidades, contribui para que mecanismos de controle sejam suportados pelas entidades de modo a possibilitar que estas tomem decisões quanto à execução ou não de ações requisitadas. O suporte à comunicação entre as entidades é mais flexível e facilidades adicionais de comunicação são proporcionadas pelo ambiente, incluindo o serviço estrutural para envio de notificações *publish-subscribe* e os serviços básicos de comunicação providos pela infra-estrutura P2P tal como a difusão de mensagens para grupos e para todos os nodos da rede. A escalabilidade é aprimorada, em virtude do menor controle requerido de entidades TLMs para a execução de atividades e do suporte a serviços de grupo que possibilitam a inclusão de mecanismos de distribuição de carga entre seus membros. A tolerância a falhas é aperfeiçoada, em virtude de aspectos tais como maior autonomia e maior independência proporcionada às entidades, da abordagem ser concebida sem estruturar as ações de gerenciamento em uma hierarquia pré-definida ou constante, do suporte a serviços de grupos que possibilitam a inclusão de mecanismos para que um *peer* assuma as funções de outro *peer* em falha, etc. Por fim, características da abordagem baseada em P2P contribuem para aumentar a facilidade e a flexibilidade para o projeto e a implementação de funcionalidades de gerenciamento na abordagem, tais como o emprego de uma arquitetura baseada em componentes e serviços que permite a composição destes, a possibilidade de fazer uso dos serviços providos pela infra-estrutura P2P e dos serviços estruturais, a não existência de restrição quanto ao modelo de informação empregado, as facilidades providas pelo ambiente para o desenvolvimento de serviços que aprimorem a implantação e a manutenção do próprio ambiente.

Abordagens fortemente distribuídas, contudo, apresentam também características que trazem maior dificuldade para sua utilização, o que é compartilhado por ambas as abordagens fortemente distribuídas. Tais dificuldades são relativas ao aumento da complexidade da arquitetura empregada, envolvendo a implantação, a operação e a

manutenção do próprio ambiente de gerenciamento; a operação das suas atividades; o projeto e o desenvolvimento de novas funcionalidades, etc.

Adicionalmente, observa-se, na abordagem baseada em P2P, um aumento da complexidade das entidades MLMs, resultante da maior autonomia e independência exigida destas, assim como um aumento da complexidade das entidades de gerenciamento em geral, em virtude da necessidade de suporte a papéis hierárquicos dinâmicos para estas, requerido para o gerenciamento de múltiplos domínios administrativos sem hierarquia administrativa entre eles. Identifica-se, ainda, aumento na complexidade para a implantação da abordagem em virtude da forte distribuição e de outras características desta, trazendo a necessidade de configuração de parâmetros para sua operação; aumento na complexidade da arquitetura em virtude da exigência de mecanismos de controle e de segurança quando esta for aplicada para o gerenciamento de diversos domínios administrativos; e o aumento da complexidade do ambiente de gerenciamento em virtude da necessidade de oferecer e manter uma infra-estrutura P2P que provenha serviços básicos e serviços estruturais.

Esta maior complexidade é também identificada na atividade de *polling*, na qual, na arquitetura baseada em P2P, quando a atividade é solicitada, é necessário um mecanismo que realize a configuração de todos os *grupos de entidades CRG* responsáveis pelo gerenciamento de algum equipamento para o qual o *polling* foi solicitado (diferente do que ocorre em plataformas tradicionais, nas quais o gerente tipicamente configura os equipamentos que devem ser monitorados na própria estação de gerenciamento secundária). Adicionalmente, alguns procedimentos e mecanismos são requeridos do ambiente de gerenciamento para que a atividade de *polling* seja realizada, também requeridos e utilizados para outras atividades de gerenciamento no ambiente, tais como a prévia definição e configuração (manual ou automática) de qual *grupo de entidades CRG* será responsável pelo gerenciamento de cada equipamento (com maior complexidade do que ocorre em plataformas tradicionais, nas quais um pequeno número de estações coletoras é empregado, simplificando esta definição) e um mecanismo para que as entidades envolvidas controlem as solicitações de ações recebidas, no caso de múltiplos domínios administrativos serem gerenciados (o que não se aplica em plataformas tradicionais, que apresentam uma estrutura hierárquica permanente e não suportam, assim, tal gerenciamento). Por fim, existe a complexidade relativa à exigência do ambiente oferecer e manter a infra-estrutura P2P e os serviços estruturais de envio de notificações e de armazenamento, utilizados pelos serviços de *polling*.

8.3 Emprego da Abordagem Baseada em P2P para o Gerenciamento de Redes Atuais

As discussões apresentadas nas seções anteriores demonstram que o modelo e a arquitetura baseados em P2P propostos apresentam diversos benefícios quando comparados às outras abordagens analisadas. Apresentam também, porém, algumas características que dificultam sua utilização, relativas à maior complexidade existente na abordagem, especialmente quando comparada à abordagem seguida por plataformas tradicionais, fracamente distribuída. Deste modo, o emprego da abordagem baseada em P2P para o gerenciamento de uma rede deve ser realizado avaliando a necessidade desta abordagem, assim como a adequação de uma abordagem de gerenciamento tradicional.

Nos dias atuais, redes com diferentes características são utilizadas. Algumas destas redes mantêm características tradicionais. Tais redes são controladas por apenas uma equipe de administradores ou por equipes que possuem hierarquia administrativa entre si. Estas redes suportam, deste modo, o emprego de paradigmas de gerenciamento que fazem uso de relações de hierarquia administrativa entre as entidades, como nos paradigmas tradicionais distribuídos hierárquicos.

Entre as redes tradicionais, existem redes que apresentam maior complexidade e relevância, tais como aquelas que possuem um elevado volume e heterogeneidade de recursos e serviços, uma elevada complexidade das operações e dos serviços providos, uma fundamental importância da rede para o funcionamento da organização, etc. Algumas destas redes apresentam, porém, limitações de largura de banda para o tráfego de gerenciamento e ausência de mecanismos para tolerância a falhas (*e.g.*, redundância). Tais redes representam situações cujo gerenciamento a partir dos modelos centralizado e fracamente distribuídos não é o mais indicado, em virtude dos requisitos demandados: tais requisitos, que incluem escalabilidade e tolerância a falhas, são obtidos de modo mais apropriado através de modelos fortemente distribuídos, como discutido ao longo das seções 8.1.6 e 8.1.7. A abordagem baseada em P2P proposta segue um paradigma fortemente distribuído e pode ser utilizada para o gerenciamento destas redes. A abordagem, além de propiciar a forte distribuição das ações de gerenciamento, proporciona ainda aprimoramentos em alguns dos requisitos exigidos em tais redes, incluindo escalabilidade e tolerância a falhas, como discutido na análise comparativa.

Por outro lado, algumas redes tradicionais atuais possuem mecanismos de tolerância a falhas e não possuem limitações de largura de banda ou de processamento de gerenciamento. Nestas redes, o gerenciamento pode ser realizado de modo adequado por abordagens tradicionais, tal como, por exemplo, com plataformas tradicionais. Tais redes representam situações em que a abordagem baseada em P2P, embora possa ser aplicada, não é recomendada, já que esta abordagem apresenta uma complexidade mais elevada que as abordagens tradicionais, sem que os benefícios proporcionados por ela sejam requeridos para o gerenciamento do contexto.

Além das redes que mantém características tradicionais, as redes atuais incluem, ainda, aquelas com características modernas, tais como os estudos de caso de contextos modernos discutidos no capítulo 4. Como discutido no referido capítulo e nas seções anteriores, diversos destes contextos possuem características peculiares, que demandam forte distribuição das ações de gerenciamento e impossibilitam o uso de interações entre as entidades de gerenciamento com relações de autoridade e de subordinação entre elas: ao contrário, tais contextos exigem que as entidades da abordagem distribuída possuam autonomia para tomar a decisão se irão ou não executar uma ação requisitada por outra entidade. Entre tais contextos, podem ser citados as redes *mesh* sem fio em que os nodos não pertencem a uma mesma organização, os ataques DDoS que necessitam ser tratados em redes intermediárias e as grades computacionais amplas ou que requerem o gerenciamento também das redes que provêm a interconexão entre seus domínios. Esta estrutura particular na tomada de decisão não é suportada de modo apropriado nos modelos de gerenciamento tradicionais, e representa uma característica que necessita ser suportada pelo modelo seguido para o gerenciamento destes contextos.

A abordagem baseada em P2P suporta tais requisitos. Como discutido na seção 5.4.1, mecanismos para controle da cooperação entre entidades podem ser integrados à arquitetura proposta, de modo que as entidades possam elas próprias tomarem decisões quanto à execução das ações distribuídas solicitadas a elas. Tais mecanismos podem,

por exemplo, empregar políticas para definir o grau e as características de cooperação entre as entidades, considerando aspectos tais como o domínio administrativo a que a entidade requisitante faz parte, as condições correntes da própria entidade, a relevância da ação solicitada, etc., e podem, para isto, inclusive fazer uso de propriedades e de serviços providos pela infra-estrutura P2P, tais como o suporte a grupos, os serviços estruturais, etc. Estes mecanismos podem, também, fazer uso de abordagens da Inteligência Artificial para prover e controlar a cooperação entre os domínios. Adicionalmente, a implantação de mecanismos que propiciam a tomada de decisão das entidades é facilitada na abordagem proposta por algumas características desta, que proporcionam autonomia e independência para as entidades. Entre estas, destaca-se aquela referente ao nível de controle requerido da entidade TLM para as entidades MLMs realizarem suas operações, tal como discutido na análise comparativa (seção 8.1.3). O reduzido controle requerido de outras entidades para a execução de uma ação requisitada e a autonomia e a independência existentes nas entidades da abordagem, que possibilitam que as entidades controlem elas próprias suas funções, facilita o emprego de mecanismos que permitam às entidades avaliar as ações solicitadas e optar ou não pela execução destas. Deste modo, a abordagem baseada em P2P é recomendada para o gerenciamento dos contextos modernos que exigem forte distribuição e não suportam relações com hierarquia administrativa entre suas entidades.

Por fim, os contextos modernos de rede atuais incluem também aqueles em que não é exigida forte distribuição para as atividades de gerenciamento, porém é exigida a interação entre as entidades de gerenciamento sem relações de hierarquia administrativa. Um exemplo de contexto com tais características é o encontrado em grades computacionais de pequena escala em que não é exigido o gerenciamento da infra-estrutura de rede que provê a interconexão entre seus domínios. Nesta situação, modelos fracamente distribuídos podem ser aplicados, porém estes não podem apresentar interações que exijam subordinação administrativa. Tal requisito não é atendido por abordagens como a seguida por plataformas tradicionais, que são baseadas em relações hierárquicas entre as estações. Por outro lado, o gerenciamento pode ser realizado através da abordagem baseada em P2P.

8.4 Considerações Finais

Este capítulo analisou o modelo e a arquitetura baseados em P2P propostos para o gerenciamento das redes atuais. A seção 8.1 apresentou uma análise comparativa entre o modelo e a arquitetura baseados em P2P propostos e duas outras importantes abordagens de gerenciamento distribuído. Esta seção foi seguida por considerações sobre esta análise. Por fim, a seção 8.3 discutiu a adequação da abordagem proposta para o gerenciamento de diferentes redes atuais.

9 UMA TAXONOMIA PARA SOLUÇÕES DE GERENCIAMENTO DE REDES ATUAIS

Como visto anteriormente, no capítulo 3, são duas as principais taxonomias propostas na literatura para paradigmas de gerenciamento de redes distribuídos: a proposta por Martin-Flatin, Znaty e Hubaux (MARTIN-FLATIN; ZNATY; HUBAUX, 1999) (MARTIN-FLATIN, 2003) e a proposta por Schönwälder, Quittek e Kappler (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000). Tais taxonomias foram publicadas há cerca de uma década, apresentando, cada qual, quatro paradigmas para as soluções de gerenciamento de gerenciamento de redes.

Nos dias de hoje, contudo, diversos contextos de rede possuem características peculiares. Tais características deram origem a requisitos de gerenciamento distintos dos encontrados nos sistemas tradicionais, demandando a criação de modelos de gerenciamento inovadores. As particularidades destes novos modelos não são, em muitos aspectos, identificadas e destacadas de modo apropriado nas taxonomias para paradigmas de gerenciamento de redes propostas na literatura.

Este capítulo propõe uma taxonomia para soluções de gerenciamento de redes desenvolvida com o objetivo de destacar as características e os requisitos relevantes requeridos nos modelos de gerenciamento atuais. Esta taxonomia possui como critérios principais o grau de distribuição das ações de gerenciamento e o modo como a tomada de decisão é realizada para a execução destas ações, sendo proposta para classificar soluções de gerenciamento em geral.

O capítulo é organizado como segue. A seção 9.1 analisa as limitações das taxonomias propostas na literatura para a classificação das soluções de gerenciamento requeridas nos contextos de redes atuais. A seção 9.2 apresenta a taxonomia proposta, discutindo os critérios adotados na taxonomia e os paradigmas de gerenciamento propostos, enquanto a seção 9.3 analisa a taxonomia proposta. A seção 9.4 discute a classificação de soluções baseadas no modelo de gerenciamento P2P em relação à taxonomia proposta. Por fim, a seção 9.5 encerra o capítulo.

9.1 Análise das Taxonomias Existentes para Classificação das Soluções de Gerenciamento Atuais

A evolução das redes nos últimos anos deu origem ao surgimento de contextos de rede com características distintas daquelas encontradas nas redes tradicionais. Tais características trouxeram a necessidade do emprego de modelos de gerenciamento capazes de lidar com certas limitações e que possuam alguns requisitos de gerenciamento não encontrados nos modelos tradicionais, tais como: necessidade de monitorar e configurar múltiplos nodos em diversos domínios administrativos para a

operação adequada do serviço ou da própria comunicação da rede; necessidade de interação entre as entidades responsáveis pelo gerenciamento de diferentes equipamentos para o gerenciamento adequado da rede, incluindo equipamentos em diferentes domínios; necessidade de obter informações da rede completa para prover seu efetivo gerenciamento, etc. Tais contextos de rede, denominados neste documento por *contextos modernos*, foram definidos no capítulo 4, que analisou ainda três contextos modernos como estudo de caso: redes *mesh* sem fio, ataques de negação de serviço distribuídos e grades computacionais.

As principais taxonomias para paradigmas de gerenciamento de redes distribuídos propostas na literatura, apresentadas na seção 3.2, compreendem a taxonomia proposta por Martin-Flatin, Znaty e Hubaux (MARTIN-FLATIN; ZNATY; HUBAUX, 1999) (MARTIN-FLATIN, 2003) e a taxonomia proposta por Schönwälder, Quittek e Kappler (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000). Ambas as taxonomias enfocam importantes características de soluções de gerenciamento distribuídas, analisando, cada qual, alguns aspectos em comum e outros aspectos distintos. Tais taxonomias, contudo, não identificam ou destacam de modo apropriado importantes características dos modelos de gerenciamento requeridos atualmente nos contextos modernos de rede, como será discutido a seguir.

9.1.1 Análise dos Estudos de Caso de Contextos Modernos

Retomando como exemplo a análise do contexto moderno **rede *mesh* sem fio**, discutida na seção 4.3.1, se identifica que as soluções mais adequadas para o gerenciamento destas redes são aquelas baseadas em modelos fortemente distribuídos. Dentre estes, quando os nodos da rede pertencem a apenas um domínio administrativo ou a domínios administrativos que possuem hierarquia administrativa entre eles, modelos que envolvam relações de autoridade e subordinação entre as entidades de gerenciamento podem ser empregados.

Tal disposição de hierarquia administrativa para os nodos, contudo, não ocorre em diversas redes *mesh* sem fio, como discutiu a análise realizada na referida seção: em muitas redes, os nodos fazem parte de diferentes domínios administrativos independentes, sem hierarquia entre eles. Esta situação ocorre, por exemplo, nas redes *mesh* sem fio comunitárias (BRUNO; CONTI; GREGORI, 2005) (ISMAEL et al, 2008), onde cada nodo é tipicamente administrado individualmente pelo seu próprio proprietário, sendo esta configuração descrita por alguns autores como o lado extremo de uma rede com múltiplos domínios administrativos (JARRETT; WARD, 2006). Em tais redes, os modelos de gerenciamento a serem empregados necessitam ser reavaliados, atentando-se para a não utilização de modelos que fazem uso de interações entre as entidades com relações de autoridade e subordinação, já que cada domínio deve ter autonomia para tomar suas decisões de gerenciamento. Deste modo, as entidades de diferentes domínios podem interagir e cooperar para a realização das atividades, mas estas interações devem respeitar a autonomia de cada domínio, que deve poder decidir se irá ou não realizar uma ação de gerenciamento solicitada por uma entidade de outro domínio.

Considerando a classificação dos sistemas de gerenciamento segundo a *taxonomia de Martin-Flatin, Znaty e Hubaux*, as condições para o gerenciamento do primeiro grupo de redes *mesh* sem fio (em que os nodos pertencem ao mesmo domínio administrativo ou a domínios com hierarquia administrativa entre eles) o enquadram tanto no paradigma hierárquico fortemente distribuído como no paradigma cooperativo

fortemente distribuído, eliminando-se os demais paradigmas da taxonomia já que estes se baseiam em estruturas centralizadas ou fracamente distribuídas, não apropriadas para o gerenciamento de redes *mesh*. Por outro lado, as soluções de gerenciamento para o segundo grupo de redes *mesh* se enquadrariam apenas no paradigma cooperativo fortemente distribuído, já que este é o único paradigma distribuído desta taxonomia onde não existem relações de subordinação entre as entidades. Contudo, as discussões acerca do paradigma cooperativo fortemente distribuído nesta taxonomia se baseiam na utilização de agentes inteligentes (apresentados na seção A.3), enquanto, nos dias atuais, modelos de gerenciamento que não exigem a subordinação entre as entidades e propiciam a cooperação de entidades podem também ser desenvolvidos fazendo uso de outras abordagens, como será descrito posteriormente. Assim, o enquadramento nesta taxonomia das soluções de gerenciamento do segundo grupo de redes *mesh* acaba por ser demasiadamente restrito, já que acaba por restringir as soluções possíveis para aquelas baseadas em agentes inteligentes.

Considerando agora a *taxonomia proposta por Schönwälder, Quittek e Kappler*, os requisitos para o gerenciamento tanto do primeiro como do segundo grupo de redes *mesh* sem fio enquadram as soluções de gerenciamento possíveis no paradigma fortemente distribuído ou no paradigma cooperativo. A inexistência de diferenciação no enquadramento do gerenciamento destes diferentes tipos de redes *mesh* deve-se ao fato de que esta taxonomia enfoca a estrutura das interações entre as entidades, sem considerar se existem aspectos de autoridade e subordinação entre as entidades da solução analisada. Assim, as soluções apropriadas para o gerenciamento das redes de ambos os grupos poderiam seguir, segundo a taxonomia, tanto o paradigma fortemente distribuído como o paradigma cooperativo. Para as redes *mesh* do segundo grupo, porém, soluções baseadas nestes paradigmas podem ser seguidas desde que, além dos critérios definidos na taxonomia para os paradigmas, as soluções não façam uso de relações de autoridade e subordinação entre as entidades.

A tabela 9.1 sumariza a análise das soluções apropriadas para o gerenciamento de redes *mesh* sem fio em relação às referidas taxonomias.

Tabela 9.1: Soluções de gerenciamento para redes *mesh* sem fio em relação às principais taxonomias propostas na literatura

Redes *mesh* sem fio	Paradigmas em que as soluções de gerenciamento se enquadram	
	Taxonomia de Martin-Flatin, Znaty e Hubaux	**Taxonomia de Schönwälder, Quittek e Kappler**
1º grupo – Soluções de gerenciamento para redes cujos nodos pertencem a um único domínio administrativo ou a domínios que possuem hierarquia administrativa entre si	Paradigma hierárquico fortemente distribuído e paradigma cooperativo fortemente distribuído.	Paradigma fortemente distribuído e paradigma cooperativo.
2º grupo – Soluções de gerenciamento para redes cujos nodos pertencem a diferentes domínios administrativos independentes, sem hierarquia administrativa entre si	Apenas o paradigma cooperativo fortemente distribuído, já que os demais paradigmas são baseados em relações de autoridade e subordinação. Contudo, para enquadrar adequadamente a solução neste paradigma, esta deve ser baseada em agentes inteligentes.	Paradigma fortemente distribuído e paradigma cooperativo. A solução de gerenciamento pode seguir qualquer um destes dois paradigmas, porém, além dos critérios definidos pelos paradigmas, deve ainda não fazer uso de relações de autoridade e subordinação.

Outro exemplo de contexto moderno cuja análise pode ser retomada para avaliar as taxonomias propostas na literatura é o representado pelos **ataques de negação de serviço distribuídos**. Apresentada na seção 4.3.2, esta análise abordou a necessidade de muitos tipos de ataques DDoS serem detectados e tratados nas redes intermediárias (entre as máquinas origem do ataque e a máquina alvo) e arrazoou que tais mecanismos representam soluções de gerenciamento distribuídas. Adicionalmente, discutiu ainda as características de dois mecanismos em particular que seguem esta abordagem para detectarem, reagirem e tratarem ataques DDoS, descritos em (IOANNIDIS; BELLOVIN, 2002) e em (ZHANG; PARASHAR, 2006). Como discutido na análise, em virtude da necessidade destas soluções serem executadas em roteadores presentes em vários pontos da Internet, que representam equipamentos de rede pertencentes a múltiplos domínios administrativos, estas soluções são baseadas em modelos fortemente distribuídos em que não há relações de autoridade e subordinação entre as entidades.

Considerando a *taxonomia proposta por Martin-Flatin, Znaty e Hubaux*, tais modelos poderiam se enquadrar apenas no paradigma cooperativo fortemente distribuído, já que os demais paradigmas distribuídos são baseados em relações de autoridade e subordinação entre as entidades. Contudo, uma vez que o paradigma cooperativo fortemente distribuído é apresentado nesta taxonomia associado ao uso de agentes inteligentes, o enquadramento neste paradigma das soluções em geral para detecção e reação aos ataques possui restrições, já que exige que tais soluções sejam baseadas em agentes inteligentes. Por fim, considerando as duas soluções de gerenciamento avaliadas de modo específico na análise realizada (seção 4.3.2), o

enquadramento no paradigma é questionável, uma vez que tais referências não apontam o uso de agentes inteligentes.

Analisando agora a classificação da *taxonomia proposta por Schönwälder, Quittek e Kappler*, os mecanismos para detecção e reação aos ataques DDoS em redes intermediárias se enquadram tanto no paradigma fortemente distribuído como no paradigma cooperativo, já que ambos descrevem modelos com um elevado número de gerentes em relação ao número total de entidades. Porém, ao empregar uma solução de gerenciamento baseada nestes paradigmas para o gerenciamento deste contexto, deve ainda ser verificado se tal solução suporta a autonomia entre as entidades, sem ser baseada em relações de autoridade e subordinação entre estas. Considerando, por fim, as duas soluções de gerenciamento avaliadas de modo específico na análise, ambas seguem o paradigma cooperativo segundo esta taxonomia, já que todos os roteadores envolvidos no mecanismo podem ser enquadrados no papel de gerentes de nível intermediário, e, assim, o número de entidades com papel de gerente equivale ao número de entidades do ambiente de gerenciamento.

A tabela 9.2 sumariza a análise dos mecanismos para detecção e reação a ataques DDoS analisados em relação às taxonomias propostas na literatura.

Tabela 9.2: Mecanismos para detecção e reação a ataques DDoS em relação às principais taxonomias propostas na literatura

	Paradigmas em que as soluções de gerenciamento se enquadram	
Ataques de negação de serviço (DDoS)	**Taxonomia de Martin-Flatin, Znaty e Hubaux**	**Taxonomia de Schönwälder, Quittek e Kappler**
Mecanismos para detecção e reação a ataques DDoS que necessitam ser executados em redes intermediárias (mecanismos em geral).	Apenas paradigma cooperativo fortemente distribuído, já que os demais paradigmas distribuídos são baseados em relações de autoridade e subordinação. Contudo, para enquadrar adequadamente o mecanismo neste paradigma desta taxonomia, ele deve ser baseado em agentes inteligentes.	Paradigma fortemente distribuído e paradigma cooperativo. O mecanismo pode seguir qualquer um destes paradigmas, porém deve ainda não fazer uso de relações de autoridade e subordinação entre as entidades.
Mecanismo proposto por Ioannidis e Bellovin. Mecanismo proposto por Zhang e Parashar.	Enquadramento destes mecanismos no paradigma cooperativo fortemente distribuído é questionável, uma vez que suas referências não apontam o uso de agentes inteligentes.	Paradigma cooperativo.

