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

PAULO EDUARDO DE CASTRO TELES BARBOSA

Uso de Técnicas de Visualização de Informação para o Estudo de Tráfegos de Gerenciamento de Redes

Dissertação apresentada como requisito parcial
para a obtenção do grau de
Mestre em Ciência da Computação

Prof. Dr. Lisandro Zambenedetti Granville
Orientador

Porto Alegre, maio de 2010

CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Barbosa, Paulo Eduardo de Castro Teles

Uso de Técnicas de Visualização de Informação para o Estudo de Tráfegos de Gerenciamento de Redes / Paulo Eduardo de Castro Teles Barbosa. – Porto Alegre: PPGC da UFRGS, 2010.

61 p.: il.

Dissertação (mestrado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação, Porto Alegre, BR–RS, 2010. Orientador: Lisandro Zambenedetti Granville.

1. Gerência de Redes de Computadores. 2. SNMP. 3. Visualização de Informação. I. Granville, Lisandro Zambenedetti. II. Title.

“When a man lies he murders some part of the world
These are the pale deaths which men miscall their lives
All this i cannot bear to witness any longer
Cannot the kingdom of salvation take me home.”
— Cliff Burton

AGRADECIMENTOS

Agradeço à minha família pelo apoio incondicional em todos os momentos;

Ao professor Lisandro Zambenedetti Granville, orientador deste trabalho, pelas valiosas lições passadas durante o mestrado;

Aos colegas do Grupo de Redes de Computadores da Universidade Federal do Rio Grande do Sul, por todo o companheirismo e apoio que manifestaram;

À Universidade Federal do Rio Grande do Sul e seu corpo docente, por terem tornado possível a realização deste e de outros trabalhos;

À todos que, direta ou indiretamente, me ajudaram a chegar até aqui;

Ao CNPQ, por ter fomentado minhas atividades de pesquisa durante este mestrado.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Programming Interface*
CG/CR	*Command Generator / Command Responder*
CSV	*Comma Separated Values*
GraphML	*Graph Modeling Language*
HTML	*HyperText Markup Language*
ICMP	*Internet Control Message Protocol*
IP	*Internet Protocol*
IRTF	*Internet Research Task Force*
JPEG	*Joint Photographic Experts Group*
MIB	*Management Information Base*
NMRG	*Network Management Research Group*
NO/NR	*Notification Originator / Notification Receiver*
OID	*Object Identifier*
PCAP	*Packet Capture*
PDF	*Portable Document Format*
PNG	*Portable Network Graphics*
RFC	*Request for Comments*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
SVG	*Scalable Vectorial Graphics*
VLAN	*Virtual Local Area Network*
XSLT	*eXtensible Stylesheet Language Transformations*
XML	*eXtendible Markup Language*

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Em 2008, o IRTF lançou a RFC *"SNMP Traffic Measurements and Trace Exchange Formats"*, que apresenta uma metodologia para coleta e análise de tráfego SNMP, com o objetivo de identificar características e padrões de uso desse protocolo nas redes em produção. Uma das limitações desta metodologia é a não especificação de um processo de visualização dos dados gerados, o que dificulta o estudo dos resultados obtidos através da aplicação da mesma. Existem alguns trabalhos no âmbito de redes de computadores que investigam a aplicação de técnicas de visualização de informação no estudo de tráfegos. No entanto, tais trabalhos disponibilizam apenas visualizações estáticas, com pouca ou nenhuma possibilidade de interação com o usuário, *i.e.*, elas não permitem que o mesmo explore e retrabalhe a maneira que os dados são visualizados. Esta dissertação de mestrado descreve e avalia técnicas de visualização de informação interativas adaptadas para o estudo de tráfegos gerados pelo SNMP, levando em conta as características peculiares do protocolo. Quatro protótipos de visualização de tráfegos SNMP foram implementos, integrados à ferramenta *Management Traffic Analyzer* e validados com base em um modelo aninhado para o projeto e análise de visualizações.

Palavras-chave: Gerência de Redes de Computadores, SNMP, Visualização de Informação.

Information Visualizaton Techniques Applied in the Study of Network Management Traffics

ABSTRACT

In 2008 IRTF released RFC *"SNMP Traffic Measurements and Trace Exchange Formats"*, which proposes a methodology for capturing and analysis of SNMP traffic traces, in order to identify the behavior and usage patterns of the protocol in production networks. One of the limitations of such methodology is the lack of a process definition to visualize the results of the gathered data, which makes the understanding of its results more difficult. There is some work in the computer network area dealing with the application of information visualization techniques in the study of network traces. Nevertheless, such work only provide static visualization techniques, with little or none user interaction possibilities. That is, they do not allow the user to explore and rebuild the way data is visualized. This masters dissertation presents and evaluates interactive information visualization techniques, adapted for the study of SNMP traces and its unique features. Four visualization prototypes were implemented, integrated in the tool Management Traffic Analyzer, and validated following a nested model for the project and evaluation of visualization techniques.

Keywords: Network Management, SNMP, Information Visualization.

1 INTRODUÇÃO

O *Simple Network Management Protocol* (HARRINGTON; PRESUHN; WIJNEN, 2002) (SNMP) vem sendo utilizado há mais de 15 anos para o monitoramento, controle e configuração de elementos de rede. Desde então, o uso extensivo do protocolo fez com que os operadores de rede e pesquisadores adquirissem um conhecimento significativo sobre o seu funcionamento, o que o levou a encontrar-se bem documentado e entendido pelos mesmos. No entanto, ainda hoje pouco se sabe sobre os padrões de uso do protocolo em redes de produção, sendo que não está claro quais funcionalidades do SNMP estão sendo utilizadas (ou encontram-se obsoletas), quais informações são mais frequentemente consultadas e quais são os padrões de interação entre os elementos de uma rede.

O *Internet Research Task Force* (IRTF), através da RFC *"SNMP Traffic Measurements and Trace Exchange Formats"* (SCHOENWAELDER, 2008), apresentou uma metodologia sistemática para medições e geração de estatísticas sobre o uso do SNMP, com o intuito de desvendar características do uso do protocolo ainda não efetivamente conhecidas. Através do uso da metodologia, torna-se possível, por exemplo:

- mensurar quais recursos do protocolo (ex.: versões, operações, *Management Information Bases* (MIBs)) estão sendo utilizados;
- apurar como o uso do SNMP difere nos vários tipos existentes de redes de computadores e organizações;
- modelar quais são os padrões de interação comumente observados na utilização do protocolo;
- fazer o planejamento de possíveis otimizações na implementação de novas versões do protocolo;
- obter uma base para a comparação com outras abordagens de gerenciamento;
- formular um guia para o projeto de novas MIBs.

Apesar da metodologia proposta pelo IRTF ser de grande relevância para a área de gerenciamento de redes, a mesma ainda possui algumas limitações. Dentre elas pode-se destacar a ausência de uma especificação de processos de visualização dos dados gerados pelas análises. Levando-se em consideração a crescente complexidade associada a infraestruturas de rede, que são comumente compostas por dispositivos heterogêneos e topologias de larga escala, o processo de análise proposto pela metodologia tende a gerar grandes quantidades de dados. Consequentemente, um estudo sobre os dados brutos sem o uso de abstrações visuais torna-se inviável. Para contornar esta limitação, pode-se fazer

uso de técnicas de visualização de informação, que são representações dos dados resultantes das análises através de imagens, gráficos ou animações, fazendo dessa forma uso das propriedades do sistema visual humano para explorar e formular inferências dentro de um conjunto de dados e permitindo a identificação de padrões, anomalias e outras inferências de maneira rápida e intuitiva.

Um dos principais fatores que tornam técnicas de visualização de informação eficientes são os mecanismos de interação que elas disponibilizam para os usuários. Estes permitem que o operador explore os conjuntos de dados de maneira que apenas a informação desejada seja apresentada. O uso de mecanismos de interação com o usuário permite a formulação de inferências usualmente não conseguidas na visualização de um conjunto de dados como um todo. Alguns exemplos de possibilidades de interação com usuário incluem a aplicação de filtros nos dados e operações para modificar o foco da visualização, como *zooming* e *panning*.

Existem alguns trabalhos no âmbito de redes de computadores que investigam a aplicação de técnicas de visualização de informação no estudo de tráfegos. Mansmann e Vinnik (MANSMANN; VINNIK, 2006) propuseram um método para visualizar o tráfego de hospedeiros IP baseado em uma técnica de visualização conhecida como *treemap*, de forma a obter inferências a respeito do comportamento dos fluxos de rede. Keim *et al.* (KEIM et al., 2006), por sua vez, desenvolveram um conjunto de ferramentas de visualização que procura antecipar potenciais gargalos ou problemas na rede ao mostrar atividades típicas de comunicação de rede. No âmbito de gerenciamento de redes, Shoenwaelder *et al.* (SCHOENWAELDER et al., 2007) apresentaram uma abordagem para capturar e analisar amostras de tráfego SNMP, mostrando os resultados preliminares das análises através de visualizações estáticas. Salvador *et al.* (SALVADOR; GRANVILLE, 2008a) apresentaram três técnicas de visualização que mostram informações relacionadas à análise de tráfego SNMP, seguindo a metodologia proposta pelo IRTF para captura e análise de tráfego SNMP (SCHOENWAELDER, 2008). Por sua vez, Dobrev *et al.* (DOBREV; STANCU-MARA; SCHOENWAELDER, 2009) utilizaram ferramentas de visualização existentes para visualizar em tráfegos SNMP e NetFlow a dinâmica de interação entre os nodos de uma rede, procurando determinar padrões nos ciclos de *polling* das estações e nas mudanças de topologias de rede.