Finalmente, apresentada na seção 4.3.3, a análise do contexto **grades computacionais** também pode ser discutida como exemplo de contexto moderno de rede cujas características de gerenciamento não são destacadas de modo apropriado pelas taxonomias propostas na literatura. As operações em grades computacionais envolvem a coordenação e o compartilhamento de recursos computacionais dispersos em múltiplos domínios administrativos. Deste modo, a operação adequada de uma grade inclui, entre outros fatores, o gerenciamento da infra-estrutura de rede utilizada pela grade em seus diversos domínios administrativos de modo a manter a infra-estrutura de

rede operando de modo correto e com os requisitos de QoS adequados para que os diversos recursos da grade possam ser acessados e utilizados conforme necessário. Tal gerenciamento envolve atividades de monitoração e de configuração de parâmetros das redes que são utilizados por operações da grade como escalonamento, migração e monitoração de *jobs*.

A análise realizada acerca deste contexto abordou tanto as características das soluções de gerenciamento de infra-estruturas de rede utilizadas por grades computacionais em geral como duas soluções específicas propostas na literatura, descritas em (CAMINERO et al, 2007) (TOMAS et al, 2009) e em (NEISSE, 2004). Nesta análise, foi destacado que as infra-estruturas de redes utilizadas pelas grades computacionais envolvem tipicamente diversos domínios administrativos, sendo cada infra-estrutura controlada por uma equipe de administradores de rede distinta. Além disto, a equipe administradora da grade é, usualmente, distinta da equipe administradora da rede, caracterizando um cenário com múltiplas equipes de administradores, sem hierarquia administrativa entre estes. Por fim, se discutiu que, em alguns cenários, pode ser necessário também o gerenciamento das redes que provêem a interconexão entre os domínios administrativos onde a grade é executada, exigindo o gerenciamento não apenas das redes nos domínios que atendem a grade, mas também de redes pertencentes a domínios totalmente diversos.

Em virtude destas características, as soluções de gerenciamento para este contexto não podem ser baseadas em modelos centralizados ou que envolvam relações de autoridade e subordinação entre as entidades, já que não existe tal forma de relacionamento entre os domínios ou entre o gerenciamento da grade e o gerenciamento da infra-estrutura de rede utilizada pelas grades. Por outro lado, modelos que não empreguem tais relações podem ser empregados. Em contextos onde a grade não possuir escala excessivamente ampla e não for exigido o gerenciamento das redes que provêem a interconexão entre os domínios administrativos, tais modelos podem ser baseados em estruturas fracamente distribuídas e fortemente distribuídas. Já em contextos em que a grade atingir maior escala ou em contextos em que as redes que provenham a interconexão também devam ser gerenciadas, modelos baseados em estruturas fracamente distribuídas são tipicamente inadequados, já que há um elevado número de equipamentos para serem controlados.

Em relação às duas soluções de gerenciamento de infra-estruturas de rede para grades avaliadas de modo específico na análise realizada, a solução proposta por Neisse (NEISSE, 2004) segue uma abordagem fracamente distribuída em que existem interações através da solução apenas entre as entidades do sistema de grade e as entidades do sistema de gerenciamento da rede responsáveis pelo mecanismo de tradução de cada domínio: interações diretas entre as entidades de gerenciamento de rede de diferentes domínios não ocorrem. Adicionalmente, a análise de tal solução permite identificar que esta é uma situação onde as interações entre as entidades do sistema de grade e as entidades responsáveis pelo mecanismo de tradução de políticas interagem sem existência de autoridade e subordinação entre as entidades, cabendo à entidade responsável pelo mecanismo de tradução avaliar se cada solicitação será atendida e como, em função das opções definidas pelo administrador da rede daquele domínio. Em relação à solução proposta por Caminero e outros (CAMINERO et al, 2007) e Tomas e outros (TOMAS et al, 2009), esta segue uma abordagem fracamente distribuída na qual as ações de gerenciamento são solicitadas pela entidade responsável pelo escalonamento dos *jobs* da grade naquele domínio. Esta entidade interage com uma

entidade de gerenciamento do domínio (entidade BB) para que ela obtenha as informações de desempenho dos roteadores e controle a largura de banda efetiva entre dois pontos da rede do domínio. Detalhes sobre os mecanismos utilizados pela entidade BB para definir como será a execução das ações de gerenciamento não são fornecidos nas referências.

Considerando a *taxonomia proposta por Martin-Flatin, Znaty e Hubaux*, as condições para o gerenciamento de infra-estruturas de rede para grades em geral se enquadrariam apenas no paradigma cooperativo fortemente distribuído, já que este é o único paradigma da taxonomia que considera estruturas distribuídas sem relações de autoridade e subordinação. Entretanto, como discutido anteriormente, este paradigma é associado ao uso de agentes inteligentes, o que traz restrições ao enquadramento das soluções de gerenciamento de grades no paradigma, exigindo que tais soluções sejam baseadas em agentes inteligentes. Por fim, considerando as duas soluções de gerenciamento de infra-estruturas de rede para grades avaliadas de modo específico na análise realizada, o enquadramento no paradigma cooperativo fortemente distribuído não é apropriado, uma vez que tais referências não fazem uso de agentes inteligentes e não são fortemente distribuídas.

Analisando agora a *taxonomia proposta por Schönwälder, Quittek e Kappler*, as condições para o gerenciamento das infra-estruturas de rede para grades onde não for exigido o gerenciamento das redes que provêm a interconexão entre os domínios administrativo enquadrariam estas soluções no paradigma fracamente distribuído, no paradigma fortemente distribuído e no paradigma cooperativo. Por outro lado, em cenários onde também o gerenciamento das redes que provêem a interconexão seja necessário, os modelos baseados no paradigma fracamente distribuídos são tipicamente inadequados. Contudo, em ambos os cenários, um modelo baseado nestes paradigmas só pode ser empregado para tal gerenciamento se o modelo não possuir relações de autoridade e subordinação entre as entidades, aspecto que não é abordado na taxonomia. Considerando, por fim, as soluções de gerenciamento avaliadas de modo específico na análise, ambas podem ser enquadradas no paradigma fracamente distribuído.

A tabela 9.3 sumariza a análise das soluções de gerenciamento apropriadas para o gerenciamento de infra-estruturas de rede utilizadas por grades computacionais em relação às referidas taxonomias.

Tabela 9.3: Soluções para gerenciamento de infra-estruturas de rede para grades computacionais em relação às principais taxonomias propostas na literatura

Grades computacionais	Paradigmas em que as soluções de gerenciamento se enquadram	
	Taxonomia de Martin-Flatin, Znaty e Hubaux	**Taxonomia de Schönwälder, Quittek e Kappler**
Soluções para gerenciamento de infra-estruturas de rede para grades computacionais (soluções em geral).	Apenas paradigma cooperativo fortemente distribuído, já que os demais paradigmas distribuídos são baseados em relações de autoridade e subordinação. Contudo, para enquadrar adequadamente a solução neste paradigma, a solução deve ser baseada em agentes inteligentes.	Para os cenários onde não é necessário o gerenciamento das redes que provém a interconexão entre os domínios administrativos pertencentes à grade: paradigma fracamente distribuído, paradigma fortemente distribuído e paradigma cooperativo. Para os cenários onde é necessário: paradigma fracamente distribuído é inadequado. Em ambos os cenários, além dos critérios definidos pelos paradigmas, a solução de gerenciamento deve também não fazer uso de relações de autoridade e subordinação.
Solução proposta por Neisse. Solução proposta por Caminero e outros e por Tomas e outros.	Enquadramento no paradigma cooperativo fortemente distribuído não é adequado, já que tais referências não fazem uso de agentes inteligentes e não são fortemente distribuídas.	Paradigma fracamente distribuído

9.1.2 Modelo de Gerenciamento Distribuído Baseado em P2P

Como abordado ao longo dos capítulos anteriores, o modelo de gerenciamento distribuído baseado em P2P proposto neste documento pode ser utilizado para o desenvolvimento de soluções de gerenciamento para contextos de rede como os exemplos acima analisados, assim como para outros contextos de redes atuais. Em virtude de suas características, as soluções de gerenciamento baseadas neste modelo podem também ser discutidas como exemplos de soluções que, muitas vezes, não são classificadas de modo apropriado, ou da forma mais adequada, segundo as taxonomias discutidas.

Em relação à *taxonomia proposta por Martin-Flatin, Znaty e Hubaux*, as soluções de gerenciamento típicas baseadas no referido modelo, por serem fortemente distribuídas, se enquadrariam apenas no paradigma hierárquico fortemente distribuído ou no paradigma cooperativo fortemente distribuído. Contudo, o paradigma cooperativo fortemente distribuído desta taxonomia é baseado no uso de agentes inteligentes, o que não ocorre em tal modelo, impedindo, assim, o enquadramento na taxonomia das soluções de gerenciamento baseadas no modelo que proporcionam autonomia para suas entidades definirem se desejam ou não executar a ação. Adicionalmente, embora não seja o uso típico deste modelo, se a solução adotar uma abordagem fracamente distribuída, também esta não poderá ser enquadrada na taxonomia se proporcionar

autonomia para suas entidades, já que não existe um paradigma que atenda tais características.

Por fim, considerando a *taxonomia proposta por Schönwälder, Quittek e Kappler*, tipicamente as soluções baseadas no referido modelo se enquadram no paradigma fortemente distribuído ou o paradigma cooperativo da taxonomia. Não existem, nesta taxonomia, limitações para enquadrar uma solução de gerenciamento baseada neste modelo. Contudo, de acordo com o contexto para o qual a solução for empregada, em adição às características consideradas na taxonomia, outras importantes características adicionais necessitam também ser atendidas pela solução, relativas à impossibilidade do uso de relações de autoridade e subordinação nas interações entre suas entidades, como discutido anteriormente para os contextos modernos.

9.1.3 Limitações das Taxonomias Propostas na Literatura

A partir da análise dos três contextos modernos e do modelo distribuído baseado em P2P discutidos acima, é possível identificar diversas situações em que as duas principais taxonomias propostas na literatura possuem limitações para identificar e destacar de modo apropriado importantes características dos modelos de gerenciamento requeridos atualmente, relativas aos aspectos para a tomada de decisão para a execução das ações distribuídas.

Em relação à **taxonomia de Martin-Flatin, Znaty e Hubaux**, esta taxonomia tem como uma de suas importantes características o fato de considerar e explorar em sua classificação a existência de delegação vertical, explicada como uma forma de delegação onde um gerente de nível N delega uma tarefa de gerenciamento para um subordinado no nível N+1, descendo a hierarquia. Os autores explicam que o gerenciamento é distribuído de forma hierárquica quando a delegação vertical é empregada, definindo dois paradigmas hierárquicos: o paradigma hierárquico fracamente distribuído e o paradigma hierárquico fortemente distribuído.

Esta taxonomia, contudo, possui restrições para a classificação no paradigma cooperativo fortemente distribuído. Se considerarmos que tal paradigma engloba as soluções de gerenciamento fortemente distribuídas em geral em que não existem relações de subordinação entre as entidades, este paradigma tem como limitação ser descrito reportando ao uso de agentes inteligentes, atribuindo aos sistemas cooperativos a necessidade do emprego de tal abordagem e desconsiderando sistemas sem subordinação que façam uso de outros mecanismos para proporcionar a autonomia das entidades para a tomada de decisão. De fato, atualmente, é possível se identificar outras abordagens que podem ser empregadas para o desenvolvimento de soluções sem subordinação entre as entidades, sendo o modelo de gerenciamento baseado em P2P uma destas: associando, por exemplo, o emprego de políticas à aceitação do *peer* por executar uma ação de gerenciamento, o sistema que faz uso do modelo adotará um paradigma sem relações de autoridade e subordinação entre as entidades, proporcionando à entidade autonomia para decidir se deseja ou não executar a ação requisitada. Se, por outro lado, considerarmos que o paradigma cooperativo fortemente distribuído da referida taxonomia engloba as soluções de gerenciamento baseadas unicamente em agentes inteligentes, então a taxonomia possui como restrição a ausência de um paradigma para as demais soluções de gerenciamento que não possuem relações de autoridade e subordinação.

Outra restrição que a taxonomia de Martin-Flatin, Znaty e Hubaux possui diz respeito às soluções de gerenciamento fracamente distribuídas que não possuem relações de autoridade e subordinação entre as entidades, tais como a solução de gerenciamento de infra-estruturas de redes para grades proposta em (NEISSE, 2004) e outras possíveis soluções apropriadas para o gerenciamento deste contexto. A taxonomia em questão não inclui um paradigma fracamente distribuído não hierárquico, porém as soluções de gerenciamento atuais podem exibir tais características.

As considerações apresentadas acima exemplificam as limitações que esta taxonomia possui quanto ao aspecto das relações de autoridade e subordinação entre as entidades das soluções de gerenciamento. A taxonomia tem como importante benefício discutir a existência de delegação vertical junto a suas definições, porém os paradigmas propostos acabam por não explorar este aspecto de modo a abranger todas as soluções de gerenciamento dos dias atuais.

Em relação à taxonomia de **Schönwälder, Quittek e Kappler**, esta se concentra na estrutura das interações entre as entidades, sem considerar se existem ou não relações de autoridade e subordinação entre elas: a taxonomia enfoca apenas a estrutura hierárquica surgida pelas formas de comunicação entre as entidades. Tal taxonomia tem como característica particular ter seu critério principal quantitativo, em que o paradigma é definido considerando o número relativo de gerentes na solução (isto é, o número total de gerentes em relação ao número total de entidades). Este aspecto difere da forma utilizada na taxonomia discutida anteriormente, cujos paradigmas eram definidos através da discussão de aspectos organizacionais.

A utilização de um critério quantitativo como o adotado torna esta taxonomia flexível e abrangente, já que todas as soluções de gerenciamento existentes acabam por poder ser enquadradas em um dos paradigmas da taxonomia. Entretanto, tal aspecto acaba por tornar a classificação excessivamente genérica ao classificar as soluções de gerenciamento de contextos modernos tais como os discutidos anteriormente, sem abordar as relações de autoridade e subordinação ou de autonomia entre as entidades. Assim, embora tanto as soluções em geral como as soluções específicas dos três contextos analisados possam ser enquadradas em paradigmas da taxonomia, esta taxonomia possui restrições importantes ao ser empregada para melhor compreensão das soluções de gerenciamento atuais, em virtude da ausência de aspectos que destaquem de modo específico a necessidade das entidades possuírem ou não autonomia e poder de decisão nas suas interações com outras entidades, características que estão entre as mais importantes ao se discutir as particularidades das soluções de gerenciamento em contextos modernos.

9.2 Taxonomia Proposta

A discussão apresentada na seção anterior permite observar a importância da análise das soluções de gerenciamento requeridas pelas redes atuais considerar não apenas a distribuição das ações de gerenciamento, mas também as características da solução relativas ao controle, à autoridade e à autonomia nas interações entre as entidades. A taxonomia proposta neste documento tem como objetivo destacar tais aspectos, propondo uma classificação para soluções de gerenciamento em geral baseada na combinação de dois critérios principais, como será descrito nas seções 9.2.2 e 9.2.3.

9.2.1 Terminologia

Os termos utilizados nas diferentes taxonomias de gerenciamento de redes são freqüentemente empregados com significados distintos. Assim, a fim de evitar ambigüidades na taxonomia aqui proposta, alguns termos utilizados no restante do capítulo são aqui revisados e definidos.

A taxonomia proposta visa classificar "***soluções de gerenciamento"*** em geral. Tais soluções podem compreender diversos cenários, incluindo um único sistema que abrange um ou mais domínios administrativos, diversos sistemas integrados que em conjunto proporcionam o gerenciamento de um ou mais serviços da rede, e até mesmo diversos sistemas de gerenciamento não integrados e sem interação que, embora isolados, acabam por proporcionar o gerenciamento requerido no contexto (tal como nas abordagens estanques que serão posteriormente discutidas).

As *soluções de gerenciamento* proporcionam a realização de uma ou mais funcionalidades de gerenciamento através de atividades executadas pela solução. Na taxonomia, a expressão *"**atividade de gerenciamento"*** será empregada para representar um conjunto de *"**ações de gerenciamento"***, que podem ser executadas de modo distribuído em diversas entidades, e que, em conjunto, provém a atividade requerida (*e.g.*, configuração do *polling*, monitoração da rede através de *polling*, configuração de requisitos de QoS em um caminho na rede, configuração de um determinado recurso da rede, tratamento e reação a um ataque DDoS, etc.).

Ao discutir as entidades pertencentes à solução de gerenciamento, outro termo que foi identificado que poderia causar ambigüidades é o termo *"**agente"***, que possui diversas interpretações dentro da área de gerenciamento. Como explicado na seção 3.1, o termo *agente* é utilizado para representar um *software que encapsula as informações gerenciadas* ou para definir o *papel que a entidade assume no gerenciamento*, sendo, neste último uso, empregado tanto para destacar que a *entidade assume apenas funções mundanas, sem inteligência de gerenciamento e limitada ao papel de mera fornecedora de dados*, como para destacar que a *entidade executa suas funções sem necessitar dos demais, podendo assumir funções de maior complexidade*.

Em virtude destas diversas interpretações existentes, o termo *agente* será evitado na presente taxonomia sempre que possível, sendo substituído por outros termos conforme o enfoque que se deseja destacar. Neste contexto, a expressão *"**entidade fornecedora de dados simples"*** será empregada ao se referir ao conceito atribuído aos agentes dos modelos de gerenciamento iniciais, que não possuíam nenhuma inteligência do gerenciamento e possuíam o papel de meros fornecedores de dados. Em oposição a estes, as entidades responsáveis pelo processamento e pela inteligência de gerenciamento, que executam as ações de gerenciamento distribuídas e representam o papel dos gerentes tradicionais, serão referenciadas como *"**entidades responsáveis pelo processamento de gerenciamento"***.

Por fim, outros termos que devem ser explanados são os termos *"**hierarquia"*** e *"**hierárquico"***. Como já discutido na seção 3.1, estes termos são empregados na literatura com enfoques distintos. Num enfoque mais amplo, definem o *modo como as entidades são estruturadas e como as interações ocorrem entre tais entidades*, *caracterizando uma hierarquia apenas para a execução das atividades de gerenciamento*. Num enfoque mais específico, são empregadas para *expressar não apenas como é a estrutura para a execução das atividades, mas também para indicar as relações de autoridade e subordinação existentes entre elas*. Neste documento, como

discutido na referida seção, o termo *hierarquia* é empregado usualmente em seu enfoque mais amplo, e quando empregado com seu enfoque mais específico, isto será definido.

A taxonomia segue a mesma abordagem. Utiliza, assim, o termo *hierarquia* ao discutir o modo como as atividades são estruturadas, em seu enfoque mais amplo (*e.g.*, na seção 9.2.5). Mas emprega também os termos *hierarquia* e *hierárquico* ao discutir *como se dá o processo de tomada de decisão* para a execução das ações de gerenciamento. Neste contexto, portanto, os termos evocam o significado de relações de autoridade e subordinação entre as entidades. Tal uso não é contrário ao proposto na seção 3.1, já que os termos são empregados para definir, exatamente, a hierarquia existente no processo de tomada de decisão.

9.2.2 Critério 1: Grau de Distribuição do Processamento de Gerenciamento

A taxonomia proposta é baseada em dois critérios distintos. O primeiro critério analisa a *distribuição do processamento de gerenciamento entre as entidades da rede*, enfocando como se dá a distribuição da complexidade, da inteligência e da execução das ações de gerenciamento. Este critério *não considera as interações entre as entidades* para a realização das diversas ações requeridas à execução de uma funcionalidade de gerenciamento distribuída completa: ele enfoca apenas a ocorrência e a quantidade de ações distribuídas executadas, assim como a complexidade e a inteligência de tais ações.

Este critério define três categorias:

- **Abordagens centralizadas**: caracterizadas pela presença de apenas uma entidade que realiza todo o processamento de gerenciamento, concentrando a complexidade, a inteligência e a execução das ações de gerenciamento. As demais entidades, por sua vez, assumem o papel de fornecedoras de dados simples. As abordagens desta categoria compreendem as abordagens mais tradicionais de gerenciamento, nas quais a entidade gerente e as entidades agentes (fornecedoras de dados simples) possuem seus papéis claramente definidos. A entidade gerente é denominada usualmente nestas abordagens por estação de gerenciamento.
- **Abordagens fracamente distribuídas:** caracterizadas pelo suporte da abordagem a uma pequena distribuição do processamento de gerenciamento, de tal modo que a complexidade, a inteligência e a execução das ações de gerenciamento ainda se encontram pouco distribuídas entre as entidades. Estas soluções de gerenciamento possuem, tipicamente, um pequeno número de entidades que realizam diversas ações de gerenciamento de maior complexidade. Outro cenário ocorre quando algumas entidades realizam um pequeno número de ações de média complexidade, mantendo-se a complexidade, a inteligência e a execução da maior parte das ações de gerenciamento ainda concentradas em um número muito restrito de entidades. Um exemplo típico de abordagem fracamente distribuída é a arquitetura empregada em plataformas de gerenciamento de redes tradicionais comerciais largamente utilizadas, na qual existe uma estação de gerenciamento principal e algumas estações secundárias que recuperam as informações de gerenciamento dos equipamentos de rede.

- **Abordagens fortemente distribuídas:** caracterizadas pelo suporte da abordagem a uma grande distribuição do processamento de gerenciamento, de tal modo que a complexidade, a inteligência e a execução das ações de gerenciamento podem ser distribuídas para um elevado número ou para todas as entidades da abordagem. Exemplos de abordagens fortemente distribuídas incluem modelos baseados na Script MIB, e o modelo de gerenciamento distribuído baseado em P2P proposto neste documento.

A figura 9.1 esquematiza alguns exemplos de cenários para as três categorias. No esquema *a*, uma *abordagem centralizada* é demonstrada, com a presença de apenas uma entidade que executa todo o processamento de gerenciamento, e diversas entidades que possuem a função de fornecedoras de dados simples. O esquema *b*, por sua vez, demonstra dois cenários de *abordagens fracamente distribuídas*. No esquema *b.1*, é demonstrado um cenário em que um pequeno número de entidades executam diversas ações de grande complexidade; no esquema *b.2*, é apresentado um cenário em que algumas entidades executam um pequeno número de ações de média complexidade e um número restrito de entidades executa diversas ações de grande complexidade. Por fim, o esquema *c* descreve dois cenários de *abordagens fortemente distribuídas*. No esquema *c.1*, é apresentado um cenário em que diversas entidades realizam o processamento de gerenciamento e há a presença de algumas entidades que realizam a função de fornecedores de dados simples; no esquema *c.2*, é apresentado um cenário onde não existe a presença entidades fornecedoras de dados simples: todas as entidades realizam o processamento de gerenciamento.

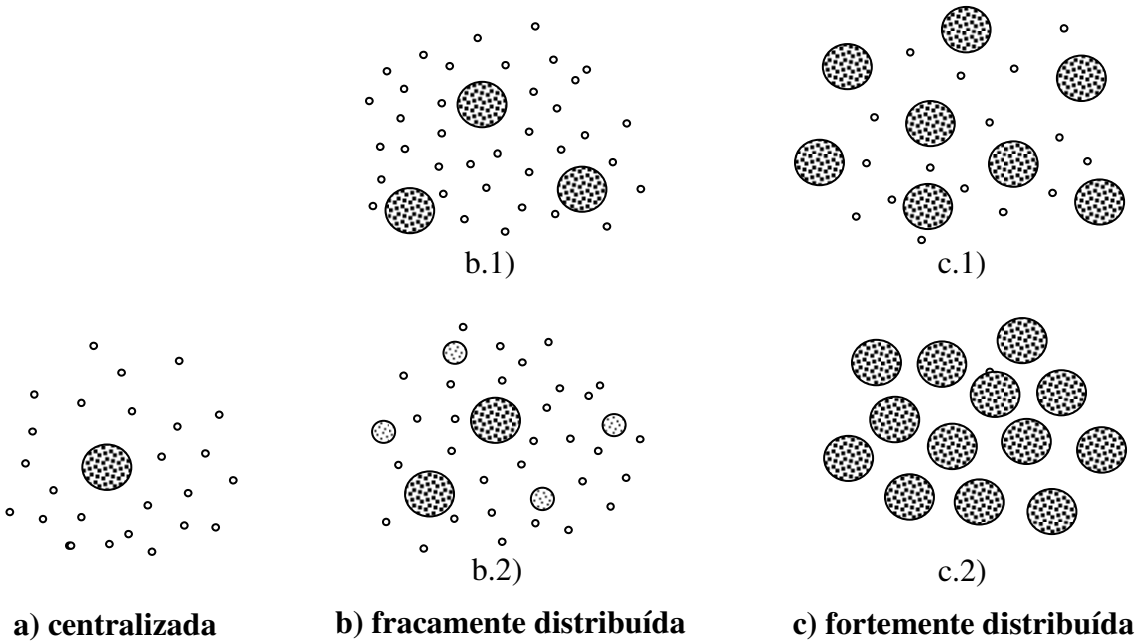


Figura 9.1 Abordagens segundo o critério de distribuição do processamento de gerenciamento

9.2.3 Critério 2: Tomada de Decisão na Execução das Ações Distribuídas

O segundo critério da taxonomia analisa *onde e como se dá a tomada de decisão nas interações entre as entidades* da solução de gerenciamento para a execução das ações distribuídas necessárias para realizar uma atividade completa. Este critério considera *como são as relações entre as entidades para a execução destas ações*, *analisando as interações, a autonomia e o poder de decisão das entidades*. As ações executadas por cada entidade incluem as ações realizadas na própria entidade e aquelas realizadas sobre as entidades fornecedoras de dados simples, responsáveis apenas pelo fornecimento de informações de gerenciamento solicitadas e caracterizadas pela ausência de autonomia e complexidade.