Apesar de os trabalhos mencionados fazerem uso de técnicas de visualização de informação nos seus estudos, até então as investigações relacionadas a análise de tráfego de gerenciamento de redes disponibilizam apenas visualizações estáticas, com pouca ou nenhuma possibilidade de interação com o usuário, *i.e.*, elas não permitem que o mesmo explore e retrabalhe a maneira que os dados são visualizados. Como mencionado anteriormente, possibilidades de interação podem conduzir a novas inferências nos dados analisados, que não seriam possíveis ao se utilizar apenas visualizações estáticas. Por isso, esforços no sentido de construir técnicas de visualização interativas são encorajados no atual estado-da-arte de visualizações em gerenciamento de redes.

Assim, considerando o estágio incipiente em que se encontra, no âmbito de análise de tráfegos de gerenciamento de redes, o uso de interatividade em técnicas de visualização de informação, esta dissertação tem por objetivo apresentar e avaliar técnicas de visualização de informação interativas adaptadas para o estudo do SNMP e suas características peculiares, desenvolvidas em conformidade com o modelo de visualização de informação proposto por Card (CARD; MACKINLAY; SHNEIDERMAN, 1999). As principais contribuições deste trabalho são: implementação de quatro protótipos de visualização de tráfegos SNMP, que mapeiam as topologias de rede de gerenciamento encontradas nos tráfe-

gos, a quantidade de mensagens/versões do SNMP encontradas, a árvore MIB dos objetos SNMP vistos em um tráfego e o relacionamento existente entre objetos SNMP; integração dos protótipos à ferramenta *Management Traffic Analyzer* (SALVADOR; GRANVILLE, 2008b), que integra em um ambiente Web todos as etapas da metodologia de captura e análise de tráfego SNMP proposta pelo IRTF; e a apresentação dos resultados de uma avaliação que teve por objetivo medir a eficiência do uso de técnicas de visualização no estudo de tráfegos de gerenciamento de redes.

O restante deste trabalho está organizado da seguinte maneira. O Capítulo 2 apresenta uma revisão bibliográfica das áreas em que esta dissertação encontra-se inserida, apresentando a metodologia utilizada para a coleta e análise de tráfego SNMP e discutindo alguns conceitos da área de visualização de informação utilizados no decorrer do texto. O Capítulo 3 apresenta os protótipos de visualização desenvolvidos para analisar e identificar padrões nos tráfegos SNMP. O Capítulo 4 discorre sobre os detalhes de implementação dos protótipos de visualização. O Capítulo 5 mostra a avaliação dos protótipos de visualização de tráfego SNMP, de forma a mensurar a eficiência do uso de técnicas de visualização de informação no estudo de tráfegos de gerenciamento. Por fim, o Capítulo 6 mostra as conclusões alcançadas e algumas propostas de trabalhos futuros.

2 REVISÃO BIBLIOGRÁFICA

Ao longo do desenvolvimento deste trabalho foi empregada uma série de conceitos pertinentes às áreas de gerenciamento de redes e computação gráfica. A seguir, serão abordados alguns temas necessários para um melhor entendimento do presente trabalho, quais sejam: metodologia para coleta e análise de tráfegos SNMP e visualização de informação.

2.1 Metodologia para Medições sobre Tráfegos SNMP

Em outubro de 2008, o *Network Management Research Group* (NMRG) do IRTF apresentou a *Request for Comments* (RFC) *"SNMP Traffic Measurements and Trace Exchange Formats"* (SCHOENWAELDER, 2008). Este documento descreve uma metodologia sistemática para coleta, medições e geração de estatísticas sobre capturas de tráfego SNMP, com o intuito de desenvolver um melhor entendimento de como o SNMP é utilizado em redes em produção ativas, através da identificação de padrões no uso do protocolo. Tais padrões incluem, dentre outros: quais informações são frequentemente consultadas; o relacionamento entre tráfego periódico e aperiódico; uso de objetos obsoletos; e quais são as MIBs mais populares. Essa metodologia é composta de etapas bem definidas e sua relativa simplicidade facilita a sua implementação.