Cinco categorias de abordagens são definidas segundo este critério:

- **Abordagens centralizadas:** caracterizadas pela presença de apenas uma entidade que concentra todo o processamento e é responsável pela tomada de decisão de todas as ações de gerenciamento executadas pela própria entidade.
- **Abordagens distribuídas hierárquicas permanentes:** caracterizadas pela existência de relações de autoridade e subordinação nas interações entre as entidades, existindo uma entidade num nível superior que possui autoridade sobre as demais para a tomada de decisão quanto à execução das ações de gerenciamento delegadas para estas entidades. As entidades subordinadas à entidade no nível superior podem ser organizadas em um único nível hierárquico, sem nenhuma forma de autoridade entre estas, ou em múltiplos níveis, existindo relações de autoridade e subordinação também entre estas entidades. As relações de autoridade e subordinação referidas neste critério dizem respeito à tomada de decisão para a realização das ações de gerenciamento. Nestas abordagens, quando uma entidade com autoridade sobre outra delega a execução de uma ou mais ações de gerenciamento para esta entidade, a entidade subordinada não possui ou ativa mecanismos para avaliar se deseja ou não executar a ação delegada recebida: uma vez recebida a ordem da entidade superior na hierarquia, a entidade irá executar a ação, sem existir autonomia ou iniciativa para esta entidade avaliar se deseja ou não executar a ação. Um importante diferencial desta categoria é que a *definição dos níveis hierárquicos da solução de gerenciamento não se altera*: a entidade de nível superior e as demais entidades de nível intermediário superior (no caso de múltiplos níveis hierárquicos) são constantes para todas as atividades executadas na solução de gerenciamento. Tais entidades, assim, assumem o papel de entidade de nível superior *para a solução de gerenciamento completa*.
- **Abordagens distribuídas hierárquicas variáveis:** caracterizadas pela existência de relações de autoridade e subordinação nas interações entre as entidades *nas atividades sendo executadas*, existindo, *em cada instância de atividade*, *uma entidade num nível superior que realiza a tomada de decisão* que define a execução de ações de gerenciamento para outras entidades inferiores naquela instância. Nestas abordagens, quando uma entidade num nível superior atribui a execução de uma ou mais ações de gerenciamento para outra entidade inferior *na hierarquia daquela instância de atividade* sendo executada, a entidade inferior irá executar a ação, sem avaliar se

deseja ou não executá-la. Porém, diferente do que ocorre nas abordagens distribuídas hierárquicas permanentes, a definição dos níveis hierárquicos não é fixa. Existe uma relação hierárquica entre as entidades *em cada instância de atividade sendo executada*, porém as entidades que assumem o papel de entidade de nível superior *variam em outras instâncias da atividade ou em outras atividades*. Tais entidades, assim, assumem o papel de entidade de nível superior *individualmente para cada instância de atividade, enquanto a solução de gerenciamento como um todo não possui uma estrutura hierárquica na relação entre as entidades*. Esta diferença entre os dois tipos de abordagens assinala uma importante diferença de suas soluções. Enquanto nas *abordagens distribuídas hierárquicas variáveis* as relações hierárquicas têm enfoque apenas operacional, se restringindo à execução de cada atividade, nas *abordagens distribuídas hierárquicas permanentes* as relações hierárquicas tem enfoque também arquitetural da solução e indicam uma relação hierárquica entre as próprias entidades.

- **Abordagens distribuídas cooperativas:** caracterizadas pela ausência de relações de autoridade e subordinação nas interações entre as entidades. As entidades interagem para a execução de ações de gerenciamento de tal modo que uma entidade solicita a outras entidades a execução de uma ou mais ações de gerenciamento, mas cada entidade que recebe o pedido tem autonomia para optar por executar as ações requisitadas ou não. Nesta abordagem, a tomada de decisão acerca da execução da ação solicitada é realizada pela própria entidade que irá executar a ação, sendo esta tomada de decisão realizada a partir das interações e das solicitações recebidas da entidade requisitante e com o intuito de proporcionar, se possível, a cooperação com tal entidade para a realização das atividades de gerenciamento.
- **Abordagens distribuídas estanques:** caracterizadas pela ausência de interações entre as entidades da solução para a execução das atividades de gerenciamento, sem existir nem relações de autoridade e subordinação nem relações de cooperação entre as entidades. Nesta abordagem, existe a presença de diversas entidades de gerenciamento na solução, cada qual com o objetivo de prover o gerenciamento de rede, e as ações são executadas de forma distribuída pelo conjunto de entidades, porém as entidades não interagem de forma explícita para que as ações sejam executadas em cada entidade. Não existe um ponto central de decisão e a tomada de decisão para as ações de gerenciamento é realizada individualmente em cada entidade. Um contexto típico onde esta abordagem pode ocorrer é no gerenciamento realizado em diferentes domínios administrativos que não possuem hierarquia administrativa entre si e que não possuem soluções de gerenciamento integradas ou que cooperem entre si. Este contexto pode ser caracterizado por cenários distintos, incluindo desde aqueles em que existe uma forma de interação externa à abordagem de gerenciamento propriamente dita que permite a execução de ações nas entidades visando um objetivo específico comum (tal como a comunicação entre as equipes administradoras de cada domínio por meios externos à solução de modo que cada equipe configure sua entidade visando tal objetivo comum), até aqueles contextos em que não existe nenhuma forma de interação externa explícita.

Cenários típicos de *abordagens centralizadas* são encontrados nas soluções de gerenciamento tradicionais em que há a presença de uma estação de gerenciamento única. De modo similar, as soluções tradicionais de gerenciamento caracterizadas pela presença de uma estação principal e um conjunto de estações secundárias, tal como em plataformas de gerenciamento comerciais tradicionais, são exemplos típicos de *abordagens distribuídas hierárquicas permanentes*.

Por outro lado, *abordagens distribuídas hierárquicas variáveis* não são tipicamente as utilizadas em soluções de gerenciamento tradicionais. Tais abordagens podem ser empregadas, por exemplo, para o gerenciamento de redes pertencentes a uma mesma organização, em que podem existir separações entre as redes de departamentos ou setores, mas existe uma relação de confiança e parceria quanto às ações requisitadas pelas entidades das outras redes, representando um único domínio administrativo.

Por sua vez, exemplos de abordagens de gerenciamento que podem ser enquadradas na categoria de abordagens distribuídas e não hierárquicas são os modelos empregados para o gerenciamento de diversas funcionalidades da Internet. A Internet é formada por uma enorme quantidade de sistemas autônomos interconectados, sendo cada sistema autônomo operado por uma organização diferente. Em função desta estrutura física e administrativa, os serviços que envolvem mais de um sistema autônomo não são gerenciados em toda sua extensão por um único núcleo de gerência. Diferentes administradores humanos, pertencentes aos diversos sistemas autônomos envolvidos, são responsáveis, cada qual, por parte deste gerenciamento, e, em conjunto, levam a rede a um estado consistente.

Um exemplo típico de serviço cujo gerenciamento envolve vários sistemas autônomos em conjunto é uma transferência de um grande volume de dados com requisitos de QoS em que o caminho na rede entre os computadores origem e destino perpassa vários sistemas autônomos diferentes, como pode ocorrer em transmissões de videoconferência ou na execução de *jobs* em grades computacionais. Nesta situação, pode ser necessário fazer a alocação de banda nos diversos sistemas autônomos, que não possuem hierarquia administrativa entre si, caracterizando, deste modo, um cenário distribuído e não hierárquico, em que não existe um ponto central para a tomada de decisão para a alocação dos recursos, mas sim, pelo contrário, um cenário em que cada domínio possui poder de decisão para definir se realizará ou não a configuração de seus próprios recursos.

Neste cenário, a alocação dos recursos pode ser realizada seguindo modos distintos. Em um modo, a alocação é realizada individualmente em cada sistema autônomo sem nenhuma forma de interação explícita entre as entidades dos diferentes domínios, sendo esta configuração realizada, por exemplo, pelos administradores humanos responsáveis por cada domínio após a prévia comunicação entre estes de forma independente e isolada do sistema de gerenciamento. Este modo de alocação se enquadra na categoria das *abordagens distribuídas estanques*, já que cada domínio é administrado individualmente de modo não integrado com os demais. Em um segundo modo, a alocação é realizada em cada sistema autônomo a partir da interação entre as entidades de gerenciamento, que solicitam a alocação dos recursos através da interação entre as entidades da solução de gerenciamento. Este modo caracteriza uma *abordagem distribuída cooperativa*, na qual as entidades interagem de modo cooperativo para a realização das atividades de gerenciamento, mantendo, contudo, a autonomia de cada uma para a tomada de decisão.

A figura 9.2 esquematiza exemplos de cenários para as cinco abordagens. No esquema *a*, uma *abordagem centralizada* é demonstrada, em que existe apenas uma entidade e esta é responsável por todas as decisões para a execução de ações de gerenciamento. No esquema *b*, um exemplo de cenário para uma *abordagem distribuída hierárquica permanente* com dois níveis é apresentada, no qual a entidade de nível superior possui poder de decisão sobre algumas entidades subordinadas. O esquema *c*, por sua vez, apresenta um cenário para uma *abordagem distribuída hierárquica variável* com duas instâncias de atividades: em cada instância, uma entidade possui poder de decisão sobre as ações que serão executadas em entidades inferiores na hierarquia. A hierarquia atribuída para a tomada de decisão em uma instância de atividade, contudo, pode ser diferente da atribuída em outras instâncias. No esquema *d*, é demonstrado um cenário para uma *abordagem distribuída cooperativa* com três entidades, que interagem sem nenhuma forma de autoridade e subordinação entre elas. Por fim, no esquema *e*, é apresentado um cenário para uma *abordagem distribuída estanque* também com três entidades, caracterizadas pela ausência de interação explícita entre as entidades através da solução de gerenciamento.

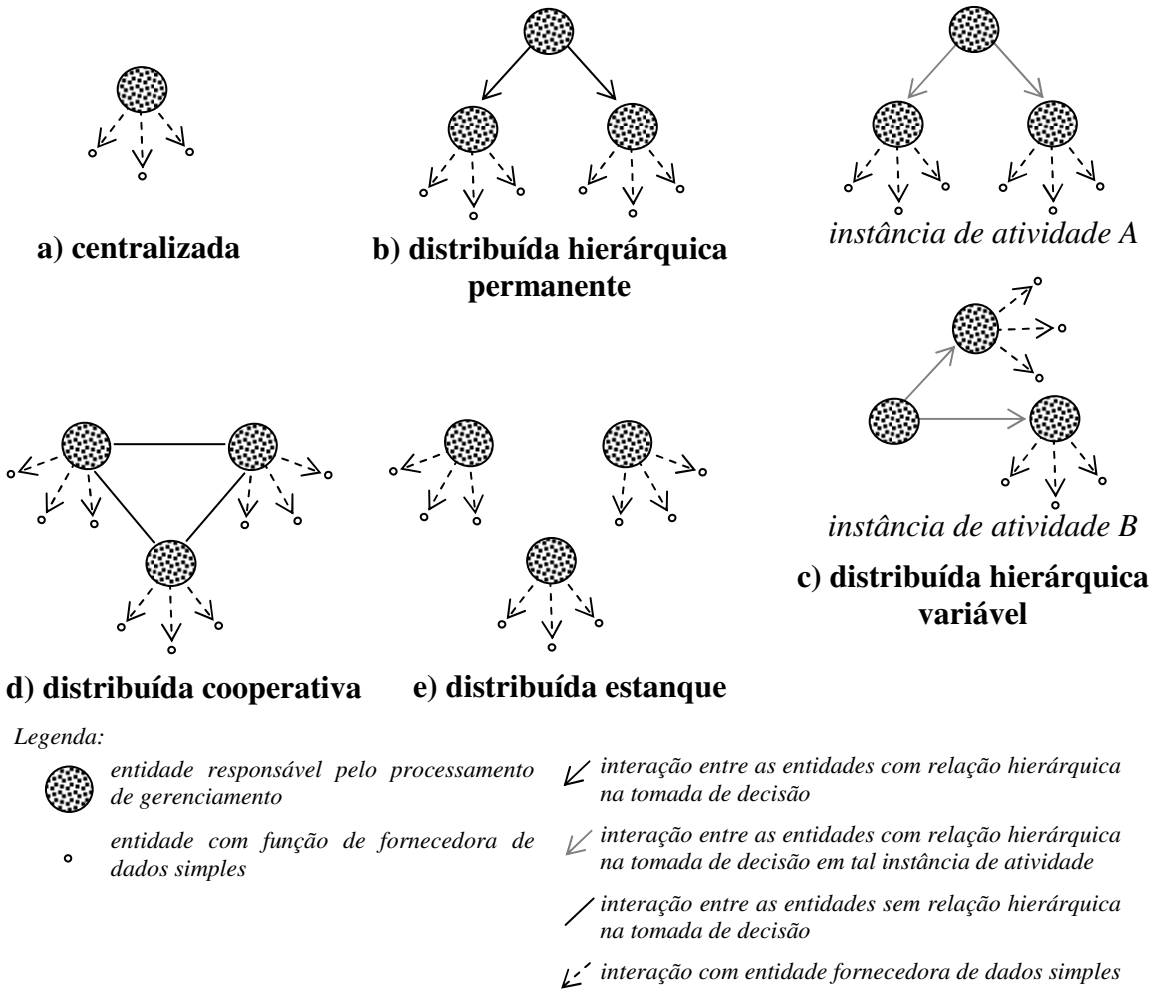


Figura 9.2: Abordagens segundo o critério de tomada de decisão na execução das ações distribuídas

As abordagens definidas são encontradas em cenários reais, freqüentemente, de forma combinada, caracterizando abordagens híbridas nas quais existem diferentes

categorias na estrutura da solução completa. Um cenário típico é no gerenciamento de múltiplos domínios administrativos que não possuem hierarquia administrativa entre eles, no qual cada domínio pode ser administrado internamente por abordagens centralizadas, hierárquicas ou cooperativas, porém a interação entre os domínios não pode envolver relações de hierarquia, sendo realizada através de abordagens estanques ou cooperativas, como acima discutido.

Cabe destacar que as abordagens hierárquicas e cooperativa podem ser encontradas em soluções de gerenciamento que representam tanto um sistema de gerenciamento único como em soluções que representam diversos sistemas integrados. Por sua vez, as abordagens estanques só são identificadas em soluções de gerenciamento que representam mais de um sistema de gerenciamento, nas quais um ou mais serviços requerem, para sua correta operação, o gerenciamento a partir dos diversos sistemas, tal como no exemplo da reserva de banda acima descrito. Nesta situação, cada sistema individual realizará a configuração dos equipamentos de seu próprio domínio. Contudo, o serviço completo desejado — no exemplo, a configuração da reserva de banda completa — envolve não apenas a configuração de cada sistema isolado, mas sim a configuração em todos os sistemas, mesmo que esta configuração se dê de modo não integrado e sem interações entre os sistemas.

Considerando a evolução típica esperada de soluções de gerenciamento de modo a proporcionar maiores facilidades e maior automação no gerenciamento das redes, os paradigmas estanques representam uma etapa anterior em relação aos paradigmas cooperativos aplicados para o gerenciamento de serviços que envolvam múltiplos domínios administrativos.

9.2.4 Paradigmas de Gerenciamento

As categorias dos dois critérios discutidos acima podem ser combinadas a fim de definir paradigmas de gerenciamento distribuídos que consideram, em simultâneo, o grau de distribuição e a tomada de decisão nas soluções de gerenciamento. A tabela 9.4 apresenta os paradigmas resultantes.

Tabela 9.4: Paradigmas de gerenciamento

	Abordagem Centralizada	**Abordagem Fracamente Distribuída**	**Abordagem Fortemente Distribuída**
Abordagem Centralizada	Paradigma Centralizado	-	-
Abordagem Distribuída Hierárquica Permanente	-	Paradigma Fracamente Distribuído Hierárquico Permanente	Paradigma Fortemente Distribuído Hierárquico Permanente
Abordagem Distribuída Hierárquica Variável		Paradigma Fracamente Distribuído Hierárquico Variável	Paradigma Fortemente Distribuído Hierárquico Variável
Abordagem Distribuída Cooperativa	-	Paradigma Fracamente Distribuído Cooperativo	Paradigma Fortemente Distribuído Cooperativo
Abordagem Distribuída Estanque	-	Paradigma Fracamente Distribuído Estanque	Paradigma Fortemente Distribuído Estanque

A taxonomia proposta neste documento é, assim, composta pelos seguintes paradigmas de gerenciamento:

- Paradigma Centralizado
- Paradigma Fracamente Distribuído Hierárquico Permanente
- Paradigma Fracamente Distribuído Hierárquico Variável
- Paradigma Fracamente Distribuído Cooperativo
- Paradigma Fracamente Distribuído Estanque
- Paradigma Fortemente Distribuído Hierárquico Permanente
- Paradigma Fortemente Distribuído Hierárquico Variável
- Paradigma Fortemente Distribuído Cooperativo
- Paradigma Fortemente Distribuído Estanque

9.2.5 Aspecto Complementar: Nível de Controle Requerido de Outras Entidades para que as Ações Distribuídas Referentes a uma Atividade Completa Sejam Realizadas

Em adição aos critérios principais que definem o paradigma de gerenciamento, a taxonomia propõe um aspecto complementar a ser observado nas soluções de gerenciamento para auxiliar a compreensão de aspectos adicionais desta. Este aspecto visa analisar qual o nível de controle requerido das entidades de gerenciamento sobre outras entidades para que as ações sejam realizadas de modo apropriado nestas e a

atividade de gerenciamento completa seja executada. Visa, conjuntamente, analisar o nível de autonomia existente nas entidades para estas realizarem suas ações sem auxílio externo. O controle aqui discutido *não diz respeito a como se dá a tomada de decisão, isto é, ao controle existente ou não na entidade que autoriza ou não a realização das operações*. Ele *considera, sim, como são as seqüências de interações e os mecanismos requeridos através da solução de gerenciamento para que uma atividade de gerenciamento que compreende a execução de ações em entidades distribuídas seja realizada de forma completa e adequada*.

Na discussão deste aspecto, é empregada a nomenclatura que considera a estrutura hierárquica formada nas interações entre as entidades para a realização das atividades de gerenciamento, fazendo uso do termo hierarquia *apenas para definir o modo como as entidades são estruturadas e como a comunicação é desempenhada entre elas*, sem levar em conta nenhum quesito relativo à tomada de decisão ou às relações de autoridade e subordinação existentes. Tal uso é baseado naquele discutido por Schönwälder, Quittek e Kappler (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000), que explica que as disposições das entidades no sistema de gerenciamento implica em uma estrutura hierárquica. Assim, baseia-se numa nomenclatura na qual as entidades que tipicamente requerem ou iniciam a atividade de gerenciamento são referenciadas como *top-level manager* (TLM), ou *gerentes de nível superior*. As demais entidades que executam as ações distribuídas para a execução completa da atividade são referenciadas como *mid-level manager* (MLM), ou *gerentes de nível intermediário*. Uma vez que os gerentes de nível intermediário também podem requerer ações para outros gerentes de nível intermediário inferiores na estrutura de execução, para a análise deste aspecto complementar, as entidades da solução de gerenciamento são preferencialmente referenciadas como *entidade de nível superior*, para a entidade que requisita a ação, e *entidade de nível inferior*, para a entidade que executa a ação requerida.

Este aspecto complementar da taxonomia não é definido através de categorias discretas específicas: ele pode ser compreendido como um espectro de situações, variando desde soluções de gerenciamento nas quais é requerido um controle elevado por parte das entidades de nível superior para a execução das ações distribuídas e as entidades não possuem autonomia para realizar suas ações, até soluções nas quais todas as ações são realizadas sem nenhuma forma de controle externo e as entidades são totalmente autônomas. Exemplos de níveis de controle que podem ser encontrados nas atividades incluem:

- Controle mediano é requerido da entidade de nível superior para que as ações sejam realizadas; a entidade (entidade de nível inferior) não possui autonomia para realizar suas ações de modo independente. Um exemplo é a interação requerida para a utilização da Script MIB: tipicamente a entidade que executa a Script MIB (entidade de nível inferior) requer da entidade de nível superior diversas operações para que as ações de gerenciamento sejam realizadas, incluindo transferir o *script*, iniciar a execução deste, monitorar sua execução, etc.
- Controle é requerido da entidade de nível superior para que as ações sejam realizadas em conjunto, tal como numa composição de serviços. A entidade possui autonomia para executar suas ações de modo independente, sem requerer controle de outra entidade. Porém, para que a atividade de gerenciamento completa seja realizada de modo efetivo, uma ou mais

entidades são responsáveis por controlar a seqüência de ações. Considerando a estrutura entre as entidades para a execução das ações de gerenciamento, é requerido da entidade de nível superior um grau de controle muito pequeno, tal como apenas requisitar a execução da ação na seqüência apropriada e obter o resultado desta. Um cenário típico é uma composição de serviços em que cada entidade tem inteligência e autonomia para realizar o serviço individual requerido a ela, porém o serviço completo exige que as entidades interajam de acordo com a seqüência específica. Um exemplo é o controle requerido do serviço *SvGpPollingDommainControl* na configuração do *polling* descrita na seção 7.2.

- Nenhuma forma de controle é requerida de outras entidades para a execução das ações de gerenciamento. As entidades executam suas ações de modo totalmente autônomo, e não é necessário que nenhuma entidade coordene a execução das ações nas diversas entidades.

A figura 9.3 esquematiza estes exemplos em relação ao aspecto complementar proposto.

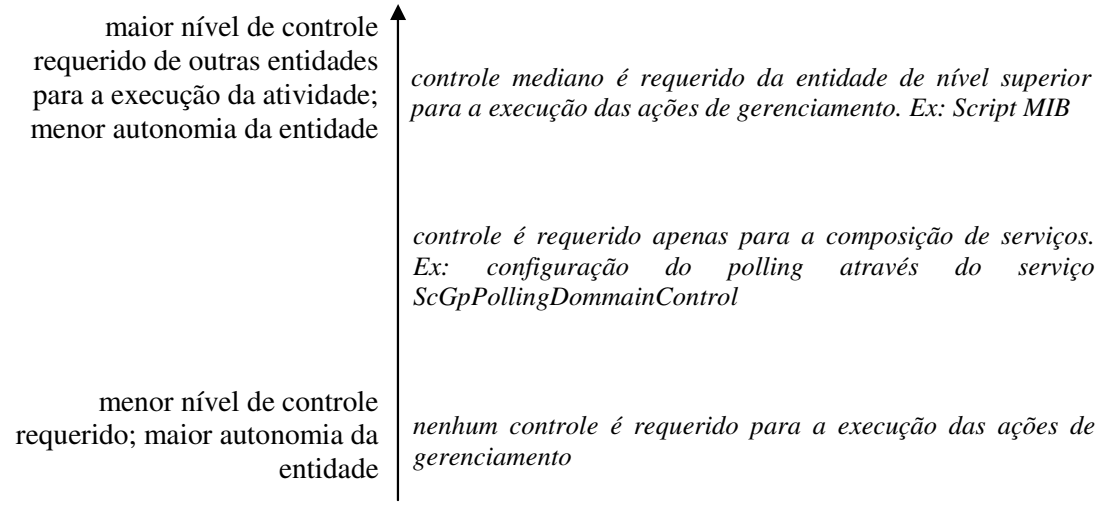


Figura 9.3: Exemplos do aspecto complementar relativo ao controle requerido de outras entidades

A análise deste aspecto nas atividades realizadas na solução de gerenciamento é importante para destacar de modo claro e explícito a diferença entre este aspecto e o critério principal 2 da taxonomia, distinguindo, respectivamente, o controle requerido para a execução das ações, de onde e como se dá a tomada de decisão para a execução destas. Este aspecto, contudo, é apenas complementar à taxonomia, não influindo na classificação dos paradigmas de gerenciamento.