Uma das motivações que levaram à publicação dessa metodologia foi o fato de que, apesar de várias publicações recentes tratarem da performance do SNMP em geral, do impacto da adoção de mecanismos de segurança no SNMPv3 e da performance relativa do SNMP comparada ao uso de Web Services, as mesmas carecem de uma melhor fundamentação, devido aos autores tipicamente assumirem certos padrões de interação do SNMP sem evidências experimentais sobre a consistência desses padrões (SCHOENWAELDER, 2008).

Nas próximas subseções serão apresentadas as etapas que compõem a metodologia do IRTF, assim como os aspectos do SNMP que devem ser esclarecidos a partir das análises geradas pelo uso dessa metodologia.

2.1.1 Captura de Tráfego SNMP

A primeira etapa da metodologia para medições sobre tráfegos SNMP do IRTF consiste na captura de amostras de tráfego SNMP em arquivos do tipo PCAP (*Packet Capture*). Esta pode ser feita através de *sniffers* como o Wireshark (WIRESHARK, 2009) e o TCPDUMP (JACOBSON; LERES; MCCANNE, 2009), ou por outras aplicações similares. Deve-se escolher com cautela o ponto em que o *sniffer* será posicionado na rede, de forma que ele possa capturar o maior número possível de pacotes SNMP. Especialmente

em redes locais baseadas em *bridges*, é importante garantir que a estação que fará o monitoramento tenha acesso a todas as VLANs (*Virtual LANs*) por onde passe tráfego de gerenciamento. Na maioria dos casos, o *sniffer* deve ser posicionado muito próximo do sistema de gerenciamento, assim como devem ser configuradas portas de monitoramento específicas nas redes locais baseadas em *bridges*.

A metodologia recomenda que a duração das capturas seja de, no mínimo, uma semana. Com isso objetiva-se capturar os padrões diários de troca de mensagens e um ciclo de comportamento semanal do protocolo. No entanto, períodos ainda maiores de captura são encorajados, para uma maior precisão nas análises a serem feitas. Caso o tamanho dos arquivos contendo o tráfego SNMP seja muito grande, pode-se dividir o mesmo em vários pedaços através do uso de ferramentas como o TCPSLICE e o PCAPMERGE (JACOBSON; LERES; MCCANNE, 2009).

Por fim, para cada tráfego capturado, um conjunto de metadados deve ser armazenado juntamente com os arquivos PCAP. Os metadados devem incluir informações como: onde a captura foi feita (nome da rede e da organização, descrição do ponto da rede onde o tráfego foi coletado), data de coleta, informações para contato, tamanho da captura, quaisquer eventos anormais ocorridos, falhas em equipamentos, mudanças na infraestrutura de rede, dentre outras informações. Também é importante prover um identificador unívoco para cada um dos tráfegos.

2.1.2 Conversão dos Arquivos PCAP em Formato Legível

Nesta segunda etapa, os arquivos PCAP capturados na etapa anterior devem ser convertidos para um formato que seja legível tanto por operadores quanto por máquinas, para facilitar que dados confidenciais não estejam presentes na captura (tarefa do operador) e para que as informações relevantes sejam extraídas de maneira eficiente (tarefa de computadores). Os formatos adotados pela metodologia e que seguem essas premissas são o XML *(eXtended Markup Language)* e o CSV *(Comma Separated Values)*.

Uma escolha natural para atender os requisitos mencionados acima é a linguagem XML, que é facilmente legível por humanos e possui suporte para a maioria das linguagens de programação de alto nível, o que facilita o desenvolvimento de *scripts* capazes de extrair informações úteis a respeito dos tráfegos. No entanto, como XML é uma linguagem que faz uso de muitas *tags* (causando sobrecarga no processamento), arquivos nesse formato podem ser difíceis de serem processados, se o tráfego neles representado for muito extenso. Para contornar este problema, a metodologia recomenda que se utilizem APIs que façam o *streaming* do arquivo XML, para evitar que uma representação completa do arquivo seja colocada na memória, o que degradaria o desempenho do sistema em caso de tráfegos muito grandes.

Uma alternativa mais leve em relação ao XML é o formato CSV, que consiste basicamente em se armazenar num arquivo de texto puro as informações que compõem uma mensagem SNMP sequencialmente, numa única linha, com seus valores separados por vírgula. Em caso do emprego do CSV, aconselha-se que apenas as informações mais relevantes sobre o SNMP sejam registradas, de forma a criar arquivos mais compactos e rápidos de processar.

2.1.3 Filtragem do Tráfego para Anonimização de Informações Sensíveis

As mensagens do protocolo SNMP usualmente carregam informações sensíveis que, por questões de segurança, não podem ser divulgadas (*e.g.*, listas de controle de acesso e strings de comunidade). Para garantir a segurança dos operadores que se dispuserem a

oferecer amostras de tráfego SNMP pertencentes a suas redes, nessa etapa um processo de remoção/anonimização desses dados sensíveis é empregado. Embora conceitualmente este processo constitua-se em uma nova etapa, pode fazer parte da etapa anterior, por razões de desempenho.

A filtragem desses dados pode ser feita através da análise e alteração da representação do tráfego SNMP no formato XML ou CSV. No caso do formato XML, processadores XSLT padrão, como o xsltproc (XMLSOFT, 2009), podem ser utilizados para esse propósito. Também poderão ser utilizadas bibliotecas de linguagens de programação de alto nível, específicas para o tratamento de documentos XML, para a manipulação desses arquivos. Por exemplo, pessoas familiarizadas com a linguagem Perl poderão utilizar a biblioteca XML::LibXML (XMLSOFT, 2009) para realizar a filtragem dos dados obtidos.

2.1.4 Armazenamento dos Tráfegos Capturados

Tanto o arquivo PCAP contendo a captura de tráfego SNMP bruta quanto sua representação filtrada em formato XML ou CSV devem ser armazenados em repositórios de dados estáveis. Tais repositórios devem ser mantidos por grupos de pesquisa, operadores de rede, ou por ambos. É de fundamental importância que os tráfegos capturados não sejam perdidos ou modificados, pelo fato de os mesmos formarem a base de futuros projetos de pesquisa e possam ser necessários para verificar resultados de pesquisa publicados.

Algoritmos de compressão sem perdas podem ser utilizados para comprimir arquivos grandes, de forma a diminuir o custo de armazenamento dos mesmos em repositórios estáveis. Ademais, algoritmos de criptografia podem ser utilizados para aumentar a segurança dos dados armazenados.

A metodologia enfatiza que é importante armazenar, além dos arquivos formatados em XML ou CSV, as capturas em formato PCAP. Isto se dá pelo fato de que as amostras PCAP são a fonte mais autêntica de informações sobre o protocolo SNMP, e eventuais mudanças na metodologia podem requerer um novo processamento dos arquivos PCAP para reconstruir os formatos intermediários.

2.1.5 Análise das Capturas de Tráfego

O último passo da metodologia consiste na análise dos arquivos filtrados, a fim de se agregar estatísticas em relação aos dados de tráfego SNMP contido nesses arquivos e, a partir delas, extrair informações que ajudem a responder às questões em aberto sobre a utilização prática do SNMP. A análise dos dados é processada através da execução de programas ou *scripts* que procuram agregar os dados do tráfego de gerenciamento de forma a fornecer informações úteis, como predominâncias e/ou tendências dentro desses tráfegos (*e.g.*, qual versão do protocolo é mais utilizada, qual a relação entre os objetos carregados por determinadas mensagens e quais os objetos mais acessados).

Devido à abundância de bibliotecas para tratamento de arquivos XML existentes entre as linguagens de alto nível, os *scripts* de análise dos dados filtrados poderão ser escritos em praticamente qualquer linguagem de programação. Contudo, a metodologia recomenda que esses *scripts* sejam implementados utilizando-se a linguagem de programação Perl juntamente com a biblioteca XML::LibXML, a fim de se criar um "vocabulário" comum entre pesquisadores e operadores de rede, e também entre os diversos grupos que estão realizando essa pesquisa pelo mundo. Além disso, Perl possui uma vantagem natural com relação a linguagens de programação como C/C++, porque geralmente apresenta um menor tempo necessário para o desenvolvimento dos *scripts* de análise.

2.1.6 Aspectos dos Tráfegos SNMP a serem Analisados

Esta subseção enumera uma lista de perguntas que podem ser respondidas através da análise de tráfegos SNMP. Estas são as questões encontradas na RFC que apresenta a metodologia descrita nessa seção (SCHOENWAELDER, 2008). No entanto, os autores enfatizam que a lista não é exaustiva, o que permite a outros pesquisadores formular novas questões em relação ao funcionamento do SNMP.