9.3 Análise da Taxonomia Proposta

Dada a definição da taxonomia proposta, os exemplos de contextos modernos discutidos na seção 9.1 podem agora ser classificados segundo esta nova taxonomia. Iniciando a análise pelas **redes *mesh* sem fio**, identifica-se que as soluções de gerenciamento para estas redes devem seguir, de acordo com o critério 1 da taxonomia, abordagens fortemente distribuídas. Em relação ao critério 2, as soluções cujos nodos

pertencem a apenas um domínio administrativo ou a domínios administrativos que possuem hierarquia administrativa entre si (identificados na análise da seção 9.1.1 como *primeiro grupo*) podem ser baseadas em abordagens hierárquicas permanentes ou abordagens cooperativas, resultando, assim, no emprego do paradigma fortemente distribuído hierárquico permanente ou paradigma fortemente distribuído cooperativo. Podem, ainda, em redes com nodos em apenas um domínio administrativo, serem baseadas em abordagens hierárquicas variáveis, resultando, assim, no emprego do paradigma fortemente distribuído hierárquico variável. Por outro lado, as soluções para gerenciamento das redes cujos nodos pertencem a múltiplos domínios administrativos independentes, sem hierarquia administrativa entre eles (identificados na análise anterior como *segundo grupo*), devem ser baseadas necessariamente em abordagens cooperativas. Isto ocorre porque, como visto, as abordagens hierárquicas da taxonomia definem ou aceitam a existência de relações de autoridade e subordinação entre as entidades, não existentes em situações como estas, enquanto as abordagens cooperativas definem exatamente a autonomia das entidades, como é requerido nestas situações. Deste modo, o gerenciamento apropriado das redes pertencentes a este *segundo grupo* deve ser realizado através de soluções fortemente distribuídas cooperativas.

Analisando o segundo exemplo de contexto moderno, representado pelos **ataques de negação de serviço distribuídos**, com ênfase nos ataques que necessitam ser identificados e tratados em redes intermediárias, identifica-se que os mecanismos para detecção e reação aos ataques devem seguir abordagens fortemente distribuídas, conforme o critério 1 da taxonomia. Isto ocorre porque estas soluções devem ser executadas em múltiplos roteadores presentes em vários pontos da Internet para serem efetivas, resultando em um número elevado de entidades com processamento de gerenciamento. Devem, além disso, seguir abordagens cooperativas, conforme o critério 2 da taxonomia, já que os múltiplos roteadores representam equipamentos de múltiplos domínios administrativos e, nestas situações, abordagens hierárquicas não são permitidas. Assim, os mecanismos para detecção e reação aos ataques DDoS em redes intermediárias devem ser baseados no paradigma fortemente distribuído cooperativo. Este paradigma é também o seguido pelos dois mecanismos para detecção e reação aos ataques estudados em particular (IOANNIDIS; BELLOVIN, 2002) (ZHANG; PARASHAR, 2006).

Por fim, retomando o terceiro exemplo de contexto moderno, representado pelas **grades computacionais**, identifica-se que as soluções para gerenciamento da infra-estrutura de rede requerida pelas grades podem ser baseadas, de acordo com o critério 1, em abordagens fracamente distribuídas ou abordagens fortemente distribuídas, conforme os requisitos de gerenciamento da grade. Em contextos onde a grade não possuir escala ampla e não for exigido o gerenciamento das redes que provêem a interconexão entre os domínios administrativos, ambas as abordagens fracamente distribuídas e fortemente distribuídas são adequadas; por outro lado, quando a grade abranger em número elevado de domínios ou exigir o gerenciamento também das redes que provêem a interconexão entre seus múltiplos domínios, então abordagens fortemente distribuídas são tipicamente as mais adequadas. Em relação ao critério 2, excetuando-se aqueles contextos atípicos onde a grade estende-se por apenas um domínio administrativo ou por domínios administrativos com hierarquia entre si, as soluções de gerenciamento devem, necessariamente, serem baseadas em abordagens cooperativas. Assim, conforme as características do contexto, as soluções para gerenciamento da infra-estrutura de rede requeridas por grades tipicamente devem ser

baseadas no paradigma fracamente distribuído cooperativo ou no paradigma fortemente distribuído cooperativo.

Considerando as soluções de gerenciamento analisadas em particular, a solução proposta em (NEISSE, 2004), se considerada de modo completo, é baseada no paradigma fracamente distribuído cooperativo. Nesta solução, o sistema de grade é integrado ao sistema de gerenciamento, e as entidades do sistema de grade interagem com cada entidade do sistema de gerenciamento responsável pelo mecanismo de tradução de um domínio. As entidades de gerenciamento propriamente ditas não interagem umas com as outras: a interação é realizada através do sistema de grade. Assim, se analisadas isoladamente, as entidades do sistema de gerenciamento poderiam ser classificadas como baseadas no paradigma fracamente distribuído estaque. Contudo, a análise da solução completa resulta numa solução cooperativa, já que o sistema de grade é integrado ao sistema de gerenciamento e este provê a interação entre as entidades. Esta interação, contudo, respeita a autonomia das entidades de cada domínio, motivo pelo qual a solução é baseada em uma abordagem cooperativa, e não hierárquica. Em relação à solução proposta em (CAMINERO et al, 2007) e (TOMAS et al, 2009), esta é, também, uma solução fracamente distribuída, na qual a entidade de gerenciamento do domínio recebe solicitações da entidade responsável pelo escalonamento dos *jobs* daquele domínio. Embora detalhes sobre a abordagem não sejam fornecidos, considerando a solução de gerenciamento completa, integrada à grade computacional, é possível identificar-se que as interações ocorrem, também, através das entidades da grade computacional. Contudo, não é possível identificar-se se a solução atribui autonomia para as entidades de gerenciamento de cada domínio, resultando numa abordagem fracamente distribuída cooperativa, ou se estas entidades seguem de modo estrito o que foi determinado pela entidade da grade computacional, o que resultaria numa abordagem fracamente distribuída hierárquica permanente, embora tal abordagem não seja apropriada para situações típicas de gerenciamento de grades computacionais.

A tabela 9.5 sumariza a análise dos três exemplos de contextos modernos em relação à taxonomia proposta.

Tabela 9.5: Soluções para gerenciamento de contextos modernos em relação a taxonomia proposta neste documento

		Paradigmas em que as soluções de gerenciamento se enquadram
		Taxonomia Proposta
Redes *mesh* sem fio	**1º grupo – Nodos pertencentes a um único domínio administrativo ou a domínios que possuem hierarquia administrativa entre si**	Paradigma fortemente distribuído hierárquico permanente, paradigma fortemente distribuído hierárquico variável (nodos em um domínio administrativo) e paradigma fortemente distribuído cooperativo.
	2º grupo – Nodos pertencentes a diferentes domínios administrativos independentes	Paradigma fortemente distribuído cooperativo, já que este paradigma é o que define autonomia nas interações entre as entidades.
Ataques DDoS	**Mecanismos que necessitam ser executados em redes intermediárias (mecanismos em geral).**	Paradigma fortemente distribuído cooperativo, já que este paradigma é o que define autonomia nas interações entre as entidades.
	Mecanismo proposto por Ioannidis e Bellovin. Mecanismo proposto por Zhang e Parashar.	Baseados no paradigma fortemente distribuído cooperativo.
Grades comp.	**Soluções para gerenciamento de infra-estruturas de rede para grades computacionais (soluções em geral).**	Para os cenários onde não é necessário o gerenciamento das redes que provêem a interconexão entre os domínios administrativos pertencentes à grade, são adequadas soluções baseadas no paradigma fracamente distribuído cooperativo e no paradigma fortemente distribuído cooperativo. Para os cenários onde é necessário este gerenciamento, são requeridas soluções baseadas no paradigma fortemente distribuído cooperativo.
	Solução proposta por Neisse.	Baseada no paradigma fracamente distribuído cooperativo.
	Solução proposta por Caminero e outros e por Tomas e outros.	Baseada no paradigma fracamente distribuído hierárquico permanente ou no paradigma fracamente distribuído cooperativo (não é possível determinar).

A análise acima apresentada permite observar que a classificação dos contextos modernos pode ser feita de forma clara na taxonomia proposta, identificando os novos requisitos das soluções de gerenciamento originados por novas características destes contextos. Permite ainda, combinada com a análise da seção 9.1, observar que a taxonomia proposta considera aspectos das soluções de gerenciamento de contextos modernos não abordados nas principais taxonomias propostas na literatura e que representam limitações destas para classificar de modo apropriado tais soluções, como discutido a seguir.

Comparando com a taxonomia proposta por Martin-Flatin, Znaty e Hubaux, a taxonomia proposta permite classificar todas as soluções de gerenciamento discutidas. Além disto, tem como vantagem destacar de modo explícito como se dá a tomada de decisão para a realização das ações de gerenciamento e as relações de autoridade e subordinação, ou de autonomia, existentes entre as entidades. A taxonomia proposta tem ainda como pontos positivos a definição de critérios distintos para identificar o grau de distribuição das ações e a tomada de decisão, permitindo destacar estes dois aspectos claramente em cada um dos paradigmas propostos.

Comparando com a taxonomia proposta por Schönwälder, Quittek e Kappler, a taxonomia proposta tem como vantagem identificar e destacar como se dá a tomada de decisão para a realização das ações. Este aspecto não foi enfocado na referida taxonomia da literatura e a torna excessivamente ampla ao destacar as características de soluções de gerenciamento para contextos modernos, sem levar em consideração os importantes requisitos das soluções que envolvem mais de um domínio administrativo para a operação de seus serviços.

Por fim, em relação às duas referidas taxonomias, a taxonomia proposta neste documento tem ainda como ponto relevante a definição dos paradigmas estanques. Embora tais paradigmas não sejam identificados ao avaliar um sistema de gerenciamento isolado, estes paradigmas (especialmente o paradigma fracamente distribuído estanque) podem ocorrer ao analisar o gerenciamento de serviços de rede que envolvam mais de um domínio administrativo, tais como o gerenciamento de infra-estruturas de rede para grades computacionais por cada equipe de administradores ou a configuração de uma reserva de banda para transmissões de videoconferência pré-agendadas realizada manualmente em cada domínio. A ocorrência de soluções de gerenciamento estanques tende a diminuir na medida em que soluções que permitam a cooperação entre múltiplos domínios administrativos sejam desenvolvidas, representando um cenário intermediário no qual é exigido o gerenciamento de múltiplos domínios administrativos para a execução do serviço, porém tal gerenciamento ainda não é realizado de modo integrado. Assim, a diferenciação entre o gerenciamento de um serviço que envolve múltiplos domínios administrativos através dos paradigmas estanques ou dos paradigmas cooperativos é um benefício relevante proporcionado pela taxonomia proposta, inclusive por destacar uma solução de gerenciamento que pode ser aperfeiçoada.

9.4 Classificação das Soluções Baseadas no Modelo de Gerenciamento P2P em Relação à Taxonomia Proposta

A taxonomia aqui proposta pode também ser empregada para a classificação das soluções que seguem o modelo de gerenciamento distribuído baseado em P2P. As soluções que seguem o referido modelo são, tipicamente, abordagens fortemente distribuídas cooperativas ou abordagens fortemente distribuídas hierárquicas variáveis, de acordo com os mecanismos empregados em sua arquitetura para proporcionar, ou não, autonomia para a tomada de decisão nas entidades. Um exemplo de mecanismo que pode ser empregado para uma solução fortemente distribuída cooperativa baseada no referido modelo é o uso de políticas, verificadas pelo grupo de entidades que recebe a solicitação por um serviço. No estudo de caso de *polling* distribuído apresentado no capítulo 7, por exemplo, este mecanismo pode ser operacionalizado pelo *grupo de entidades para controle dos recursos gerenciados* (CRG) na atividade de *configuração*

do polling. Tal mecanismo pode ser utilizado pelo *grupo CRG* ao receber cada solicitação para configuração do serviço, de modo que cada requisição de *polling* recebida pelo *grupo CRG* seja avaliada por ele antes de ser configurada e este possua autonomia para aceitar ou não a configuração solicitada para seu grupo.

Por outro lado, a arquitetura do *polling* proposto básica, sem ativação de mecanismos para prover autonomia para as entidades optarem ou não pela execução do serviço, se caracteriza como fortemente distribuída hierárquica variável. Nestas soluções, a entidade que solicita a configuração do *polling* é atendida pelas demais entidades sem que estas ativem mecanismos para verificar se desejam ou não executar a ação: é empregada, assim, uma relação hierárquica para aquela atividade, na qual a entidade requisitante assume o papel de entidade de nível superior na hierarquia. Contudo, em outras instâncias da atividade de *configuração do polling* e em outras atividades executadas no ambiente de gerenciamento, outras entidades da solução podem disparar a atividade, passando assim a assumirem o papel de entidades de nível superior para a dada atividade. Esta abordagem, entretanto, não é a indicada para o gerenciamento de redes que possuam múltiplos domínios administrativos, já que, embora ela não defina uma relação hierárquica entre as entidades da solução completa, ela exige que haja uma total aceitação às ações requisitadas por outras entidades da solução.

Por fim, além das soluções acima descritas, soluções fracamente distribuídas que seguem o modelo podem também ser desenvolvidas, porém estas não caracterizam o uso típico do modelo. Nestes casos, as soluções podem também ser abordagens hierárquicas variáveis ou abordagens cooperativas.

9.5 Considerações Finais

Este capítulo propôs uma nova taxonomia para paradigmas de gerenciamento de redes. Inicialmente, discutiu as limitações das principais taxonomias apresentadas na literatura para classificar as soluções de gerenciamento para contextos modernos, incluindo ainda a classificação nestas das soluções baseadas no modelo de gerenciamento P2P. Em seguida, apresentou a taxonomia proposta e analisou esta taxonomia frente às soluções de gerenciamento para contextos modernos e em relação às taxonomias da literatura. Por fim, discutiu a classificação das soluções baseadas no modelo de gerenciamento P2P em relação à taxonomia proposta.

Como visto, a taxonomia proposta permite classificar as soluções de gerenciamento para contextos modernos de modo apropriado, identificando e destacando requisitos das soluções de gerenciamento atuais que envolvem mais de um domínio administrativo para a operação de seus serviços. Esta representa uma das principais características desta taxonomia, que destaca de modo explícito como se dá a tomada de decisão nas interações entre as entidades da solução de gerenciamento para a execução das ações distribuídas. Deste modo, a taxonomia possibilita enfatizar os aspectos de controle presentes na solução de gerenciamento, e as relações de autoridade e subordinação, ou de autonomia, entre as entidades. Por fim, a taxonomia permite ainda, entre as soluções para gerenciamento das redes atuais, classificar aquelas baseadas no modelo de gerenciamento P2P proposto neste documento, também possibilitando enfatizar tais características e aspectos para estas soluções em particular.

10 CONCLUSÕES

O gerenciamento de diversas redes atuais apresenta limitações quando realizado a partir de modelos tradicionais, baseados nos paradigmas centralizado e fracamente distribuído. Tais limitações deram origem à necessidade do emprego de modelos de gerenciamento inovadores, com características fortemente distribuídas.

A presente Tese versou sobre estes tópicos, discutindo as limitações dos modelos tradicionais para o gerenciamento das redes atuais e investigando um modelo fortemente distribuído baseado na tecnologia P2P para o gerenciamento destas redes, assim como analisando a classificação das soluções baseadas neste modelo segundo os paradigmas de gerenciamento. Tais tópicos foram investigados na Tese a partir de três objetivos principais, que serão discutidos a seguir.

A evolução das redes e dos serviços providos por estas deram origem a diferentes contextos de redes nos dias atuais. Entre estes, podem ser identificadas redes, serviços e aplicações de rede que possuem características distintas daquelas encontradas em contextos de redes tradicionais e que apresentam certas peculiaridades, tais como a comunicação baseada na cooperação entre múltiplos nodos; a necessidade de cooperação entre nodos ou serviços da rede para a execução de determinados serviços ou atendimentos a alguns requisitos, incluindo nodos em diferentes domínios administrativos; a topologia ou os parâmetros de desempenho apresentando grande dinamicidade, etc. Em virtude destes diferenciais, tais contextos de rede não são gerenciados de modo apropriado pelos modelos de gerenciamento tradicionais. Sobre este tópico versou o **primeiro objetivo principal** desta Tese, que resultou em sua **primeira contribuição principal: a análise dos fatores que tornam os modelos de gerenciamento baseados nos paradigmas tradicionais não apropriados para o gerenciamento de contextos modernos de rede**.

A busca por este objetivo implicou, inicialmente, na discussão sobre a ocorrência de tais contextos nas redes atuais, que foram denominados *contextos modernos de rede do ponto de vista de gerenciamento* (capítulo 4). Três contextos modernos foram então selecionados para serem tratados como estudos de caso: redes *mesh* sem fio, ataques de negação de serviço distribuídos (ataques DDoS) e grades computacionais. A busca pela identificação das características dos modelos de gerenciamento apropriados para estes contextos resultou em uma das contribuições secundárias desta Tese: a definição de uma metodologia para análise de contextos modernos. Esta metodologia foi então utilizada para exame dos três estudos de caso de contextos modernos, resultando na identificação das características e dos requisitos para o gerenciamento destes, assim como dos fatores que tornam os modelos baseados nos paradigmas tradicionais não apropriados para o gerenciamento destes contextos, que também representam contribuições secundárias deste trabalho.

O estudo realizado permitiu identificar diversos requisitos de gerenciamento de contextos modernos distintos daqueles encontrados em redes tradicionais. Tais requisitos incluem, entre outros: necessidade de monitorar e configurar equipamentos em diversos domínios administrativos para a operação adequada do serviço ou da própria rede; necessidade de interação entre as entidades responsáveis pelo gerenciamento de diferentes equipamentos para o gerenciamento adequado da rede, incluindo equipamentos em diferentes domínios administrativos; necessidade de suportar alterações freqüentes de topologia; necessidade de lidar com degradação de recursos ou particionamentos freqüentes na rede; necessidade de obter informações e atuar simultaneamente e coletivamente, ao longo de diversas porções da rede, para prover seu efetivo gerenciamento; etc.

A análise destes requisitos permitiu concluir que um dos importantes fatores que tornam os modelos baseados nos paradigmas tradicionais não apropriados para o atendimento destes requisitos diz respeito à necessidade do emprego de grande distribuição nas ações de gerenciamento em alguns contextos. Outro importante fator identificado em alguns destes requisitos foi a necessidade das soluções de gerenciamento suportarem lidar e interagir com múltiplos domínios administrativos, controlados por diferentes equipes de administradores e sem hierarquia administrativa entre si. Tais fatores ocorrem, em algumas situações de rede modernas analisadas, em simultâneo. Em outras situações, apenas um dos fatores foi identificado. Ambos os fatores não são relacionados aos modelos baseados nos paradigmas tradicionais, demandando, ou modelos fortemente distribuídos, ou modelos sem relações de hierarquia entre as entidades, ou ambos.

As limitações referidas acima para o gerenciamento dos contextos de rede modernos a partir dos modelos tradicionais somam-se às limitações ao emprego destes modelos, também discutidas neste documento, para o gerenciamento de redes com características tradicionais. Tais aspectos demonstram a importância da utilização de modelos baseados em paradigmas fortemente distribuídos e que suportem a interação entre múltiplos domínios administrativos em diversas redes atuais. Contudo, embora modelos de gerenciamento fortemente distribuídos baseados em algumas tecnologias tenham sido propostos e discutidos há diversos anos, raramente sistemas baseados nestes modelos foram aplicados para o gerenciamento em redes reais e poucos exemplos concretos da utilização destes são encontrados em ambientes de produção. Percebe-se, assim, a necessidade de investigar modelos alternativos fortemente distribuídos para lidar com tais limitações e requisitos de gerenciamento das redes atuais.

O **segundo objetivo principal** desta Tese versou sobre esta necessidade, resultando em **sua segunda e terceira contribuições principais: a definição e a investigação de um modelo distribuído baseado na tecnologia P2P para o gerenciamento das redes atuais e de uma arquitetura para um ambiente de gerenciamento fortemente distribuído baseada neste modelo**. A tecnologia P2P tem sido largamente utilizada em redes reais, de produção, para diversas áreas de aplicação, e possui características que a tornam uma alternativa promissora para ser investigada como suporte para a realização das atividades de gerenciamento, como discutido ao longo deste documento.

A fim de atingir este objetivo, um modelo de gerenciamento distribuído baseado em P2P foi proposto. Este modelo visualiza a rede P2P como uma infra-estrutura que provê suporte para que as operações de gerenciamento sejam desempenhadas com forte distribuição e sem papéis hierárquicos permanentes. Para a proposição do modelo, denominado modelo de gerenciamento de redes distribuído baseado em P2P, foram

introduzidos inicialmente seus quatro tipos de entidades de gerenciamento, assim como alguns conceitos e características deste, nas quais se incluem a visão estendida do recurso gerenciado (através da visão unificada do software de gerenciamento do recurso real com a entidade para controle dos recursos gerenciados do modelo); e o conceito de *grupos de peers* como uma entidade virtual unificada formada por um conjunto dinâmico de *peers* que possuem similaridades sob um ou mais aspectos e um conjunto de políticas ou capacidades em comum (capítulo 5).

O modelo proposto representa uma visão conceitual das principais entidades presentes no gerenciamento de redes baseado em P2P e como estas entidades estão organizadas, conforme definido na terminologia deste documento (seção 3.1). Este modelo é materializado no gerenciamento de redes real através de uma arquitetura para um ambiente de gerenciamento. Buscou-se, assim, a definição desta arquitetura para o modelo proposto, enfocando nesta o modo como as funcionalidades de gerenciamento são estruturadas no ambiente distribuído baseado em P2P e como é realizada a execução de suas atividades, considerando a infra-estrutura P2P sobre a qual o ambiente está estruturado e a utilização de forte distribuição na execução das atividades.

Para a proposição da arquitetura, foram discutidas as características da infra-estrutura P2P sobre a qual a arquitetura é concebida, a estrutura do ambiente de gerenciamento, sua organização em categorias, e os principais serviços estruturais requeridos no ambiente. A arquitetura proposta é composta por serviços e aplicações, suportando composições destes. Permite, através de sua estrutura, fazer uso das facilidades e dos serviços providos pela infra-estrutura P2P, tais como os serviços de indexação e busca de nodos e recursos, as facilidades para compartilhamento de recursos, as facilidades para comunicação e colaboração, etc. Possibilita, ainda, fazer uso dos mecanismos proporcionados pelo emprego dessa infra-estrutura P2P, incluindo o suporte a serviços como mecanismo para compartilhar a lógica e os recursos computacionais entre os diversos *peers*, o aprimoramento da conectividade entre os nodos de gerenciamento, a integração de serviços estruturais baseados em P2P para suporte a mecanismos tais como envio de notificações *publish-subscribe* e armazenamento distribuído, etc.

Buscando-se investigar como as funcionalidades de gerenciamento podem ser realizadas no ambiente proposto, foi realizado um estudo das funcionalidades das diversas áreas FCAPS pertinentes a um ambiente de gerenciamento como o proposto. Tal estudo incluiu o levantamento de funcionalidades já presentes nos ambientes de gerenciamento tradicionais, que podem agora ser remodeladas para fazer uso das facilidades providas pelo ambiente proposto, assim como a identificação de funcionalidades cuja disponibilidade surgiu a partir das potencialidades do ambiente. As funcionalidades analisadas representam exemplos de como a arquitetura proposta pode ser explorada para aprimorar as funcionalidades de gerenciamento, através do uso das facilidades proporcionadas pelo emprego de uma infra-estrutura P2P e do suporte à alta distribuição das ações de gerenciamento, resultando numa das contribuições secundárias deste trabalho.

Com o intuito de melhor compreender os serviços estruturais do ambiente, foi estudado e analisado o serviço estrutural de envio de notificações como exemplo (capítulo 6). O estudo realizado investigou as potencialidades do serviço no ambiente de gerenciamento proposto, discutindo os importantes benefícios da integração no ambiente de um serviço de envio de notificações *publish-subscribe* baseado em P2P com características e requisitos de QoS sofisticados. Deste estudo resultou a análise das

principais características de um serviço de envio de notificações no ambiente baseado em P2P, o que representou uma das contribuições secundárias da presente Tese.

Com base no estudo realizado, pode ser observado que, uma vez que um serviço de envio de notificações baseado em P2P não representa um serviço específico de um ambiente de gerenciamento de redes, este pode ser provido, em parte ou em sua totalidade, pela própria infra-estrutura P2P utilizada pelo ambiente, atentando-se apenas para que os requisitos deste serviço relevantes para o gerenciamento de redes discutidos neste documento sejam respeitados. Se não for disponibilizado pela infra-estrutura P2P, o serviço deve então ser desenvolvido de forma integrada a esta infra-estrutura. Neste caso, uma abordagem *publish-subscribe* baseada em P2P já proposta pode ser utilizada (tais como as apresentadas na seção 6.4). Entretanto, observou-se que é importante considerar esta integração atentando-se para as características da abordagem *publish-subscribe* utilizada e as características da infra-estrutura P2P empregada no ambiente, nas quais alterações podem ser necessárias com vistas a possibilitar tal integração, inclusive para atendimento aos requisitos de QoS demandados no ambiente de gerenciamento de redes.