O primeiro aspecto citado pela metodologia é o cômputo de **estatísticas básicas**, que corresponde ao conjunto de informações genéricas em relação ao tráfego que foi analisado. Dentre os elementos que compõem essa análise, pode-se citar: versões e operações do SNMP utilizadas, distribuição do tamanho de mensagens, número de agentes e gerentes na rede, dentre outros.

Uma característica intrínseca do SNMP é a sua utilização tanto para periodicamente consultar dispositivos quanto para atender requisições aperiódicas feitas por um operador ou aplicação de gerenciamento. Estes dois tipos de abordagem geram, respectivamente, tráfegos periódicos e aperiódicos. É importante entender a **relação entre o tráfego periódico e aperiódico** gerado, para uma melhor compreensão da abordagem de gerenciamento que está sendo utilizada em uma determinada rede em produção.

As mensagens SNMP possuem seu tamanho restrito pelos mapeamentos da camada de transporte e pelos *buffers* utilizados pelos mecanismos SNMP. Devido a isso, e objetivando subsidiar aprimoramentos nas futuras versões do protocolo SNMP, é interessante investigar qual a **distribuição dos tamanhos das mensagens** encontradas na amostra de tráfego SNMP. Além disso, é importante que se compreenda a **distribuição da latência**, especialmente a distribuição do tempo de processamento pelos dispositivos que estão processando as requisições do protocolo. Algumas implementações do SNMP inferem os atrasos da rede através da medição do tempo de requisição-resposta, abordagem essa que poderá ser validada ou não a partir do estudo desse tempo de processamento das requisições.

O SNMP permite que as estações de gerenciamento requisitem informações de múltiplos agentes de maneira concorrente. É interessante identificar qual o **nível de concorrência** típico observado em redes em produção, ou mesmo se plataformas de gerenciamento fazem uso de abordagens mais sequenciais para a requisição de dados.

As tabelas SNMP podem ser lidas de diversas maneiras. A maneira mais simples (e ineficiente) é a leitura célula por célula, percorrendo-se as colunas da tabela sequencialmente. Abordagens mais avançadas fazem a leitura de tabelas linha a linha, ou mesmo a leitura de múltiplas linhas de uma só vez. Outras otimizações incluem a supressão da leitura de elementos de índice, possível na maioria dos casos, e a requisição apenas de um subconjunto das colunas de uma tabela. Através do conhecimento de quais **abordagens para leitura de tabelas** estão sendo utilizadas, pode-se verificar se as consultas de tabelas em uma determinada rede estão sendo otimizadas.

As aplicações de gerenciamento são responsáveis por realizar periodicamente o *polling* entre os dispositivos da rede, a fim de determinar o seu status. Através do uso do conceito de *traps*, os dispositivos gerenciáveis podem ser programados para notificarem os gerentes SNMP sobre eventos que tenham ocorrido, para que esses gerentes adotem as medidas aplicáveis àquele evento de maneira mais rápida do que o processo convencional de *polling*. Análises de tráfego SNMP podem identificar exatamente o quanto de *polling* convencional e o quanto de **notificações utilizando *traps*** estão sendo realmente empregados. Uma questão ainda mais particular que deve ser levantada é a identificação de quanto as notificações geradas por *traps* levam a uma mudança no comportamento do

polling das estações de gerenciamento.

Outro aspecto do SNMP a ser estudado se refere à identificação dos **módulos MIB populares**. Uma análise dos prefixos dos *Object Identifiers* (OIDs) pode identificar quais módulos MIB estão sendo mais utilizados, e os objetos mais importantes definidos por estes módulos. Este tipo de estudo ajuda no desenvolvimento e manutenção dessas MIBs e de outras relacionadas.

Atualmente, muitos objetos do protocolo SNMP são considerados obsoletos, pelo fato dos mesmos não conseguirem representar a realidade dos dispositivos de redes atuais. Como exemplo desse fato, pode-se citar o objeto **ipRouteTable**, lançado na Internet em 1993 e posteriormente considerado obsoleto por não ser apto a representar roteamento sem uso de classes. Entretanto, apesar de considerados obsoletos, alguns desses objetos continuam sendo citados em publicações populares e até mesmo em trabalhos acadêmicos. Devido a isso, seria interessante verificar se as aplicações SNMP de fato ainda fazem **uso de objetos obsoletos**, ou se elas foram atualizadas para substituírem os mesmos por suas novas versões.

A fim de se estimar o tamanho de mensagens SNMP, algumas vezes assume-se alguns valores sobre a distribuição do tamanho de codificação dos vários tipos de dados dessas mensagens. Esta estimativa é utilizada para determinar restrições de transporte e de *buffers* das implementações do protocolo. Por isso, é interessante estudar nos tráfegos SNMP a **distribuição do tamanho da codificação** dos tipos de dados encontrados nas mensagens.

No SNMP, os contadores podem sofrer descontinuidades (MCCLOGHRIE; PERKINS; SCHOENWAELDER, 1999). Um indicador de descontinuidade muito utilizado é o escalar **sysUpTime** da MIB SNMPv2, que pode resetar seu valor para indicar descontinuidade de contadores. Algumas MIBs introduzem indicadores de descontinuidade mais específicos, como o **ifCounterDiscontinuityTime** da IF-MIB. É interessante estudar a relação entre **contadores e descontinuidades**, para inferir até que ponto estes objetos estão sendo utilizados pelas plataformas de gerenciamento para lidar com eventos de descontinuidade.

Geradores de comandos cooperativos podem fazer uso de travas (*locks)* de alerta para coordenar o uso do protocolo SNMP durante as operações de escrita de informações. O objeto escalar **snmpSetSerialNo** da MIB SNMPv2 é o objeto padrão para este tipo de operação. É interessante descobrir se existem geradores de comandos que coordenam suas ações através do **uso de *spin locks***.

A operação de criação de linhas não é suportada nativamente pelo SNMP. Entretanto, tabelas conceituais que possuem suporte para a criação de linhas tipicamente fornecem uma coluna de controle que utiliza a convenção textual **RowStatus**, definida na MIB SNMPv2-TC (CASE et al., 1996). O objeto **RowStatus** em si suporta diferentes modos de criação de linhas, tais como os modos *createAndWait* e *createAndGo*. Além disso, diferentes abordagens podem ser utilizadas para inferir se o identificador de instância não possui uma semântica especial associada. Devido a isso, é interessante estudar quais das diferentes abordagens existentes para **criação de linhas em tabelas** estão sendo realmente utilizadas nas aplicações de gerenciamento das redes em produção.

2.2 Visualização de Informação

Existem situações em que dados abstratos, comumente em grande volume, necessitam de análise para que se possa extrair inferências sobre os mesmos. Nesse contexto se insere

a visualização de informação, uma área de aplicação de técnicas de computação gráfica, geralmente interativas, que visam auxiliar o processo de análise e compreensão de um conjunto de dados, através de representações gráficas manipuláveis (FREITAS, 2007).

Este processo é composto por etapas definidas em modelos de referência de visualização, que permitem a identificação dos componentes essenciais a serem considerados na utilização de uma determinada técnica ou no desenvolvimento de uma nova. Dentre esses modelos destaca-se o modelo de visualização de Card *et al.* (CARD; MACKINLAY; SHNEIDERMAN, 1999), cujas etapas são mostradas na Figura 2.1.

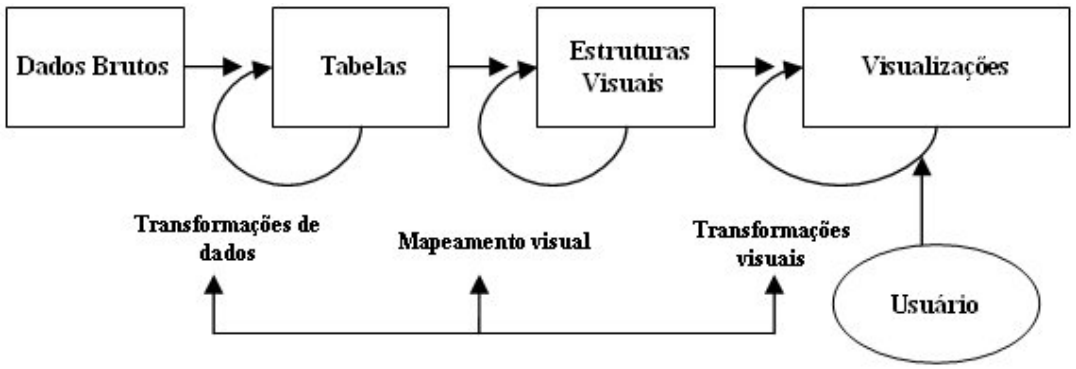

Figura 2.1: Modelo de Visualização de Card *et al.*

Esse modelo divide o processo de visualização de informação em quatro etapas:

- **Coleta dos dados**: na primeira etapa os dados que se deseja analisar são coletados e armazenados em repositórios de dados;
- **Representação dos dados em tabelas**: nesta etapa as fontes de dados geradas pela fase anterior são mapeadas para tabelas, representações dos dados em um formato compatível com a visualização a ser gerada;
- **Representação visual**: nesta etapa as tabelas resultantes são mapeadas para abstrações visuais, modelos de dados que contêm características visuais como layout, cor, tamanho e forma dos elementos visuais, e que devem conter toda a informação necessária para gerar uma representação visual dos dados;
- **Visualizações**: por último, os componentes da representação são renderizados para formar as visualizações (do inglês *views*, diferindo do processo de visualização de informação), cujo resultado é exibido para o usuário.