Observou-se, ainda, que a integração no ambiente de gerenciamento de um serviço de envio de notificações que explore de modo amplo os requisitos proporcionados por uma abordagem *publish-subscribe* e as potencialidades e facilidades providas por sua integração a uma infra-estrutura P2P envolve um desenvolvimento de elevada complexidade. Assim, sugere-se que seja desenvolvido inicialmente um serviço com propriedades básicas, que seja depois complementado para atendimento a requisitos adicionais, conforme desejado. Segundo esta proposta, inicialmente podem ser suportadas as características e os requisitos de QoS mais relevantes e considerados essenciais para um ambiente de gerenciamento, tais como, por exemplo: o emprego de um esquema de subscrições que permita inclusão de novos eventos, que considere características importantes para gerenciamento (tais como tipo de recurso que originou a notificação, identificador deste recurso, tipo de informação enviada na notificação, conteúdo de tal informação, etc.), e que possibilite um pequeno número de falsos positivos; o uso de uma arquitetura não centralizada; o atendimento ao requisito de garantia de entrega de *no mínimo um* (de modo que cada assinante receba ao menos uma mensagem de uma dada notificação emitida); e o consumo de largura de banda aceitável para sua operação. Tal serviço pode ser aprimorado, numa etapa seguinte, com a inclusão de requisitos adicionais também de significativa relevância, tais como: o atendimento ao requisito de persistência de mensagens; e o atendimento ao requisito de ordenação das notificações. Em etapa posterior, novos requisitos podem ser atendidos com vistas a proporcionar o aprimoramento do serviço, tais como: o atendimento ao requisito de garantia de entrega de *exatamente um*; a possibilidade de subscrições delimitarem a largura de banda máxima que o serviço pode utilizar para entrega de notificações subscritas; e o emprego de mecanismos de correlação de eventos associados à composição de eventos. Por fim, se desejado, o serviço pode ainda ser aprimorado para incluir requisitos complementares, tais como: possibilidade das subscrições indicarem o nível de atendimento aos diversos requisitos de QoS desejado; o atendimento ao controle de período de validade de notificações; e o controle de entrega de forma esporádica. Contudo, é recomendado que os requisitos almejados sejam identificados no projeto inicial do serviço, com o intuito de compreendê-lo de modo amplo, já que observou-se que muitos requisitos são intensamente relacionados entre si e relacionados às características da infra-estrutura P2P empregada.

Por fim, a partir do estudo do serviço estrutural de envio de notificações desenvolvido como exemplo, foi observado que a definição e o desenvolvimento de serviços estruturais baseados em P2P completos envolvem grande complexidade. Por outro lado, benefícios da integração de serviços estruturais ao ambiente foram também observados, incluindo a possibilidade de explorar a infra-estrutura P2P para aprimoramento dos serviços, assim como a possibilidade de proporcionar facilidades sofisticadas nestes serviços e fazer uso destas pelas diversas funcionalidades de gerenciamento do ambiente, através do suporte provido pela arquitetura à composição de serviços, que podem invocar serviços estruturais.

Como estudo de caso do modelo e da arquitetura baseados em P2P, foi então realizada a definição e a análise de uma arquitetura para uma atividade de gerenciamento que faz uso do modelo e da arquitetura (capítulo 7), o que resultou em uma das contribuições secundárias da Tese. A atividade selecionada foi o *polling* distribuído, empregado para a monitoração do estado e para a coleta periódica de dados de desempenho dos recursos gerenciados.

O estudo de caso realizado demonstrou como pode ser realizada uma atividade de modo fortemente distribuído no ambiente, incluindo sua separação em duas etapas, uma responsável pela configuração das entidades de gerenciamento envolvidas, outra responsável pela execução das ações de gerenciamento propriamente ditas, já executadas de forma totalmente distribuída em cada *entidade CRG* responsável por um recurso gerenciado relacionado. O estudo desenvolvido demonstrou, ainda, como uma atividade de gerenciamento pode ser desenvolvida fazendo uso da composição de serviços provida pelo ambiente e como coordenar tais serviços para a realização da atividade completa. Adicionalmente, o estudo demonstrou como a atividade pode fazer uso de serviços estruturais do ambiente baseado em P2P, através de tal composição de serviços.

Por fim, o modelo e a arquitetura de gerenciamento baseado em P2P propostos foram analisados com vistas a avaliar suas características e funcionalidades, assim como analisar seu emprego para o gerenciamento das redes atuais (capítulo 8). Da análise realizada, pode-se concluir que a abordagem baseada em P2P compartilha com outras abordagens também fortemente distribuídas os benefícios resultantes do emprego de um paradigma fortemente distribuído, incluindo:

- Escalabilidade aprimorada, em virtude da redução da concentração do processamento e do tráfego de gerenciamento.
- Tolerância a falhas aprimorada, em virtude do emprego de grande número de entidades com inteligência de gerenciamento, da possibilidade de posicionar estas mais próximas aos recursos gerenciados, da redução do número de recursos pelo qual cada entidade é responsável, etc.

Concluiu-se, ainda, que o modelo e a arquitetura baseados em P2P proporcionam alguns benefícios adicionais quando comparados a outras abordagens fortemente distribuídas como a baseada na Script MIB, analisada na referida análise. Entre estes, incluem-se os itens a seguir:

- Um menor controle é requerido pelas entidades MLMs da entidade TLM, em virtude de todas as entidades do modelo serem concebidas para possuir independência e autonomia de outras entidades, possuindo cada entidade controle sobre como executar ou solicitar a execução de ações distribuídas.

- A maior autonomia proporcionada para as entidades do ambiente contribui para que mecanismos para controle e tomada de decisão sejam suportados por elas, requisito necessário quando a rede gerenciada incluir mais de um domínio administrativo não subordinado um ao outro.
- A comunicação e a interação entre as entidades é mais flexível, sendo realizada através de mensagens do ambiente e de invocações de operações de serviços. Pode, ainda, ser realizada através de facilidades adicionais proporcionadas pelo ambiente de gerenciamento, tais como os serviços básicos de comunicação disponibilizados pela infra-estrutura P2P (*e.g.*, a difusão de mensagens para grupos ou para todos os nodos da rede) e o serviço estrutural para envio de notificações *publish-subscribe* baseado em P2P.
- A escalabilidade é aperfeiçoada, em virtude de ser exigido menor nível de controle da entidade TLM e do suporte a serviços de grupo proporcionado pelo ambiente (que pode empregar mecanismos para distribuição de carga entre seus membros).
- A tolerância a falhas é aperfeiçoada, em virtude da maior autonomia e independência existente nas entidades, da abordagem ser concebida a partir de uma estrutura hierárquica dinâmica (sem fazer uso de uma estrutura hierárquica permanente e com papéis fixos para as entidades), e do suporte a serviços de grupos existente (que pode empregar mecanismos para que um *peer* do grupo assuma as funções de um *peer* em falha ou cuja conectividade aos recursos gerenciados está interrompida).
- A arquitetura baseada em serviços e composição destes contribui para oferecer maior facilidade para o projeto e a implementação de novas funcionalidades de gerenciamento, permitindo um desenvolvimento modular e a reutilização dos serviços de gerenciamento. A possibilidade de fazer uso de serviços providos pela infra-estrutura P2P e dos serviços estruturais do ambiente também contribui para esta maior facilidade.
- A infra-estrutura P2P e a arquitetura do ambiente proporcionam suporte para o desenvolvimento de serviços que aprimorem a implantação e a manutenção de suas funcionalidades de gerenciamento.

Por outro lado, concluiu-se que o modelo e a arquitetura baseados em P2P apresentam também algumas características que elevam sua dificuldade de utilização. Tais características são relacionadas a diferentes fatores, incluindo serem baseados em um paradigma fortemente distribuído, serem concebidos para gerenciar redes pertencentes a múltiplos domínios administrativos que não possuem hierarquia entre si, e necessitarem da utilização de uma infra-estrutura P2P. Acerca destes aspectos, as seguintes considerações podem ser apresentadas:

- O emprego de paradigmas fortemente distribuídos acarreta em aumento de complexidade na arquitetura do ambiente de gerenciamento, envolvendo o projeto, o desenvolvimento, a implantação, a operação e a manutenção deste. Acarreta, ainda, em aumento de complexidade na arquitetura das atividades de gerenciamento executadas sobre o ambiente, em virtude das funcionalidades de gerenciamento serem realizadas através de ações distribuídas em um número elevado de entidades, requerendo o projeto de

tais atividades de modo fortemente distribuído e o uso de mecanismos para interação entre as entidades, para a coordenação de tais ações, para acesso às informações de gerenciamento distribuídas, etc.

- A maior autonomia requerida das entidades da abordagem baseada em P2P e a flexibilidade proporcionada pela abordagem com a não exigência de papéis fixos (permanentes) serem assumidos pelas entidades acarretam em maior complexidade na abordagem, requerendo o projeto e o desenvolvimento de entidades e atividades que atendam a estes requisitos, o que não é identificado em arquiteturas tradicionais. Tais requisitos são demandados para que a abordagem possa ser empregada para o gerenciamento de múltiplos domínios administrativos sem hierarquia entre si, o que exige que as entidades suportem mecanismos para controle e tomada de decisão acerca de ações solicitadas por outras entidades e exige que as entidades dos diversos domínios possam solicitar ações.
- A aplicação da abordagem para o gerenciamento de múltiplos domínios administrativos sem hierarquia entre si eleva também a complexidade da abordagem em virtude da exigência de que mecanismos de controle e de segurança sejam oferecidos pelo ambiente para permitir que as atividades de gerenciamento sejam realizadas de modo apropriado entre os diversos domínios administrativos e com controles e níveis de acesso adequados.
- A existência de forte distribuição das ações e outras características da abordagem baseada em P2P elevam a complexidade de implantação do ambiente de gerenciamento pela exigência de que sejam configurados parâmetros na sua implantação, tais como a definição dos *grupos CRG* do ambiente, a definição dos recursos gerenciados por cada *grupo CRG*, etc.
- A necessidade de oferecer e manter uma infra-estrutura P2P que provenha serviços básicos e serviços estruturais traz maior complexidade ao projeto e ao desenvolvimento do ambiente de gerenciamento. Entretanto, uma vez que abordagens P2P têm sido utilizadas amplamente nas redes atuais em diferentes áreas de aplicação, discute-se que a experiência obtida com esta utilização pode ser empregada para o desenvolvimento da camada de infra-estrutura P2P requerida no ambiente.

Por fim, a partir destes conjuntos de considerações, concluiu-se que a abordagem baseada em P2P apresenta uma complexidade elevada *quanto ao ambiente de gerenciamento*, especialmente ao seu projeto e desenvolvimento, quando comparada a abordagens fracamente distribuídas ou a abordagens fortemente distribuídas como a baseada na Script MIB. Por outro lado, uma vez disponível o ambiente de gerenciamento, o *desenvolvimento de funcionalidades de gerenciamento no ambiente* apresenta maior flexibilidade e maior facilidade quando comparado a abordagens fortemente distribuídas como a baseada na Script MIB.

As considerações acima apresentadas permitiram concluir-se que o modelo e a arquitetura baseados em P2P apresentam diversos benefícios quando comparados a outras abordagens de gerenciamento, porém apresentam também maior complexidade, especialmente se comparados a abordagens fracamente distribuídas. Em virtude disto, o modelo e a arquitetura baseados em P2P devem ser empregados para o gerenciamento de uma rede analisando-se a necessidade destes e a adequação do emprego de uma

abordagem tradicional, tal como a seguida por plataformas de gerenciamento comerciais tradicionais.

Uma discussão da abordagem baseada em P2P quanto às diferentes situações de redes atuais foi então realizada. Desta discussão, concluiu-se que, quanto às redes atuais com características tradicionais, a abordagem baseada em P2P é indicada para o gerenciamento de redes tais como aquelas que possuem requisitos especiais de complexidade e relevância, apresentando, porém, limitações de largura de banda ou ausência de mecanismos de tolerância a falhas. Em tais redes, o gerenciamento a partir de abordagens fracamente distribuídas não é o mais indicado, em virtude de suas características. A abordagem baseada em P2P pode ser utilizada para o gerenciamento destas redes, propiciando ainda, além dos benefícios resultantes da forte distribuição, aprimoramentos em requisitos de gerenciamento exigidos em tais redes, tais como escalabilidade e tolerância a falhas. Por outro lado, a abordagem baseada em P2P não é recomendada para o gerenciamento de redes tradicionais que não possuem tais limitações, uma vez que estas podem ser gerenciadas de modo apropriado através de abordagens tradicionais: nestas situações, a abordagem baseada em P2P iria apresentar uma complexidade mais elevada, sem que os seus benefícios sejam requeridos para o gerenciamento da rede.

Em adição às redes tradicionais, as redes atuais incluem aquelas com características modernas, tais como os estudos de caso analisados no capítulo 4. Diversas destas redes, como discutido ao longo deste documento, possuem características peculiares, que demandam o emprego de modelos de gerenciamento fortemente distribuídos e não podem ser gerenciadas a partir de abordagens que empregam relações de autoridade e subordinação entre as entidades, sem propiciar às entidades autonomia para a tomada de decisão quando à execução ou não de uma ação requisitada. Tais requisitos não são suportados por abordagens de gerenciamento tradicionais. A abordagem baseada em P2P, por outro lado, suporta tais requisitos, sendo recomendada para o gerenciamento destes contextos.

Definido e analisado o modelo de gerenciamento baseado em P2P, buscou-se analisar-se, como **terceiro objetivo principal** desta Tese, como as soluções de gerenciamento para as redes atuais baseadas neste modelo podem ser classificadas segundo os paradigmas de gerenciamento existentes. A busca por este objetivo iniciou com a análise e conseqüente identificação de limitações das principais taxonomias propostas na literatura para a classificação das soluções de gerenciamento requeridas para contextos de redes modernos (capítulo 9), o que representou uma das contribuições secundárias desta Tese. Esta análise utilizou como exemplos as soluções requeridas para o gerenciamento dos contextos modernos analisados no capítulo 4 e as soluções em geral baseadas no modelo de gerenciamento proposto. Desta análise, concluiu-se que as particularidades dos modelos requeridos para o gerenciamento de diversos contextos de redes atuais não são, em muitos aspectos, identificadas e destacadas de modo apropriado nas taxonomias para paradigmas de gerenciamento de redes propostas na literatura.

Esta conclusão deu origem à **quarta contribuição principal** desta Tese, representada pela **definição de uma taxonomia para soluções de gerenciamento que visa destacar as características e os requisitos relevantes requeridos nos modelos de gerenciamento atuais**. Esta taxonomia foi baseada em dois critérios: o grau de distribuição das ações de gerenciamento e o modo como a tomada de decisão é realizada para a execução destas ações. Foi, ainda, aprimorada pela definição de um

aspecto complementar, que discute o nível de controle requerido de outras entidades para que as ações distribuídas referentes a uma atividade de gerenciamento completa sejam realizadas.

Uma vez definida a taxonomia, foi discutida a classificação das soluções de gerenciamento requeridas para os três estudos de caso de contextos modernos segundo esta taxonomia, o que resultou em uma das contribuições secundárias desta Tese. Tal discussão permitiu concluir-se que a taxonomia proposta permite classificar as soluções de gerenciamento para contextos modernos de forma clara, identificando os novos requisitos destas soluções originados pelas novas características destes contextos. Permitiu, ainda, concluir-se que a taxonomia proposta considera e destaca aspectos das soluções de gerenciamento não abordados nas principais taxonomias propostas na literatura e que representam limitações destas para a classificação dessas soluções. Por fim, foi ainda discutida a classificação das soluções baseadas no modelo de gerenciamento P2P segundo a taxonomia proposta. Esta classificação resultou em uma contribuição secundária da Tese.

Como **contribuição adicional**, os seguintes artigos foram publicados ou aceitos para publicação no contexto deste trabalho:

- MELCHIORS, C.; MATTJIE, D.; SANTOS, C.; PANISSON, A.; GRANVILLE, L. Z.; TAROUCO, L. M. R. Chapter 14: A P2P-Based Strongly Distributed Network Polling Solution. In: PATHAN, A. K; PATHAN, M,; LEE, H. Y. (Eds.) **Advancements in Distributed Computing and Internet Technologies: Trends and Issues**. Hershey: IGI Global Publishers, 2012. p. 289-313.

- MELCHIORS, C.; GRANVILLE, L. Z.; TAROUCO, L. M. R. Chapter XVI: P2P-Based Management of Collaboration Communications Infrastructures. In: NIIRANEN, S.; YLI-HIETANEN, J.; LUGMAYR, A. (Eds.) **Open Information Management: Applications of Interconnectivity and Collaboration.** Hershey: IGI Global Publishers, 2009. p. 343-373.

- MELCHIORS, C.; SANTOS, A. H.; MATTIJIE, D.; SANTOS, C. R. P.; PANISSON, A.; GRANVILLE, L. Z.; TAROUCO, L. M. R. A Network Polling Solution through a P2P-based Distributed Management Environment. In: ACM SYMPOSIUM ON APPLIED COMPUTING, ACM SAC, 25., Mar. 2010, Sierre. **Proceedings...** New York: ACM, 2010. p. 731-732.

- GRANVILLE, L. Z.; ROSA, D.; PANISSON, A.; MELCHIORS, C.; ALMEIDA, M. J. B.; TAROUCO, L. M. R. Managing Computer Networks Using Peer-to-Peer Technologies. **IEEE Communications Magazine**, New York, v. 43, n. 10, p. 62-68, Oct. 2005.

- PANISSON, A.; ROSA, D. M.; MELCHIORS, C.; GRANVILLE, L. Z.; ALMEIDA, M. J. B.; TAROUCO, L. M. R. Designing the Architecture of P2P-Based Network Management Systems. In: IEEE SYMPOSIUM ON COMPUTER AND COMMUNICATIONS, ISCC, 11., 2006, Caliari. **Proceedings...** Los Alamitos, CA: IEEE Computer Society, 2006. p. 69-75.

A pesquisa realizada ao longo da presente Tese possibilitou a identificação de várias oportunidades para **trabalhos futuros,** representando pesquisas adicionais que podem ser realizadas complementares ao estudo aqui desenvolvido. Em relação ao modelo baseado em P2P, identificou-se a oportunidade de investigação de arquiteturas de ambientes de gerenciamento baseadas no modelo proposto que abordem outras perspectivas que não a investigada na presente Tese, como discutido ao longo da seção 5.4. Deste modo, uma primeira faceta adicional para a definição de uma arquitetura de um ambiente de gerenciamento pode abordar os mecanismos de controle, de coordenação e de segurança requeridos para que as atividades sejam executadas no ambiente com os níveis de permissão e controle apropriados. A análise de uma arquitetura sob esta perspectiva deve considerar ambientes com múltiplos administradores de rede e operações que envolvam múltiplos domínios administrativos não subordinados uns aos outros.

Outra faceta que pode ser abordada diz respeito aos controles para segurança requeridos em um ambiente de gerenciamento baseado no modelo para que este se mantenha seguro a ataques externos. A arquitetura para um ambiente de gerenciamento sob esta perspectiva deve, por exemplo, suportar funcionalidades e mecanismos que permitam evitar a interrupção das atividades de gerenciamento por ataques externos, manter trilhas de auditoria de segurança que registrem as operação de gerenciamento realizadas, etc. Tal arquitetura deve considerar, inclusive, as características e as restrições de segurança relativas à infra-estrutura P2P.

Por fim, um terceiro enfoque adicional para uma arquitetura baseada no modelo compreende a investigação dos mecanismos para a implantação e a manutenção do ambiente de gerenciamento ao longo do tempo. Uma arquitetura que aborde esta perspectiva deve, por exemplo, propiciar mecanismos para a implantação inicial do ambiente de gerenciamento, a implantação de um novo domínio administrativo em um ambiente já configurado, a inclusão de novos recursos gerenciados no ambiente, a atualização do software do ambiente, etc. Tais mecanismos podem, como visto, fazer uso das potencialidades proporcionadas pela infra-estrutura P2P, beneficiando-se com os serviços disponibilizados por esta.

Em adição a estes estudos, outros podem ainda investigar os serviços estruturais da arquitetura do ambiente baseado em P2P proposta. Nesta perspectiva, uma oportunidade de pesquisa compreende a definição de uma arquitetura e o desenvolvimento de um serviço de envio de notificações *publish-subscribe* baseado em P2P integrado à arquitetura do ambiente proposta. Tal serviço pode fazer uso das conclusões obtidas ao longo do capítulo 6, que apresentou o estudo e a análise realizados para este serviço no ambiente. Por fim, outra oportunidade de pesquisa envolve a análise, a definição de uma arquitetura e o desenvolvimento de um serviço de armazenamento distribuído baseado em P2P integrado à arquitetura do ambiente.

REFERÊNCIAS

ABELÉM, A. J. et al. Redes *Mesh*: Mobilidade, Qualidade de Serviço e Comunicação em Grupo. In: RODRIGUEZ, N.; ABELEM, A. J. G., COSTA, J. C. W. A. (Org.). **Livro de Minicursos do SBRC2007**. 1a ed. Belém: Editora da UFPA, 2007, p. 51-107.

ABERER, K. et al. The essence of P2P: A reference architecture for overlay networks. IEEE INTERNATIONAL CONFERENCE ON PEER-TO-PEER COMPUTING, P2P'05, 5., 2005. **Proceedings...** IEEE Computer Society, 2005.

AHMED, L. et al. Resource and Service Discovery in Large-Scale Multi-Domain Networks. **IEEE Communication Surveys**, [S.l.], v. 9, n. 4, p. 2-30, 2007.

AKASHI, O.; SUGAWARA, T.; MURAKANI, K.; MARUYAMA, M.; TAKAHASHI, N. Multiagent-based Cooperative Inter-AS Diagnosis in ENCORE. n: IEEE/IFIP Network Operations and Management Symposium, 2000. **Proceedings...** IEEE, 2000. p. 521-534.

AKYILDIZ, I. F.; WANG, X.; WANG, W. Wireless mesh networks: a survey. **Computer Networks and ISDN Systems**, Amsterdan, v. 47, n. 4, p. 445-487, Mar. 2005.

ANDROUTSELLIS-THEOTOKIS, S.; SPINELLIS, D. A Survey of Peer-to-Peer Content Distribution Technologies. **ACM Computing Surveys**, New York, v. 36, n. 4, p. 335-371, Dec. 2004.

ARNEDO-MORENO, J.; HERRERA-JOANCOMARTI, J. A survey on security in JXTA applications. **Journal of Systems and Software**, New York, v. 82, n.9, p. 1513-1525, Sep. 2009.

BARTSCH-SPORL, B.; LENZ, M.; HUBNER, A. Case-Based Reasoning: Survey and Future Directions. In: GERMAN CONFERENCE ON KNOWLEDGE-BASED SYSTEMS, XPS-99, 5., 1999, LNAI 1570. **Proceedings...** Berlin: Springer, 1999, p. 67-89.

BEHNEL, S.; FIEGE, L.; MÜHL, G. On Quality-of-Service and Publish-Subscribe. In: IEEE INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS WORKSHOPS, ICDCS 2006, 26., 2006. **Proceedings...** Washington: IEEE Computer Society, 2006. p. 20-25.

BERKOVSKY, S.; KUFLIK, T.; RICCI, F. P2P Case Retrieval with an Unspecified Ontology. In: INTERNATIONAL CONFERENCE ON CASE-BASED REASONING: CASE-BASED REASONING RESEARCH AND DEVELOPMENT, ICCBR 2005, 6.,

2005, LNAI 3620. **Proceedings...** Berlin: Springer. p. 91-105.

BIESZCZAD, A.; PAGUREK, B.; WHITE, T. Mobile Agents for Network Management. **IEEE Communications Surveys and Tutorials**, [S.l], v.1, n.1, 1998.

BINZENHÖLFER et al. A P2P-Based Framework for Distributed Network Management. In: CESANA, M; FRATTA, L. (Eds.) **Wireless Systems and Network Architectures in Next Generation Internet:** Second International Workshop of the EURO-NGI Network of Excellence, LNCS 3833. New York: Springer, 2006, p. 198-210.

BINZENHÖLFER et al. **A P2P-Based Framework for Distributed Network Management.** 2005. 18 f. Technical Report No. 351. Research Report Series, Institute of Computer Science, University of Würzburg, Würzburg.

BROGI, A.; et al A Service-Oriented Model for Embedded Peer-to-Peer Systems. **Eletronic Notes in Theoretical Computer Science**, Amsterdam, v. 194, n. 4, p. 5-22, Apr. 2008.

BROOKS, R.R. Mobile Code Paradigms and Security Issues. **IEEE Internet Computing**, Piscataway, v.8, n. 3, p.54-59, May-Jun. 2004.

BRUNO, R.; CONTI, M.; GREGORI, E. Mesh Networks: Commodity Multihop Ad Hoc Networks. **IEEE Communications Magazine**, New York, v. 43, n. 3, p. 123-131, Mar. 2005.

CAMINERO, A. et al. An Autonomic Network-Aware Scheduling Architecture for Grid Computing. In: INTERNATIONAL WORKSHOP ON MIDDLEWARE FOR GRID COMPUTING, MGC, 5., 2008. **Proceedings...** ACM, 2007.

CARRANO, R.C.; MARTINS, R.R.; MAGALHÃES, C.S. The Ruca Project and Digital Inclusion. In: Latin American Network Operations and Management Symposium, LANOMS, 2007. **Proceedings...** IEEE, 2007, p. 38-49.

CASE, J. et al. **Introduction and Applicability Statements for Internet Standard Management Framework**: RFC 3410. [S.l.]: Internet Engineering Task Force, Network Working Group, 2002.

CASE, J. et al. **Introduction to Community-based SNMPv2**: RFC 1901. [S.l.]: Internet Engineering Task Force, Network Working Group, 1996.

CASE, J. et al. **Simple Network Management Protocol (SNMP)**: RFC 1157, STD 15. [S.l.]: Internet Engineering Task Force, Network Working Group, 1990.

CHAN, L. et al. CAESAR: Middleware for Complex Service-Oriented Peer-to-Peer Applications. In: WORKSHOP ON MIDDLEWARE FOR SERVICE ORIENTED COMPUTING, MW4SOC, 7., 2007, Newport. **Proceedings...** ACM, New York, 2007, p. 12-17.

CHEIKROUHOU, M.; CONTI, P.; LABETOULLE, J. Automatic Configuration of PVCs in ATM Networks with Software Agents. In: IEEE/IFIP Network Operations and Management Symposium, 2000. **Proceedings...** IEEE, 2000. p. 535-548.

CHIRITA, P. et al. Publish/Subscribe for RDF-based P2P Networks. In EUROPEAN SEMANTIC WEB CONFERENCE, ESWC, 1., 2004. **Proceedings...** 2004.

CHOI, Y.; PARK, D. Mirinae: A Peer-to-Peer Overlay Network for Large-Scale Content-Based Publish/Subscribe Systems. In: INTERNATIONAL WORKSHOP ON NETWORK AND OPERATING SYSTEMS SUPPORT FOR DIGITAL AUDIO AND VIDEO. **Proceedings...** New York: ACM, 2005, p. 105-110.

CLEMM, A. **Network Management Fundamentals**. Indianopolis: Cisco Press, 2007.

COMER, D. E. **Automated Network Management Systems: Current and Future Capabilities**. Pearson Prentice Hall, 2006.

COURTENAGE, S.; WILLIAMS, S. The Design and Implementation of a P2P-Based Composite Event Notification System. In: INTERNATIONAL CONFERENCE ON ADVANCED INFORMATION NETWORKING AND APPLICATIONS, AINA'06, 20., 2006. **Proceedings...** Washington: IEEE Computer Society, 2006, p. 701-706.

CURBERA, F. et al. Unraveling the Web services web: an introduction to SOAP, WSDL, and UDDI. **IEEE Internet Computing**, Piscataway, vol. 6, n. 2, p. 86-93, Mar./Apr. 2002.

DAM, M.; STADLER, R. A Generic Protocol for Network State Aggregation. In: Radiovetenskap och Kommunication, RVK, 2005, Linkoping, Sweeden. **Proceedings...** [S.l.:s.n], 2005.

DASWANI, N.; GARCIA-MOLINA, H.; YANG, B. Open Problems in Data-Sharing Peer-to-Peer Systems. In: INTERNATIONAL CONFERENCE ON DATABASE THEORY, ICDT 2003, 9., LNCS 2572. **Proceedings...**. Springer, 2003. p. 1-15.

DEBUSMANN, M.; KELLER, A. SLA-driven management of distributed systems using the common information model. In: IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT, IM, 8., 2003. **Proceedings...** 2003, p. 563-576.

DEBUSMANN, M.; SCHMID, M.; KROEGER, R. Generic Performance Instrumentation of EJB Applications for Service-Level Management. In: IEEE/IFIP NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, NOMS, 2002. **Proceedings...** 2002, p. 19-32.

DEPAOLI, F.; MARIANI, L. Dependability in Peer-to-Peer Systems. **IEEE Internet Computing**, Piscataway, v. 8, n. 4, p. 54-61, Jul. 2004.

DING, C. H.; NUTANONG, S.; BUYYA, R. Peer-to-Peer Networks for Content Sharing. In: SUBRAMANIAN, R; GOODMAN, B. **Peer-to-Peer Computing: The Evolution of a Disruptive Technology.** Hershey: Idea Group, 2005. p. 28-65.

DISTRIBUTED MANAGEMENT TASK FORCE. **CIM Operations over HTTP**: DSP0200. [S.l.], 2009. (2009-b).

DISTRIBUTED MANAGEMENT TASK FORCE**. Common Information Model (CIM) Infrastructure Specification:** DSP0004. [S.l.], 2009. (2009-a).

DISTRIBUTED MANAGEMENT TASK FORCE. **Representation of CIM in XML**: DSP0201. [S.l.], 2009. (2009-c).

DISTRIBUTED MANAGEMENT TASK FORCE. **Web-Based Enterprise Management (WBEM)**. Disponível em: <http://www.dmtf.org/standards/wbem/>. Acesso em janeiro de 2010. (2010-a).

DOUCEUR, J. The Sybil Attack. In: INTERNATIONAL WORKSHOP ON PEER-TO-PEER SYSTEMS, 1., LNCS 2429. **Proceedings...** Springer, p. 251-260, 2002.

DU, T. C.; LI, E. Y.; CHANG, A. Mobile Agents in Distributed Network Management. **Communications of the ACM**, New York, v. 46, n. 7, p. 127-132, Jul. 2003.

DUARTE, J. L. et al. Management Issues on Wireless Mesh Networks. In: Latin American Network Operations and Management Symposium, LANOMS, 2007. **Proceedings...** IEEE, 2007, p. 8-19.

EUGSTER, P. et al. The Many Faces of Publish/Subscribe. **ACM Computing Surveys**, New York, v. 35, n. 2, p. 114-131, Jun. 2003.

FESTOR, O. et al. Integration of WBEM-based Management Agents in the OS1 Framework. In: IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT, IM, 6., 1999. **Proceedings...** 1999, p. 49-64.

FIOREZE, T. et al. Comparing Web services with SNMP in a management by delegation environment. In: IFIP/IEEE International Symposium on Integrated Network Management, 9., IM 2005. **Proceedings...** [S.l.], 2005. p. 601-614.

FOSTER, I.; KESSELMAN, C. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. **International Journal of Supercomputer Applications**, [S.l], v.15, n. 3, 2001.

FRANKLIN, S.; GRAESSER, A. Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents. In: International Workshop on Agent Theories, Architectures, and Languages, 3., 1996. **Proceedings...** Springer-Verlag, 1996.

FUGGETTA, A.; PICCO, G. P.; VIGNA, G. Understanding Code Mobility. **IEEE TRANSACTIONS ON SOFTWARE ENGINEERING**, [S.l.], v. 24, n. 5, p. 342-361, May 1998.

GASPARY, L. P. et al. Flexible security in peer-to-peer applications: Enabling new opportunities beyond file sharing. **Computer Networks**, New York, v. 51, p. 4797-4815, Dec. 2007.

GLASS, S.; PORTMANN, M.; MUTHUKKUMARASAMY, V. Securing Wireless Mesh Networks. **IEEE Internet Computing**, Piscataway, v. 12, n. 4, p. 30-36, Jul.-Aug. 2008.

GOLDSZMIDT, G.; YEMINI, Y. Delegated Agents for Network Management. **IEEE Communications Magazine**, New York, v. 36, n. 3, p. 66-70, Mar. 1998.

GOLDSZMIDT, G.; YEMINI, Y. Distributed Management by Delegation. In: International Conference on Distributed Computing Systems, ICDCS, 15., 1995.

Proceedings... Vancouver: IEEE, 1995. p. 333-340.

GOLDSZMIDT, G.; YEMINI, Y.; YEMINI, S. Network Management by Delegation: the MAD Approach. In: CONFERENCE OF THE CENTRE FOR ADVANCED STUDIES ON COLLABORATIVE RESEARCH, Toronto, 1991. **Proceedings...** IBM Press: p. 347-361, 1991.

GONG, L. JXTA: A network programming environment. **IEEE Internet Computing**, Piscataway, v. 5, n. 3, p. 88-95, May 2001.

GRANVILLE, L. Z.; ROSA, D.; PANISSON, A.; MELCHIORS, C.; ALMEIDA, M. J. B.; TAROUCO, L. M. R. Managing Computer Networks Using Peer-to-Peer Technologies. **IEEE Communications Magazine**, New York, v. 43, n. 10, p. 62-68, Oct. 2005.

GTISC. **Emerging Cyber Threats Report for 2009**. GTISC (Georgia Tech Information Security Center), October 15, 2008.

GUIAGOUSSOU, M.H.; BOUTABA, R.; KADOCH, M. A Java API for advanced faults management. In: IEEE/IFIP INTERNATIONAL SYMPOSIUM ON INTEGRATED MANAGEMENT, 2001. **Proceedings...** Seattle: IEEE, 2001. p. 483-498.

GUPTA, A. et al. Meghdoot: Content-Based Publish/Subscribe over P2P Networks. In: ACM/IFIP/USENIX INTERNATIONAL CONFERENCE ON MIDDLEWARE, 5., 2004, LNCS 3231. **Proceedings...** New York: Springer, 2004, p. 254-273.

HALEPOVIC, E.; DETERS, R. The costs of using JXTA. In: INTERNATIONAL CONFERENCE ON P2P COMPUTING, 3., 2003. **Proceedings...** IEEE Computer Society, 2003, p. 160-167.

HANSAN, R. et al. A Survey of Peer-to-Peer Storage Techniques for Distributed File Systems. In: INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY, ITCC, 2005. **Proceedings...** IEEE Computer Society, 2005, p. 1-9.

HARRINGTON, D.; PRESUHN, R.; WIJNEN, B. **An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks**: RFC 3411, STD 62. [S.l.]: Internet Engineering Task Force, Network Working Group, 2002.

HEGERING, H.G.; ABECK, S.; NEUMAIR, B. **Integrated Management of Networked Systems: Concepts, Architectures, and Their Operational Application**. San Francisco: Morgan Kaufmann, 1999.

HIERTZ, G. et al. Principles of IEEE 802.11s. In: INTERNATIONAL CONFERENCE ON COMPUTER COMMUNICATIONS AND NETWORKS, ICCCN, 16., 2007, Honolulu. **Proceedings...** IEEE, 2007. p. 1002 – 1007.

HUANG, Y.; GARCIA-MOLINA, H. Publish/Subscribe in a Mobile Environment. **Wireless Networks**, Hingham, v. 10, p. 643-652, Nov. 2004.

IEEE. **Status of the Project IEEE 802.11s: Mesh Networking**. IEEE. Disponível em: < http://grouper.ieee.org/groups/802/11/Reports/tgs_update.htm >. Acesso em: fev. 2009.

IETF. **Distributed Management (disman)**. IETF. Disponível em: < http://www.ietf.org/wg/concluded/disman.html >. Acesso em março de 2010.

INTERNATIONAL TELECOMMUNICATION UNION. **ITU-T Recommendation X.753**: information technology – Open Systems Interconnection – Systems management: Command sequencer for system management. Genebra, 1997.

IOANNIDIS, J.; BELLOVIN, S. M. Implementing Pushback: Router-Based Defense Against DDoS Attacks. In: NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM, NDSS 02, 2002, San Diego. **Proceedings...** Internet Society, 2002. Disponível em: <http://www.isoc.org/isoc/conferences/ndss/02/proceedings.shtml>.

ISHMAEL, J. et al. Deploying Rural Community Wireless Mesh Networks. **IEEE Internet Computing**, Piscataway, v. 12, n. 4, p. 22-29, Jul.-Aug. 2008.

JARRETT, M.; WARD, P. Trusted Computing for Protecting Ad-hoc Routing. In: ANNUAL COMMUNICATION NETWORKS AND SERVICES RESEARCH CONFERENCE, CNSR, 4., 2006. **Proceedings...** IEEE Computer Society, 2006. p. 1-8.

KAMIENSKI et al. On the Use of Peer-to-Peer Architectures for the Management of Highly Dynamic Environments. In: INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING AND COMMUNICATIONS WORKSHOP, PERCOMW, 4., 2006. **Proceedings...** IEEE, 2006.

KARRER, R. P.; BOTTA, A.; PESCAPE, A. High-speed backhaul networks: Myth or reality? **Computer Communications**, Newton, v.31, p.1540–1550, May 2008.

KAWAMURA, R.; STADLER, R. Active Distributed Management for IP Networks. **IEEE Communications Magazine**, New York, v.38, n.4, p. 114-120, Apr. 2000.

KAZAA. **Homepage Kazaa**. 2010. Disponível em: <http://www.kazaa.com>/. Acesso em fev. 2010.

KOLODNER, J. **Case-Based Reasoning**. Morgan Kaufmann, 1993.

KOUBARAKIS, M. et al. Selective Information Dissemination in P2P Networks. **SIGMOD Record**, New York, v. 32, n. 3, p. 71-73, Sep. 2003.

KOVALENKO, V. N.; KORYAGIN, D. A. The Grid: Analysis of Basic Principles and Ways of Application. **Programming and Computer Software**, New York, v. 35, n. 1, p. 18-34, Jan. 2009.

KRAUTER, K.; BUYYA, R.; MAHESWARAN, M. A taxonomy and survey of grid resource management systems for distributed computing. **Software Practice and Experience**, New York, v. 32, p. 135-164, Fev. 2002.

KRSTI, I.; GARFINKEL, S. L. Bitfrost: the One Laptop per Child Security Model. In: SYMPOSIUM ON USABLE PRIVACY AND SECURITY, SOUPS, 3., 2007, Pittsburgh. **Proceedings...** New York: ACM, 2007. p. 132-142.

LEPPINEN, M.; PULKKINEN, P.; RAUTIAINEN, A. Java-and-CORBA-Based Network Management. **IEEE Computer**, Los Alamitos, v. 30, n. 6, p. 83-87, Jun. 1997.

LEVI, D.; SCHÖNWÄLDER, J. **Definitions of Managed Objects for the Delegation of Management Scripts**: RFC 3165. [S.l.]: Internet Engineering Task Force, Network Working Group, 2001.

LIOTTA, A.; PAVLOU, G.; KNIGHT, G. Exploiting Agent Mobility for Large-Scale Network Monitoring. **IEEE Network**, Piscataway, v. 16, n.3, p. 7-15, May/Jun. 2002.

LOCATELLI, F. et al. Spotting Intrusion Scenarios from Firewall Logs Through a Case-Based Reasoning Approach. In: IFIP/IEEE INTERNATIONAL WORKSHOP ON DISTRIBUTED SYSTEMS: OPERATIONS AND MANAGEMENT, DSOM 2004, 15., LNCS 3278. **Proceedings...** Berlin: Springer, p. 196-207.

LUA, E. et al. A Survey and Comparison of Peer-to-Peer Overlay Network Schemes. **IEEE Communications Surveys & Tutorials**, [S.l.], v. 7, n. 2, p. 72-93, 2005.

LUNDGREN, H. et al. Experiences from the Design, Deployment and Usage of the UCSB Testbed. **IEEE Wireless Communications**, Piscataway, vol. 13, n. 2, pp. 18–29, 2006.

MAHAMBRE, S. P.; KUMAR, S. D. M.; BELLUR, U. A Taxonomy of QoS-Aware, Adaptative Event-Dissemination Middleware. **IEEE Internet Computing**, v. 11, n. 4, p. 35-44, Jul.-Aug. 2007.

MANGANA, E. P. **A Distributed and Heuristic Policy-based Management Architecture for Large-Scale Grids**. 2008. 252f. Tese de Doutorado - Universitat Politècnica de Catalunya.

MARQUEZAN, C. et al. Distributed Autonomic Resource Management for Network Virtualization. In: NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, NOMS, 12., 2010. **Proceedings...** IEEE.

MARQUEZAN, C. et al. Maintenance of Monitoring Systems Throughout Self-Healing Mechanisms. In: International Workshop on Distributed Systems: Operations and Management, DSOM, 19., 2008. **Proceedings...** Springer, 2008, p. 176-188.

MARTINEZ, P. et al. Using the script MIB for policy-based configuration management. In: 2002 IEEE/IFIP Network Operations and Management Symposium, NOMS 2002. 2002. **Proceedings...** IEEE, p. 187-, 2002.

MARTIN-FLATIN, J. P; DOFFOEL, P. A; JECKLE, M. Web Services for Integrated Management: a Case Study. In: 2nd European Conference on Web Services, ECOWS 2004, Erfurt, Germany, September 2004. **Proceedings...** LNCS 3250, Springer, 2004. p. 239-253.

MARTIN-FLATIN, J. **Web-Based Management of IP Networks and Systems.** Chichester: John Wiley & Songs, 2003.

MARTIN-FLATIN, J.; ZNATY S.; HUBAUX, J. A Survey of Distributed Enterprise Network and Systems Management Paradigms. **Journal of Network and Systems Management**, New York, v. 7, n. 1, p. 9-26, 1999.

MAUTHE, A; HUTCHISON, D. Peer-to-Peer Computing: Systems, Concepts and Characteristics. **Praxis der Informationsverarbeitung und Kommunikation**, [S.l.], v.

26, n. 2, p. 60-64, Apr.-Jun. 2003.

MAZUMDAR, S. Inter-Domain Management between CORBA and SNMP: Web-based Management CORBA/SNMP Gateway Approach. In: IFIP/IEEE INTERNATIONAL WORKSHOP ON DISTRIBUTED SYSTEMS: OPERATIONS AND MANAGEMENT, DSOM, 7., 1996, Italy. **Proceedings...** 1996.

MCBURNEY, P.; PARSONS, S. **The Knowledge Engineering Review**, New York, v. 20, n. 3, 2005.

MCPHERSON, D.; DOBBINS, R.; HOLLYMAN, M.; LABOVITZ, C.; NAZARIO, J. **Wordwide Infrastrucutre Security Report, Volume V**: 2009 Report. Arbor Networks, January 19, 2010.

MELCHIORS, C. **Levantamento da Tecnologia Peer-to-Peer com Vistas ao Gerenciamento Cooperativo de Redes de Computadores**. 2005. 45p. Trabalho Individual (Mestrado em Ciência da Computação) – Instituto de Informática, UFRGS, Porto Alegre.

MELCHIORS, C. **Raciocínio Baseado em Casos Aplicado ao Gerenciamento de Falhas em Redes de Computadores**. 1999. 151f. Dissertação (Mestrado em Ciência da Computação) – Instituto de Informática, UFRGS, Porto Alegre.

MELCHIORS, C.; TAROUCO, L. M. R. Troubleshooting network faults using past experience. In: IEEE/IFIP NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, NOMS, 2000. **Proceedings...** IEEE, p. 549-562, 2000.

MESHKOVA, E et al. A survey on resource discovery mechanisms, peer-to-peer and service discovery frameworks. **Computer Networks**, New York, v. 52, p. 2097-2128, Aug. 2008.

MILOJICIC, D. S. et al. **Peer-to-Peer Computing** (Tech. Rep. HPL-2002-57). Palo Alto: HP Laboratories Palo Alto, 2003.

MIRKOVIC, J.; PRIER, G.; REIHER, P. Attacking DDoS at the Source. In: IEEE International Conference on Network Protocols, ICNP 02, 10., 2002, Paris. **Proceedings...** IEEE Computer Society, 2002. p. 312-321.

MIRKOVIC, J.; REIHER, P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. **ACM SIGCOMM Computer Communitions Review**, New York, v. 34, n. 2, p. 39-54, Apr. 2004.

MOUNTZIA, M.A.; RODOSEK, G. D. Using the Concept of Intelligent Agents in Fault Management of Distributed Services. **Journal of Network and Systems Management**, [S.l.], v. 7, n. 4, p. 425-446, Dec. 1999.

NEISSE, R. **Um Modelo Hierárquico Baseado em Políticas para o Gerenciamento Integrado de Redes de Computadores e Grids Computacionais**. 2004. 69f. Dissertação de Mestrado – PPGC/UFRGS, Porto Alegre.

OASIS. **OASIS Commitees by Categories: Web Services**. Disponível em: < http://www.oasis-open.org/committees/tc_cat.php?cat=ws >. Acesso em: jan. 2010.

OASIS. **UDDI Spec TC: UDDI Version 3.0.2**: UDDI Spec Technical Committee Draft, Dated 20041019. [S.l.], 2004.

OBJECT MANAGEMENT GROUP. **Common Object Request Broker Architecture**: Core Specification. Version 3.0.3. Needham, março de 2004.

OBJECT MANAGEMENT GROUP. **Homepage OMG**. 2009. Disponível em: <http://www.omg.org/>. Acesso em junho de 2009.

OBJECT MANAGEMENT GROUP. UML Profile and Metamodel for Services (SOA-Pro), Revised Submission, **OMG Document ad/2008-05-03**. Needham, 2008.

OLIVIERO, F.; PELUSO, L.; ROMANO, S. P. REFACING: An autonomic approach to network security based on multidimensional trustworthiness. **Computer Networks**, New York, v. 52, n. 14, p.2745-2763, Oct. 2008.

OLPC. Mesh Network Details OLPC. **OLPC**. Disponível em: < http://wiki.laptop.org/go/Mesh_Network_Details>. Acesso em: fev. 2009.

PALLER, G.; KOKKINEN, H. Modular, Service-Oriented API for Peer-to-Peer Middleware. In: INTERNATIONAL CONFERENCE ON MOBILE WIRELESS MIDDLEWARE, OPERATING SYSTEMS, AND APPLICATIONS, MOBILWARE, 1., 2008. **Proceedings...** ICST, Brussels, 2008.

PANISSON, A. **Distribuição de Carga em Sistemas de Gerenciamento de Redes Baseados em P2P**. 2007. 82f. Dissertação (Mestrado em Ciência da Computação) – Instituto de Informática, UFRGS, Porto Alegre.

PANISSON, A.; ROSA, D.; MELCHIORS; C.; GRANVILLE, L. Z.; ALMEIDA, M. J.; TAROUCO, L. M. R. Designing the Architecture of P2P-Based Network Management Systems. In: IEEE SYMPOSIUM ON COMPUTER AND COMMUNICATIONS, ISCC, 11., 2006, Caliari. **Proceedings...** Los Alamitos, CA: IEEE Computer Society, 2006. p. 69-75.

PAVLOU, G. On the Evolution of Management Approaches, Frameworks and Protocols: A Historical Perspective. **Journal of Network Systems Management**, New York, v. 15, p. 425-445, Dec. 2007.

PENG, T.; LECKIE, C.; RAMAMOHANARAO, K. Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems. **ACM Computing Surveys**, New York, v. 39, n. 1, article 3, Apr. 2007.

PERKINS, D. T. SNMP Versions. **The Simple Web**, v. 5, n. 1, 1997.

PETRIE, C. I. Agent-based engineering, the Web, and intlligent. **IEEE Expert**, Piscataway, v. 11, n. 6, p. 24-29, Dec. 1996.

PIETRO, A. G.; STADLER, R. A-GAP: An Adaptive Protocol for Continuous Network Monitoring with Accuracy Objectives. **IEEE Transactions on Network and Service Management**, [S.l.], v. 4, n. 1, p. 2-12, Jun. 2007.

PRESUHN, R. et al. **Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)**: RFC 3416, STD 062. [S.l.]: Internet Engineering

Task Force, Network Working Group, 2002.

QUITTEK, J.; BRUNNER, M. Applying and Evaluating Active Technologies in Distributed Management. **Journal of Network and Systems Management**, New York, v. 11, n. 2, p. 171-197, Jun. 2003.

RANJAN, R. **Coordinated Resource Provisioning in Federated Grids**. 2007. 234f. Tese de Doutorado - Department of Computer Science and Software Engineering, University of Melbourne, Melbourne.

RANJAN, R.; HARWOOD, A.; BUYYA, R. A case for cooperative and incentive-based federation of distributed clusters. **Future Generation Computer Systems**, Amsterdan, v. 24, p. 280-295, Apr. 2008. (2008-a)

RANJAN, R.; HARWOOD, A.; BUYYA, R. Peer-to-Peer Based Resource Discovery in Global Grids: A Tutorial. **IEEE Communications Surveys & Tutorials**, [S.l.], v. 10, n. 2, p. 6-33, 2nd Quarter 2008. (2008-b)

RATNASAMY, S. et al. A Scalable Content-Addressable Network. In: CONFERENCE ON APPLICATIONS, TECHNOLOGIES, ARCHITECTURES, AND PROTOCOLS FOR COMPUTER COMMUNICATIONS, ACM SIGCOMM, 2001. **Proceedings...** ACM, 2001, p. 161-172.

RIGGIO, R. et al. JANUS: A Framework for Distributed Management of Wireless Mesh Networks. In: INTERNATIONAL CONFERENCE ON TESTBEDS AND RESEARCH INFRASTRUCTURE FOR THE DEVELOPMENT OF NETWORKS AND COMMUNITIES, TridentCom, 3., 2007. **Proceedings...** IEEE, 2007. p. 1-7.

RISSON, J.; MOORS, T. Survey of research towards robust peer-to-peer networks: Search methods. **Computer Networks**, New York, v. 50, p. 3485-3521, Dec. 2006.

RNP. Um Computador por Aluno. **Rede Nacional de Pesquisa RNP**. Disponível em: <http://www.rnp.br/pd/ruca.html>. Acesso em: fev. 2009.

ROCHA, J et al. Peer-to-Peer: Computação Colaborativa na Internet. **Livro Texto Minicursos do XXII Simpósio Brasileiro de Redes de Computadores**, 2004. SBC, 2004. p. 3-36.

ROSA, D. M. **Suporte a cooperação em sistemas de gerenciamento de redes utilizando tecnologias peer-to-peer**. 2007. 73 f. Dissertação (Mestrado em Ciência da Computação) – Instituto de Informática, UFRGS, Porto Alegre.

ROUHANA, N.; HORLAIT, E. Active networks: architecture and service distribution. In: HORLAIT, E. (Ed.) **Mobile Agents for Telecommunication Applications**. Milford: Kogan Page, 2002. p. 77-93.

RUSSELL, S.; NORVIG, P. **Artificial Intelligence: A Modern Approach**. Prentice-Hall, 1995.

SAILHAN, F. et al. Wireless Mesh Network Monitoring: Design, Implementation and Experiments. In: IEEE GLOBECOM WORKSHOPS, 2007. **Proceedings...** Washington, DC: IEEE, 2007. p. 1-6.

SANTHANAM, L. et al. Distributed Self-policing Architecture for Fostering Node Cooperation in Wireless Mesh Networks. In: CUENCA, P.; OROZCO-BARBOSA, L. (Eds.) **Personal Wireless Communications**, LNCS 4127, Berlin: Springer, 2006. p. 147-158.

SANTOS, C. R. P**. Uso de Serviços de Presença em Sistemas P2P de Gerenciamento de Redes**. 2008.82f. Dissertação (Mestrado em Ciência da Computação) – Instituto de Informática, UFRGS, Porto Alegre.

SATOH, I. Building Reusable Mobile Agents for Network Management. **IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews**, [S.l.], v.33, n.3, p. 350-357, Aug. 2003.

SCHÖNWÄLDER, J. et al. SNMP Traffic Analysis: Approaches, Tools, and First Results. In: IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT, IM, 10., 2007**. Proceedings...** IEEE, 2007, p. 323-332.

SCHÖNWÄLDER, J.; PRAS, A.; MARTIN-FLATIN, J. P. On the Future of Internet Management Technologies. **IEEE Communications Magazine**, New York, p. 90-97, Oct. 2003.

SCHÖNWÄLDER, J.; QUITTEK, J.; KAPPLER, C. Building Distributed Management Applications with the IETF Script MIB. **IEEE Journal on Selected Areas in Communications**, Piscataway, v.18, n.5, p. 702-714, May 2000.

SINGH, A. et al. Defending against eclipse attacks on overlay networks. In: WORKSHOP ON ACM SIGOPS EUROPEAN WORKSHOP, 11., 2004. **Proceedings...** New York: ACM, p. 21-26, 2004.

SMITH, J.; NETTLES, S. Active Networking: One View of the Past, Present, and Future. **IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews**, [S.l.], v. 34, n. 1, p. 4-18, Fev. 2004.

STATE, R.; FESTOR, O. A management platform over a peer-to-peer service infrastructure. In: INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS, ICT, 10., 2003. **Proceedings...** IEEE, p. 124-131.

STEPHAN, R.; RAY, P.; PARAMESH, N. Network management platform based on mobile agents. **International Journal of Network Management**, New York, v.14, p. 59-73, Jan. 2004.

STOICA, I. et al. Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications. **IEEE/ACM Transactions on Networking**, Piscataway, v. 11, n. 1, p. 17-32, Feb. 2003.

STRAUSS, F.: SCHÖNWÄLDER, J.; QUITTEK, J. Open Source Components for Internet Management by Delegation. In: IEEE/IFIP International Symposium on Integrated Network Management, 2001. **Proceedings...** p. 185-198, 2001.

SUN MICROSYSTEMS. **Java Management Extensions (JMX) Instrumentation and Agent Specification JSR-00000**. Palo Alto, 2002.

SUN MICROSYSTEMS. **Homepage Java Management Extensions (JMX)**

Technology. 2009. Disponível em: < http://java.sun.com/javase/technologies/core/mntr-mgmt/javamanagement/index.jsp >. Acesso em junho de 2009. (2009-a)

SUN MICROSYSTEMS. **Java Management Extensions White Paper**. Palo Alto: SUN Microsystems, 1999.

TCPDUMP. **TCPDUMP/LIBCAP Public Repository**. Disponível em: < http://www.tcpdump.org >. Acesso em: set. 2009.

TENNENHOUSE, D. et al. A Survey of Active Network Research. **IEEE Communications Magazine**, New York, v. 35, n.1, p. 80-86, Jan. 1997.

TOMAS, L. et al. Improving GridWay with Network Information: Tuning the Monitoring Tool. In: IEEE INTERNATIONAL SYMPOSIUM ON PARALLEL & DISTRIBUTED PROCESSING, IPDPS, 2009. **Proceedings...** Washington, IEEE Computer Society, 2009, p. 1-8.

TRAVERSAT, B. et al. **Project JXTA 2.0 Super-Peer Virtual Network**. Sun Microsystems, 2003.

UDUPA, D. K. **Network Management Systems Essentials**. New York: Mc-Graw-Hill, 1996.

WALDBUSSER, S. et al. **Introduction to the Remote Monitoring (RMON) Family of MIB Modules**: RFC 3577. [S.l.]: Internet Engineering Task Force, Network Working Group, 2003.

WALDBUSSER, S. **Remote Network Monitoring Management Information Base Version 2 using SMIv2**: RFC 2021. [S.l.]: Internet Engineering Task Force, Network Working Group, 1997.

WALDBUSSER, S. **Remote Network Monitoring Management Information Base**: RFC 2819. [S.l.]: Internet Engineering Task Force, Network Working Group, 2000.

WILLIAMS, C. et al. Redundancy Management for P2P Storage. In: INTERNATIONAL SYMPOSIUM ON CLUSTER COMPUTING AND THE GRID, CCGRID, 7., 2007. **Proceedings...** IEEE Computer Society, 2007, p. 1-8.

WORLD WIDE WEB CONSORTIUM. **SOAP Version 1.2 Part 0: Primer:** Second Edition: W3C Recommendation, 27 April 2007. [S.l.], 2007. (2007-a)

WORLD WIDE WEB CONSORTIUM. **Web Services Activity**. 2010. Disponível em: < http://www.w3.org/2002/ws/ >. Acesso em: jan. 2010. (2010-a).

WORLD WIDE WEB CONSORTIUM. **Web Services Architecture:** W3C Working Group Note 11 February 2004. [S.l.], 2004.

WORLD WIDE WEB CONSORTIUM. **Web Services Description Language (WSDL) Version 2.0 Part 0**: Primer: W3C Recommendation, 26 June 2007. [S.l.], 2007. (2007-b).

YALAGANDULA, P. et al. S3: A Scalable Sensing Service for Monitoring Large Networked Systems. In: SIGCOMM workshop on Internet network management, 2006,

Pisa. **Proceedings...** New York: ACM, 2006. p. 71-76.

ZHANG, G.; PARASHAR, M. Cooperative Defense against DDoS Attacks. **Journal of Research and Practice in Information Technology**, [S.l.], v. 38, n. 1, p. 69-84, Feb. 2006.

ZHANG, Y.; HU, H.; CHEN, H. QoS Differentiation for IEEE 802.16 WiMAX Mesh Networking. **Mobile Networks and Applications**, New York, v. 13, n. 1-2, p. 19-37, Apr. 2008.

APÊNDICE A - TECNOLOGIAS PARA GERENCIAMENTO DE REDES

Diversas tecnologias têm sido propostas para utilização no gerenciamento de redes. Este apêndice apresenta uma introdução destas principais tecnologias e os paradigmas seguidos por elas, selecionadas por serem representativas ou utilizadas de modo freqüente em pesquisas ou indústria. Neste apêndice, são descritas as tecnologias utilizadas no ambiente TCP/IP; tecnologias empregadas em outros ambientes não são enfocadas. Informações adicionais sobre o tópico podem ser obtidas em documentos complementares, incluindo levantamentos das tecnologias para gerenciamento de redes em geral (MARTIN-FLATIN, 2003) (PAVLOU, 2007), levantamentos para tecnologias de gerenciamento distribuído (MELCHIORS, 2005) e levantamentos de tecnologias para delegação dinâmica (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000).

Diferentes abordagens têm sido utilizadas na literatura para agrupar as tecnologias de gerenciamento de redes. Neste documento, se optou por agrupar as tecnologias de acordo com o modo como as operações de gerenciamento são realizadas, seguindo o primeiro nível de categorias de uma taxonomia proposta em (PAVLOU, 2007). Seguindo este critério, as tecnologias utilizadas para gerenciamento de redes distribuído foram agrupadas em dois grandes grupos: tecnologias que provêem funcionalidades de gerenciamento através da invocação remota de operações e tecnologias que provêem funcionalidades de gerenciamento utilizando código móvel. Após tais grupos serem descritos, uma terceira seção é apresentada para descrever as abordagens baseadas no conceito de agentes inteligentes, não incluídos na taxonomia do referido autor. Por fim, ao final deste apêndice, as organizações utilizadas por outros autores serão apresentadas.

A.1 Tecnologias com Invocação Remota de Operações

Esta seção aborda as principais tecnologias e abordagens que provêem o gerenciamento de redes através da invocação remota de operações. Inclui, deste modo, tecnologias que invocam objetos gerenciados através das diferentes versões do protocolo *Simple Network Management Protocol* (SNMP), assim como tecnologias que seguem o paradigma de objetos distribuídos e são empregadas para gerenciamento de redes. A primeira seção apresenta a arquitetura de gerenciamento Internet, assim como as diferentes versões do protocolo SNMP, seguida pela seção que aborda a tecnologia *Remote Monitoring MIB* (RMON). As subseções a seguir abordam tecnologias que seguem o paradigma de objetos distribuídos, incluindo *Common Object Request Broker Architecture* (CORBA), *Java Management Extensions* (JMX), *Web-Based Enterprise*

Management (WBEM) e o modelo de informações utilizado nesta tecnologia denominado *Common Information Model* (CIM), e, por fim, Web Services.

A.1.1 Framework de Gerenciamento Internet

O *framework* de gerenciamento Internet (denominado *Internet Standard Management Framework*) (HARRINGTON; PRESUHN; WIJNEN, 2002)(CASE et al, 2002) está descrito em um conjunto de padrões do *Internet Engineering Task Force* (IETF) e foi concebido para o gerenciamento de equipamentos em redes TCP/IP. Com seus primeiros documentos concluídos por volta do ano 1990, este *framework* especifica o gerenciamento de redes baseado no protocolo *Simple Network Management Protocol* (SNMP), assim como o modelo de informação associado. Referido usualmente como *framework* de gerenciamento SNMP ou apenas SNMP, o *framework* teve ampla aceitação, com agentes suportados por em enorme número de equipamentos IP.

O modelo de informação do *framework* é baseado em variáveis usadas para modelar informações dos recursos gerenciados, conhecidas como *objetos SNMP*. Estes objetos são especificados através da linguagem *Structure of Management Information* (SMI) e recuperados por gerentes através da *Management Base Information* (MIB) do agente gerenciado.

Diversas versões do SNMP foram publicadas. A primeira delas é hoje conhecida como SNMPv1 (CASE et al, 1990) e é baseada em cinco operações: *get-request* e *get-next-request*, utilizadas pelos gerentes para recuperar informações da MIB; *set-request*, utilizada pelo gerente para escrever dados na MIB; *get-response*, utilizada pelos agentes para responder as operações anteriores; e *traps*, utilizadas pelos agentes para enviar mensagens. Com o passar dos anos, limitações foram sendo identificadas para esta versão, e novas versões foram lançada objetivando tratar estas questões, resultando em novas versões, incluindo o SNMPv2p, SNMPv2u, o SNMPv2*, o SNMPv2c e SNMPv3.

O SNMPv2p é hoje uma versão obsoleta. Esta versão foi baseada em uma nova versão do protocolo SNMP denominada SNMPv2 e em novas MIBs, incluindo a MIB Manager-to-Manager (M2M), que, juntamente com uma nova operação *Inform-Request*, objetivava permitir o gerenciamento distribuído através de uma hierarquia de gerentes (MARTIN-FLATIN, 2003). O SNMPv2u e SNMPv2* não foram utilizados comercialmente de modo significativo (PERKINS, 1997). O SNMPv2c é utilizado comercialmente, sendo útil para o gerenciamento de roteadores de *backbone*, em virtude do suporte à contadores de 64 bits e por oferecerem melhor manipulação de erros que o SNMPv1 (MARTIN-FLATIN, 2003). Esta versão é conhecida como Community-based SNMPv2 (CASE et al, 1996)(PRESUHN et al, 2002). O SNMPv3 (CASE et al, 2002), por fim, tem como foco a segurança.

A.1.2 Remote Monitoring MIB (RMON)

A tecnologia Remote Monitoring MIB (RMON) (WALDBUSSER et al, 2003) consiste em uma MIB SNMP especial que é executada em equipamentos de monitoração remota, denominados *probes RMON*, com o propósito de gerenciar a rede. Esta MIB permite que gerentes deleguem certas tarefas de gerenciamento para os *probes* através da configuração da MIB, incluindo tarefas para coleta de estatísticas e geração de alarmes quando limiares forem atingidos. As tarefas delegadas são estáticas.

A utilização de *probes RMON* alivia o processamento nos gerentes e reduz o volume de dados enviados pela rede.

A primeira versão do RMON data de 1991, com atualizações posteriores, sendo conhecida como RMON-1 (WALDBUSSER, 2000). A RMON-2 (WALDBUSSER, 1997), por sua vez, foi lançada em 1997 e estendeu a arquitetura inicial com a inclusão de análise do nível de aplicação. Além destas, existem atualmente um conjunto de outras MIBs relacionadas (WALDBUSSER et al, 2003) que expandem a funcionalidade previamente definida em suas MIBs iniciais.

A.1.3 Common Object Request Broker Architecture (CORBA)

A especificação ***Common Object Request Broker Architecture*** **(CORBA)** é uma especificação definida pelo *Object Management Group* (OMG) para a ***Object Management Architecture*** **(OMA)**, uma arquitetura designada para suportar a comunicação e cooperação entre objetos nos ambientes heterogêneos abertos. A especificação CORBA (OBJECT MANAGEMENT GROUP, 2004) contém os mecanismos fundamentais para a comunicação entre objetos, utilizando um ***object request broker*** **(ORB)**. O ORB é um intermediário entre o cliente e o servidor responsável por todos os mecanismos necessários para encontrar a implementação do objeto solicitado na requisição, preparar o objeto para receber a requisição e permitir a comunicação da requisição. O cliente acessa, deste modo, uma interface completamente independente da localização do objeto requisitado e da linguagem de programação utilizada para implementar o objeto.

A interface entre as chamadas dos clientes e a implementação dos objetos é definida através da linguagem denominada *Interface Definition Language* (IDL). Uma definição de interface escrita em IDL define completamente os parâmetros das operações dos objetos e fornece todas as informações necessárias para o desenvolvimento de clientes que utilizam as operações da interface. Informações sobre a especificação CORBA podem ser obtidas na especificação *Common Object Request Broker Architecture: Core Specification* (OBJECT MANAGEMENT GROUP, 2004) e nas demais especificações da OMA (OBJECT MANAGEMENT GROUP, 2009), assim como em (HEGERING; ABECK; NEUMAIR, 1999).

Entre as pesquisas desenvolvidas em gerenciamento de redes utilizando CORBA, podemos citar o trabalho proposto por Mazumdar (MAZUMDAR, 1996), que apresenta a implementação de um *gateway* utilizando CORBA e SNMP, assim como o trabalho apresentado por Leppinen, Pulkkinen e Rautiainen (LEPPINGEN; PULKKINEN; RAUTIANINEN, 1997), que propõe uma plataforma baseada em CORBA para a criação, o gerenciamento e a invocação de serviços de telecomunicações distribuídos que integra sistemas com CMIP e SNMP.

A.1.4 Java Management Extensions (JMX) e Outras Tecnologias de Gerenciamento Baseadas em Java

Em 1996, a Sun Microsystems disponibilizou o ***Java Management Application Programming Interface*** **(JMAPI)**, uma API composta por um conjunto de ferramentas e diretivas para a criação de *applets* Java para gerenciamento de redes (MARTIN-FLATIN, 2003). O JMAPI foi substituído em 1999 pelo *Java Management Extensions* (JMX). O JMX foi inicialmente denominado *Java Management API* (JMAPI) *2.0*, embora sem relação com os objetivos, API ou implementação do primeiro JMAPI.

Assim, a fim de eliminar a confusão entre o primeiro JMAPI e a nova especificação, o nome foi substituído por *Java Management Extensions*.

A tecnologia ***Java Management Extensions*** **(JMX)**, também chamada especificação JMX (SUN MICROSYSTEMS, 2002) (SUN MICROSYSTEMS, 1999), visa o gerenciamento de redes e aplicações na linguagem de programação Java. A especificação JMX define a arquitetura, padrões de projeto, API e serviços para este gerenciamento, fornecendo aos desenvolvedores Java meios para instrumentalizar o código Java, criar *smart Java agents*, implementar um *middleware* de gerenciamento distribuído, e integrar estas soluções em sistemas de gerenciamento e monitoração. Informações detalhadas sobre JMX podem ser obtidas na *Java Specification Request* (JSR) 000003 (SUN MICROSYSTEMS, 2002), assim como em (SUN MICROSYSTEMS, 2009-a).

Entre os estudos sobre a utilização de JMX no gerenciamento de redes e aplicações, podem ser citados: Guiagoussou, Boutaba e Kadoch (GUIAGOUSSOU; BOUTABA; KADOCH, 2001), que apresentam uma API que oferece extensões para o gerenciamento de falhas baseado em JMX; e Debusmann, Schmid e Kroeger (DEBUSMANN; SCHMID; KROEGER, 2002), que propõem uma abordagem para gerenciamento de servidores de aplicações EJB que utiliza um modelo de informação CIM para descrever o servidor EJB e a arquitetura JMX para a instrumentação do servidor e aplicações.

A.1.5 Web-Based Enterprise Management (WBEM)

O ***Web-Based Enterprise Management*** **(WBEM)** foi definido pelo *Distributed Management Task Force* (DMTF) com o objetivo de unificar o gerenciamento de ambientes de computação distribuída (DISTRIBUTED MANAGEMENT TASK FORCE, 2010-a). O WBEM utiliza o ***Common Information Model*** **(CIM)** como seu modelo de informação. O CIM, também definido pelo DMTF, é um modelo de informação orientado a objetos que fornece a definição de informações de gerenciamento para sistemas, redes, aplicações e serviços. O CIM é composto por duas partes: a especificação CIM e o esquema (*Schema*) CIM. A especificação CIM (DISTRIBUTED MANAGEMENT TASK FORCE, 2009-a) descreve a linguagem, nomes, *Meta Schema* e técnicas de mapeamento para outros modelos de informação, tal como MIBs SNMP. O *Meta Schema* é a definição formal do modelo, definindo os termos utilizados para expressar o modelo, seus usos e suas semânticas. O esquema CIM provê as descrições de modelos reais. A estrutura do esquema CIM é representada através da linguagem *Unified Modeling Language* (UML). A definição formal do esquema CIM é expressa em um *Managed Object File* (MOF), um arquivo ASCII ou UNICODE que pode ser utilizado como entrada em um editor, *parser* ou compilador MOF.

O WBEM utiliza o protocolo de comunicação HTTP para a transmissão das mensagens CIM (DISTRIBUTED MANAGEMENT TASK FORCE, 2009-b). Enquanto o MOF provê a representação textual da informação de gerenciamento modelada utilizando CIM, o mapeamento da representação MOF para o protocolo de comunicação HTTP é feito utilizando a *Extensible Markup Language* (XML). A informação CIM é modelada utilizando a CIM XML DTD, que define o *schema* XML para objetos e mensagens CIM (DISTRIBUTED MANAGEMENT TASK FORCE, 2009-c).

Entre as pesquisas sobre a utilização do CIM e do WBEM para o gerenciamento de redes e sistemas, podem ser citados: Debusmann e Keller (DEBUSMANN; KELLER, 2003), que apresentam uma abordagem pra utilização de CIM para o gerenciamento de SLAs de sistemas distribuídos, enfocando o problema de integrar SLAs definidas para o ambiente Web Services em um sistema de gerenciamento que faz uso do CIM; e Festor et al (FESTOR et al, 1999), que abordam a integração de agentes baseados em WBEM utilizando o CIM com plataformas e aplicações de gerenciamento baseadas em OSI.

A.1.6 Web Services

A tecnologia Web Services (WORLD WIDE WEB CONSORTIUM, 2004), padronizada pelo *World Wide Web Consortium* (W3C), utiliza alguns protocolos Web existentes e padrões XML, sendo designada para oferecer interoperabilidade máquina-à-máquina sobre a rede. Diversas especificações e tecnologias são utilizadas em Web Services (CURBERA et al, 2002), incluindo:

- ***Simple Object Access Protocol* (SOAP)** (WORLD WIDE WEB CONSORTIUM, 2007-a): protocolo para comunicação entre as aplicações clientes e os Web Services. A especificação SOAP provê a definição das informações baseadas em XML que podem ser utilizadas para troca de informações estruturadas entre os pontos da comunicação.

- ***Web Services Description Language* (WSDL)** (WORLD WIDE WEB CONSORTIUM, 2007-b): provê uma descrição formal da interface de Web Services em formato processável por máquina.

- ***Universal Description, Discovery, and Integration* (UDDI)** (OASIS, 2004): define um conjunto de serviços que suportam a descrição e descoberta de provedores Web Services, os Web Services disponibilizados por cada provedor e as interfaces técnicas que podem ser utilizadas para acessar estes serviços. O UDDI é baseado em um conjunto de padrões tais como HTTP, XML, XML Schema e SOAP.

Informações sobre a tecnologia Web Services podem ser obtidas nas especificações do W3C (WORLD WIDE WEB CONSORTIUM, 2010-a) e OASIS (OASIS, 2010).

Com relação ao modelo de gerenciamento Internet, três diferentes abordagens que podem ser adotadas para o gerenciamento com Web Services (SCHÖNWÄLDER; PRAS; MARTIN-FLATIN, 2003). Numa primeira abordagem com mapeamento direto, seguindo o paradigma gerente-agente, o agente executa um servidor HTTP e o gerente executa um cliente HTTP. O gerente efetua consultas no agente através de mensagens *Get* e *Set* via SOAP e o *polling* é realizado pela utilização de mensagens *Get* a partir do gerente. Uma segunda abordagem é a utilização do modelo *publish-subscribe*. Neste caso, o gerente comunica seu interesse em certas informações publicadas pelo agente em um registro WSDL, e o agente envia as informações para uma pilha de mensagens, que é utilizada pelo gerente para o recebimento das informações. Por fim, uma terceira abordagem é a utilização de operações avançadas nos agentes. Neste caso, os gerentes requisitam operações, tais como cálculos estatísticos ou balanceamento de carga, para os agentes, e estes as efetuam diretamente. Nestas três abordagens, um arquivo WSDL é utilizado para descrever as funcionalidades disponíveis do agente. O gerente

pode então descobrir em tempo de execução quais os agentes e funcionalidades disponíveis.

Entre as pesquisas sobre o uso de Web Services para o gerenciamento de redes, podem ser citados o trabalho de Martin-Flatin, Doffoel e Jeckle (MARTIN-FLATIN; DOFFOEL; JECKLE, 2004), que apresentam um *framework* desenvolvido para o gerenciamento de redes e provisionamento baseado em Web Services e o trabalho de Fioreze et al (FIOREZE et al, 2005), que abordam a definição e uso de *gateways* entre SNMP e Web Services.

A.2 Tecnologias Baseadas em Código Móvel

Esta seção aborda os paradigmas de código móvel e as principais abordagens baseadas nestes paradigmas utilizadas para o gerenciamento de redes. Inicialmente, os paradigmas de código móvel são apresentados. Nas subseções seguintes, são descritas as principais abordagens de código móvel utilizadas no gerenciamento de redes, discutindo o gerenciamento por delegação, a integração deste ao *framework* de gerenciamento do IETF, os agentes móveis e as redes ativas.

A.2.1 Paradigmas de Código Móvel

Uma importante revisão sobre mobilidade de código foi apresentada por Fuggetta, Picco e Vigna (FUGGETTA; PICCO; VIGNA, 1998). Este documento organizou a abordagem em três dimensões: **tecnologias**, **paradigmas** e **domínios de aplicação**. As tecnologias dizem respeito às linguagens e sistemas que fornecem os mecanismos que habilitam e suportam a mobilidade de código, e são utilizadas pelos desenvolvedores de aplicações de código móvel durante a implementação. Os paradigmas de código móvel, chamados pelos autores de *design paradigms*, envolvem os estilos de arquiteturas utilizados pelos desenvolvedores na definição das aplicações. Por fim, os domínios de aplicações são relacionados às classes de aplicações que compartilham objetivos comuns.

Estes autores definiram duas formas de mobilidade para os sistemas de código móvel: **mobilidade forte** (***strong mobility***) e **mobilidade fraca** (***weak mobility***). Os sistemas com mobilidade forte permitem a migração tanto do código como do estado de execução do código de uma unidade de execução de um ambiente computacional para outro. Já os sistemas de mobilidade fraca permitem apenas a transferência do código entre diferentes ambiente computacionais: o código transferido pode conter alguns dados de inicialização, mas o estado de execução não é migrado.

Estes autores apresentaram também uma das mais importantes classificações para os paradigmas de código móvel (FUGGETTA; PICCO; VIGNA, 1998). Nesta classificação, os paradigmas foram caracterizados de acordo com a localização dos componentes (código e recursos usados durante a execução) antes e depois da execução do serviço, pelo componente computacional que é responsável pela execução do código e pela localização onde a computação foi realizada. Quatro paradigmas são definidos:

- **Cliente-Servidor**: este paradigma é amplamente utilizado e não explora a mobilidade de código. Neste paradigma, o nodo servidor oferece um conjunto de serviços localizados em seu próprio nodo, possuindo os recursos e o código necessário para a execução dos serviços. Um nodo cliente solicita a execução de um serviço pela interação com o servidor. Como resposta, o

servidor executa o serviço solicitado utilizando o código correspondente e acessando os recursos relacionados presentes no próprio servidor. Usualmente, o serviço produz algum tipo de resultado que é retornado para o cliente.

- **Avaliação Remota** (***Remote Evaluation***, **REV**): neste paradigma, um nodo A possui o código necessário para executar um serviço, mas não possui os recursos necessários para esta execução, que se encontram em um nodo remoto B. Assim, o nodo A envia o código para a execução do serviço para o nodo B e o nodo B executa o código utilizando os recursos nele disponíveis. O resultado é enviado de volta para o nodo A.
- **Código sob Demanda** (***Code-on-Demand***, **COD**): neste paradigma, o nodo A já possui os recursos necessários para executar um serviço, mas não possui o código para manipular os recursos, que se encontra no nodo B. Assim, o nodo A interage com o nodo B solicitando o código relativo ao serviço. O nodo B envia o código para o nodo A, que pode então executar o serviço.
- **Agentes Móveis** (***Mobile Agent***, **MA**): neste paradigma, o código está localizado no nodo A, mas alguns dos serviços necessários estão localizados no nodo B. Assim, uma unidade de execução do nodo A migra para o nodo B com o código e alguns resultados intermediários, e completa sua execução no nodo B utilizando os recursos disponíveis de B. Como pode ser visto, a mobilidade deste paradigma envolve uma unidade de execução existente completa sendo movida para outro site, incluindo seu estado, o código necessário para sua execução e alguns recursos necessários para a execução da tarefa. Ele difere dos paradigmas de avaliação remota e código sob demanda, onde o foco é a transferência do código entre unidades de execução, e não a transferência da unidade de execução em si.

A figura a seguir esquematiza os paradigmas de código móvel.

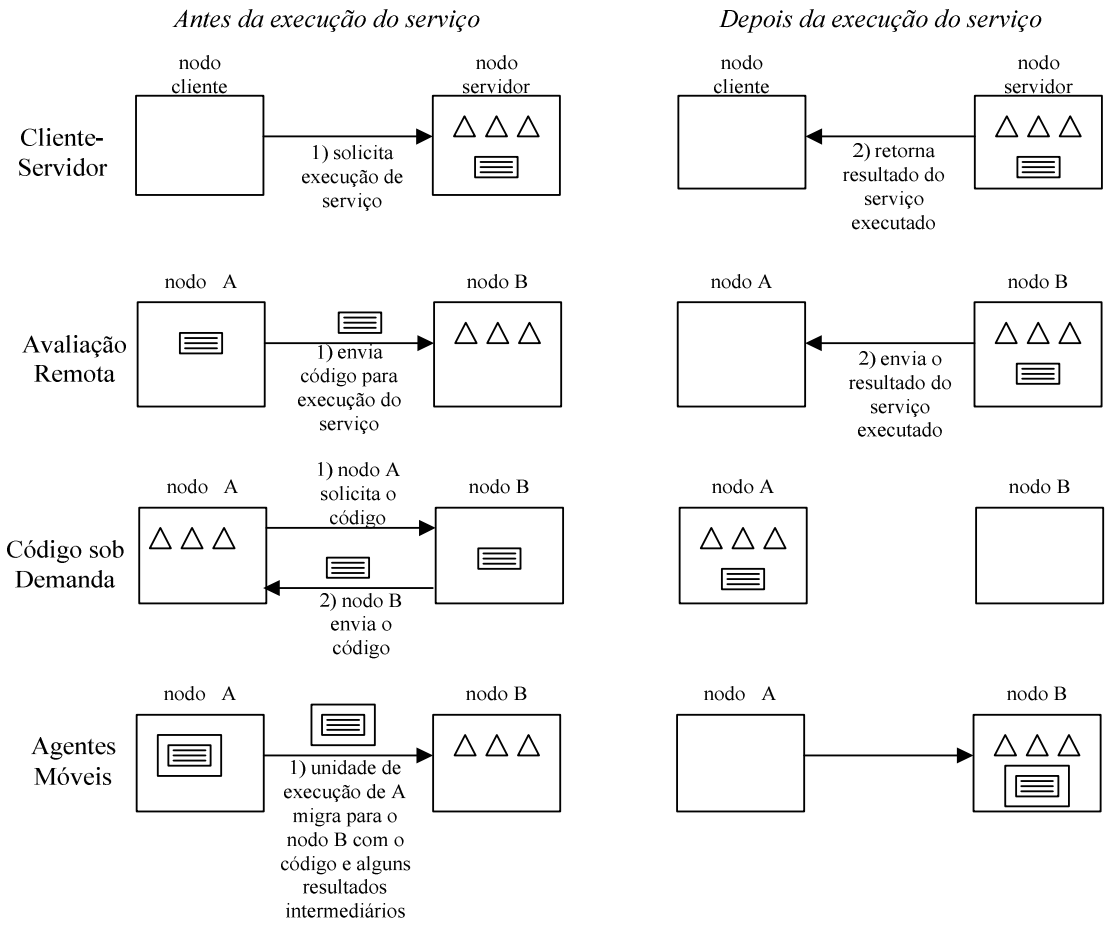


Figura A.1: Paradigmas de código móvel

Outras classificações de paradigmas de código móvel apresentam algumas diferenças. Por exemplo, Brooks (BROOKS, 2004) define seis diferentes paradigmas: cliente-servidor, avaliação remota, código sob demanda, migração de processos, agentes móveis e redes ativas. O paradigma de migração de processos envolve um sistema operacional que transfere processos de um nodo para outro para balanceamento de carga, enquanto que o paradigma de redes ativas envolve pacotes que movem através da rede re-programando a infra-estrutura de rede, combinando os paradigmas de agentes móveis e código sob demanda. Esta definição de redes ativas como paradigma difere da classificação de Fuggetta, Picco e Vigna (FUGGETTA; PICCO; VIGNA, 1998), que definem as redes ativas como um domínio de aplicação de código móvel (e não como paradigma).

Os paradigmas de código móvel podem ser implementados utilizando diversas tecnologias, que diferem nos mecanismos oferecidos para suportar mobilidade. Entre estas, pode-se citar Agent Tcl, Ara, Facile, Java, Java Aglets, TACOMA e Telescript (FUGGETTA; PICCO; VIGNA, 1998).

A.2.2 Gerenciamento por Delegação

O gerenciamento por delegação (*Management by Delegation*, MbD) foi proposto por Goldszmidt e Yemini (GOLDSZMIDT; YEMINI; YEMINI, 1991) (GOLDSZMIDT; YEMINI, 1995)(GOLDSZMIDT; YEMINI, 1998) e representou um marco no gerenciamento de redes distribuído. Este modelo é considerado o primeiro uso

dos paradigmas de código móvel no gerenciamento de redes, utilizando uma combinação do paradigma de avaliação remota e do paradigma cliente-servidor (MARTIN-FLATIN, 2003).

Este modelo segue o princípio de que as tarefas de gerenciamento podem ser delegadas dinamicamente para os equipamentos gerenciados da rede e executadas localmente nos equipamentos ao invés de serem executadas de modo centralizado. Assim, ao invés de mover os dados dos equipamentos para as plataformas de gerenciamento, se move e se executa as tarefas de gerenciamento nos próprios equipamentos.

O gerenciamento por delegação utiliza a tecnologia de processamento elástico, que suporta mover código de aplicação como agente delegado (*delegated agent*). A execução dos agentes delegados nos sistemas remotos é suportada por servidores elásticos (*elastic servers*) — processos *multi-thread* cujo código e estado do processo podem ser modificados e estendidos durante a execução. Agentes delegados são disparados dinamicamente para execução em um servidor elástico, sendo enviados e controlados através do protocolo de delegação remota (*remote delegation protocol*). Um cliente pode instanciar, suspender, abortar e retomar a execução de um agente delegado, assim como remover o agente do servidor. Os agentes delegados não precisam ser implementados por uma linguagem de programação em especial: implementações de servidores elásticos suportam, por exemplo, agentes implementados em linguagem C, C++ e TCL. O gerenciamento por delegação é a aplicação do processamento elástico para o gerenciamento de redes, onde tarefas de gerenciamento podem ser dinamicamente delegadas para os equipamentos gerenciados.

O gerenciamento por delegação foi integrado às arquiteturas de gerenciamento da ISO/ITU (International Standards Organization/International Telecommunication Union) e do IETF (Internet Engineering Task Force). A integração com a arquitetura da ISO/ITU resultou na definição de uma nova função de gerenciamento do protocolo *Common Management Information Protocol* (CMIP), denominada **command sequencer** (INTERNATIONAL TELECOMMUNICATION UNION, 1997). A integração com a arquitetura do IETF resultou na definição de um conjunto de MIBs SNMP, como será detalhado na seção a seguir.

A.2.3 Integração do Gerenciamento por Delegação no Framework do IETF

O modelo de gerenciamento por delegação foi integrado ao *framework* de gerenciamento Internet do IETF pelo grupo de trabalho *Distributed Management*, ou *disman* (IETF, 2010). Este grupo de trabalho desenvolveu meios para distribuir, executar e controlar tarefas de gerenciamento em localizações remotas, totalmente integrado ao *framework* baseado em SNMP, produzindo diversas MIBs SNMP.

As funções de gerenciamento a serem delegadas foram definidas como *scripts*, que são transferidos para localizações remotas onde são executados, podendo ser iniciados remotamente, receber parâmetros, e retornar os resultados para o gerente. A delegação de *scripts* de gerenciamento para entidades remotas foi definida na **Script MIB** (LEVI; SCHÖNWÄLDER, 2001). A Script MIB é responsável por diversas atividades: transferir *scripts* de gerenciamento para localizações distribuídas; iniciar, suspender, retomar e terminar os *scripts* nestas localizações; transferir parâmetros para os *scripts*; monitorar e controlar os *scripts* em execução; transferir os resultados produzidos pelos *scripts* em execução. Os *scripts* são implementados como código executável que pode

ser instalado em nodos da rede. As implementações da Script MIB podem suportar múltiplas linguagens simultaneamente, não tendo sido definida nenhuma linguagem em especial para os *scripts* (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000).

A instalação de um *script* em um nodo da rede é feita da forma a seguir. O gerente verifica na tabela `smLangTable` as linguagens suportadas pela implementação da Script MIB do nodo. Com esta informação, ele seleciona o *script* adequado em um repositório de *scripts* e cria uma nova linha na tabela `smScriptTable` do nodo para a instalação do *script*. O *script* pode ser então instalado de duas formas: o gerente pode colocar o *script* no nodo utilizando operações SNMP Set ou pode utilizar operações SNMP Set para escrever no nodo a URL do *script* e então solicitar ao agente SNMP do nodo que faça o *download* do *script* do repositório.

Quando um gerente deseja executar um *script* em um nodo, ele primeiro verifica se o *script* já está instalado no nodo, instalando-o caso contrário. O gerente cria a seguir uma linha na tabela `smLaunchTable` apontando para um *script* na tabela `smScriptTable` e informando os parâmetros de segurança do ambiente de execução. O *script* é iniciado com uma operação SNMP Set para o objeto `smLaunchStart`. Uma linha é criada automaticamente na tabela `smRunTable` para o *script* iniciado. Esta tabela é então utilizada para controlar o *script* e obter o resultado de sua execução (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000).

Além da Script MIB, outras MIBs foram definidas pelo grupo DISMAN do IETF. Entre estas, podem ser citadas a Schedule MIB, utilizada para agendar operações de gerenciamento periódicas ou em datas e horários específicos, a Alarm MIB, utilizada para modelar e armazenar alarmes e a Alarm Reporting Control MIB, utilizada para controlar o anúncio de situações de alarme, entre outras (IETF, 2005). Uma importante implementação da Script MIB, denominada Jasmin, foi desenvolvida pela Technical University of Braunschweig e pela NEC C&C Research Laboratories (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000) (STRAUSS; SCHÖNWÄLDER.; QUITTEK, 2001), sendo formada por vários componentes de software *open-source*.

A.2.4 Agentes Móveis

A aplicação do paradigma de agentes móveis para o gerenciamento de redes tem sido discutida por alguns autores (STEPHAN; RAY; PARAMESH, 2004) (SATOH, 2003) (DU; LI; CHANG, 2003) (BIESZCZAD; PAGUREK; WHITE, 1998). Este paradigma, apresentado na seção A.2.1, representa um paradigma de código móvel em que unidades de execução migram completamente de um nodo para outro, movendo seu estado, o código necessário para sua execução e alguns recursos necessários para a execução da tarefa, e, no nodo receptor, dão continuidade a sua execução.

Uma vantagem apresentada para esta tecnologia é que sistemas de gerenciamento complexos podem ser implementados de modo mais estruturado se seus componentes são projetados como agentes, cada um designado para realizar uma tarefa específica ou atingir um objetivo específico, trazendo benefícios com relação à engenharia de software (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000). A redução do tráfego de gerenciamento na rede é outro benefício apontado, já que agentes podem migrar para junto dos equipamentos gerenciados, coletar e processar os dados junto a estes equipamentos e reportar apenas circunstâncias excepcionais para a estação de gerência.

Entre os estudos desenvolvidos para gerenciamento de redes baseados em agentes móveis, podem ser citados a plataforma proposta por Stephan, Ray e Paramesh (STEPHAN; RAY; PARAMESH, 2004), que possui diferentes tipos de agentes que podem ser disparados para nodos remotos para coletar e processar informações de gerenciamento; e o *framework* proposto por Satoh (SATOH, 2003), utilizado para construção de sistemas de gerenciamento de redes baseados em agentes móveis onde os agentes podem mudar seu itinerário dinamicamente.

A.2.5 Redes Ativas

As redes ativas (SMITH; NETTLES, 2004) seguem o princípio de que as mensagens podem carregar código e dados, podendo ser usadas, assim, para adaptar rapidamente a rede para mudanças necessárias. Os principais objetivos dos sistemas de redes ativas incluem prover suporte para evolução facilitada e para customizações específicas das aplicações.

Duas abordagens principais são utilizadas para redes ativas: a **abordagem *programmable switch*** e a **abordagem *capsule*** (TENNENHOUSE et al, 1997). Na abordagem *programmable switch*, o formato dos pacotes e células é mantido, sendo utilizado um mecanismo discreto para o *download* de programas nos nodos. Nesta abordagem, é utilizada uma arquitetura onde o processamento de mensagens é separado da tarefa de injetar programas no nodo. Os usuários primeiro injetam o código nos nodos, e, então, enviam os pacotes através dos nodos programáveis, de modo similar a como é feito nas redes atuais. Quando o nodo recebe um pacote, ele examina seu cabeçalho e dispara o programa adequado para operar sobre o seu conteúdo.

A abordagem *capsule* possui um conceito diferente. Nesta abordagem, os pacotes passivos das arquiteturas de redes atuais são substituídos por mini programas ativos que são encapsulados em *frames* de transmissão e são executados nos nodos ao longo de seu caminho até o destino. Assim, todas as mensagens são formadas por programas. As mensagens podem conter também dados embutidos, mas cada mensagem deve conter ao menos uma instrução de código.

Kawamura e Stadler (KAWAMURA; STADLER, 2000) apontam que, embora as motivações para a proposta dos conceitos de redes ativas e agentes móveis tenham sido muito diferentes, tais abordagens estão começando a se sobrepor, especialmente no domínio de gerenciamento. Assim, um pacote ativo pode ser interpretado como um agente móvel simplificado que executa em todos os nodos ao longo de um caminho na rede. Da mesma forma, um agente móvel que move de um nodo para outro pode ser interpretado como um pacote ativo. As redes ativas têm sido aplicadas para diversas atividades de gerenciamento de redes, incluindo configuração de roteadores, detecção de elementos da rede e mapeamento da rede (ROUHANA; HORLAIT, 2002).

A.3 Agentes Inteligentes

Além dos modelos de gerenciamento baseados nas tecnologias distribuídas acima discutidas, uma abordagem que tem sido também proposta para uso em gerenciamento de redes é a baseada em agentes inteligentes (FRANKLIN; GRAESSER, 1996) (RUSSEL; NORVIG, 1995). Este conceito é originário da comunidade de Inteligência Artificial Distribuída (IAD), diferindo do conceito adotado para o termo agente e termos correlatos em áreas como a engenharia de software ou o gerenciamento de redes.

Diferentes definições têm sido propostas para descrever *agentes inteligentes*, não existindo um consenso sobre como definir *o que é um agente inteligente* ou quais são as *propriedades que este deve possuir para ser diferenciado dos agentes propostos em outras áreas do conhecimento*, como detalham alguns trabalhos (PETRIE, 1996) (FRANKLIN; GRAESSER, 1996) (MARTIN-FLATIN, 2003). Considerando esta restrição, entre as propriedades obrigatórias para agentes inteligentes, podem ser citadas as propostas por Martin-Flatin (MARTIN-FLATIN, 2003), que definem que agentes inteligentes devem ser:

- autônomos. Neste contexto, os agentes devem operar sem intervenção humana direta, e devem ter algum tipo de controle sobre suas ações e seu estado interno.
- reativos. Neste contexto, os agentes devem perceber o ambiente, e responder em tempo hábil para mudanças que ocorram neste.
- cooperativos, incluindo ser comunicativos e coordenados.
- temporalmente contínuos, sendo executados permanentemente.
- orientados a objetivos, incluindo ser proativos. A proatividade é explanada como uma propriedade que define que os agentes devem ser hábeis para tomar a iniciativa para atingir seu objetivo, em oposto a apenas reagir a eventos externos. A proatividade é descrita pelos autores como uma das principais diferenças entre os agentes móveis da comunidade de engenharia de software e os agentes inteligentes da DAI.

A aplicação do conceito de agentes inteligentes na área de gerenciamento de redes tem sido proposta por algumas pesquisas. Entre estas, podemos citar os trabalhos propostos por Mountzia e Rodosek (MOUNTZIA; RODOSEK, 1999), por Akashi e outros (AKASHI et al, 2000) e por Cheikhrouhou, Conti e Labetoule (CHEIKHROUHOU; CONTI; LABETOULLE, 2000).

A.4 Tecnologias para Gerenciamento de Redes e Classificações

Não há consenso na literatura sobre que organização utilizar para agrupar as tecnologias empregadas para gerenciamento de redes. Martin-Flatin, Znaty e Hubaux agrupam as tecnologias conforme o paradigma de gerenciamento que cada tecnologia implementa (MARTIN-FLATIN; ZNATY; HUBAUX, 1999)(MARTIN-FLATIN, 2003). As tecnologias são, assim, apresentadas do seguinte modo: tecnologias que seguem o paradigma centralizado, sendo subdivididas em gerenciamento baseado em SNMP (*e.g.*, SNMPv1 e o SNMPv2c) e gerenciamento baseado em HTTP; tecnologias que seguem o paradigma hierárquico fracamente distribuído, sendo subdivididas em gerenciamento de telecomunicações (englobando a arquitetura OSI/TMN) e gerenciamento em redes IP (*e.g.*, SNMPv2p com a MIB M2M e RMON); tecnologias que seguem o paradigma hierárquico fortemente distribuído, sendo subdivididas em paradigmas de código móvel (*e.g.*, SNMP Script MIB e redes ativas) e paradigmas de objetos distribuídos (*e.g.*, CORBA, Java RMI e WBEM); e tecnologias que seguem o paradigma cooperativo fortemente distribuído, baseadas no paradigma de agentes inteligentes.

Schönwälder, Quittek e Kappler se concentram em tecnologias que podem ser empregadas para a construção de sistemas de gerenciamento distribuídos e oferecem

delegação dinâmica (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2000). Tais tecnologias são organizadas em dois grupos: tecnologias que se integram e estendem *frameworks* de gerenciamento existentes (englobando o CMIP command sequencer e a SNMP Script MIB) e tecnologias que definem completamente novos *frameworks* para gerenciamento de redes (englobando agentes móveis e redes ativas).

Pavlou (PAVLOU, 2007) se concentra nas tecnologias em geral empregadas para o gerenciamento de redes e as agrupa em duas formas distintas: de acordo com uma perspectiva histórica e de acordo com o modo como as tarefas de gerenciamento são realizadas, propondo uma taxonomia. Os grupos definidos de acordo com a perspectiva histórica compreendem: abordagens procedurais (englobando as abordagens anteriores às arquiteturas de gerenciamento OSI e SNMP); abordagens baseada em protocolos orientados a objetos (*e.g.*, arquiteturas de gerenciamento OSI e SNMP); abordagens de objetos distribuídos (*e.g.*, CORBA e Java RMI); abordagens de gerenciamento por delegação e código móvel (*e.g.*, SNMP Script MIB, CMIP command sequencer e agentes móveis); e abordagens de gerenciamento baseado em Web e XML (*e.g.*, WBEM e Web Services). Por fim, a taxonomia de acordo com o modo como as tarefas de gerenciamento são realizadas (apresentada detalhadamente na seção 3.3.2) define duas abordagens principais para gerenciamento: o gerenciamento por invocação remota, subdividido em invocações através de um agente (*e.g.*, OSI-SM, SNMP e WBEM) e invocações diretamente para os objetos gerenciados (*e.g.*, CORBA, Java RMI e WebServices); e o gerenciamento por delegação, subdividido em abordagens baseada em gerente-agente com mobilidade *one-hop* (*e.g.*, SNMP Script MIB e CMIP command sequencer) e abordagens baseadas em código móvel com múltiplos *hops* (*e.g.*, agentes móveis). Este autor não inclui em suas classificações as abordagens baseadas no conceito de agentes inteligentes.

A organização empregada neste apêndice utilizou parcialmente a taxonomia de acordo com as tarefas de gerenciamento proposta por Pavlou, utilizando seu primeiro nível de categorias. O segundo nível das categorias não foi utilizado em virtude destas subcategorias serem baseadas no uso ou não de agentes do paradigma gerente-agente, ao mesmo tempo em que há múltiplos enfoques na área de gerenciamento de redes para o termo agente (conforme discutido anteriormente na seção de terminologia). Assim, a fim de tornar a apresentação mais intuitiva, optou-se, neste documento, por utilizar apenas o primeiro nível das categorias, incluindo ainda uma terceira categoria para as abordagens baseadas em agente inteligentes.

A utilização dos paradigmas de gerenciamento ao organizar as tecnologias, como realizado por Martin-Flatin, Znaty e Hubaux, não foi adotada por não ter sido considerada adequada, uma vez que uma tecnologia pode ser empregada para mais de um paradigma. A organização proposta por Schönwälder, Quittek e Kappler, por sua vez, enfoca apenas tecnologias de delegação dinâmica, enquanto que primeira organização utilizada por Pavlou possui enfoque apenas histórico.