2.2.1 Visualização de Tráfegos de Gerenciamento

Como é possível notar na seção anterior, em nenhum momento na metodologia de captura e análise de tráfego SNMP é mencionado como os dados resultantes da aplicação da mesma devem ser visualizados. No entanto, a quantidade de informações gerada é potencialmente muito grande, o que dificulta ou mesmo inviabiliza um estudo sobre os dados da forma como são representados após a última etapa da metodologia.

Para ilustrar como esse problema pode ser resolvido, um exemplo de aplicação de técnica de visualização em tráfegos SNMP é mostrado a seguir. Seguindo o modelo proposto por Card *et al.*, os dados brutos correspondem aos arquivos PCAP capturados, que contêm

Operação	Versão	0h	1h	2h	3h	4h	5h	6h	7h	8h	9h	10h	11h
get-request	v1	3097	3096	3098	3094	3100	3131	3144	3117	3092	3093	3097	3090
get-next-request	v1	7056	7056	7056	7056	7056	7056	7056	7056	7056	7056	7056	7056
get-bulk-request	v1	0	0	0	0	0	0	0	0	0	0	0	0
set-request	v1	0	0	0	0	0	0	0	0	0	0	0	0
trap	v1	34	30	0	5	18	4	30	9	75	0	78	34
trap2	v1	0	0	0	0	0	0	0	0	0	0	0	0
inform	v1	0	0	0	0	0	0	0	0	0	0	0	0
response	v1	9130	9132	9134	9129	9136	9059	9072	9081	9124	9081	9088	9113
report	v1	0	0	0	0	0	0	0	0	0	0	0	0
get-request	v2c	38080	38061	38005	38057	38055	37807	37802	37887	38029	37729	37730	37974
get-next-request	v2c	24	24	24	24	24	24	24	24	24	24	24	24
get-bulk-request	v2c	2368	2364	2364	2364	2364	2364	2364	2364	2364	2364	2364	2374
set-request	v2c	0	0	0	0	0	0	0	0	0	0	0	0
trap	v2c	0	0	0	0	0	0	0	0	0	0	0	0
trap2	v2c	309	257	217	220	252	436	460	1038	324	221	397	251
inform	v2c	0	0	0	0	0	0	0	0	0	0	0	0
response	v2c	40438	40440	40384	40440	40440	40168	40165	40259	40415	40092	40093	40366
report	v2c	0	0	0	0	0	0	0	0	0	0	0	0
get-request	v3	0	0	0	0	0	0	0	0	0	0	0	0
get-next-request	v3	0	0	0	0	0	0	0	0	0	0	0	0
get-bulk-request	v3	0	0	0	0	0	0	0	0	0	0	0	0
set-request	v3	0	0	0	0	0	0	0	0	0	0	0	0
trap	v3	0	0	0	0	0	0	0	0	0	0	0	0
trap2	v3	0	0	0	0	0	0	0	0	0	0	0	0
inform	v3	0	0	0	0	0	0	0	0	0	0	0	0
response	v3	0	0	0	0	0	0	0	0	0	0	0	0
report	v3	0	0	0	0	0	0	0	0	0	0	0	0

Tabela 2.1: Mensagens SNMP em Intervalos de 1 Hora

as mensagens SNMP trocadas entre os elementos da rede. Através da aplicação da metodologia proposta pelo IRTF, chega-se às tabelas descritas na segunda etapa do modelo de visualização, que contêm os resultados das análises feitas sobre os tráfegos SNMP. A Tabela 2.1 mostra o resultado de uma análise das mensagens SNMP presentes em um intervalo de 12 horas de captura, retirada de uma amostra de tráfego de gerenciamento da Rede Nacional de Pesquisa (RNP). Como se pode notar, mesmo em um intervalo de tempo relativamente pequeno (considerando que a metodologia recomenda capturas de no mínimo 1 semana de tráfego), fica difícil inferir padrões na troca de mensagens.

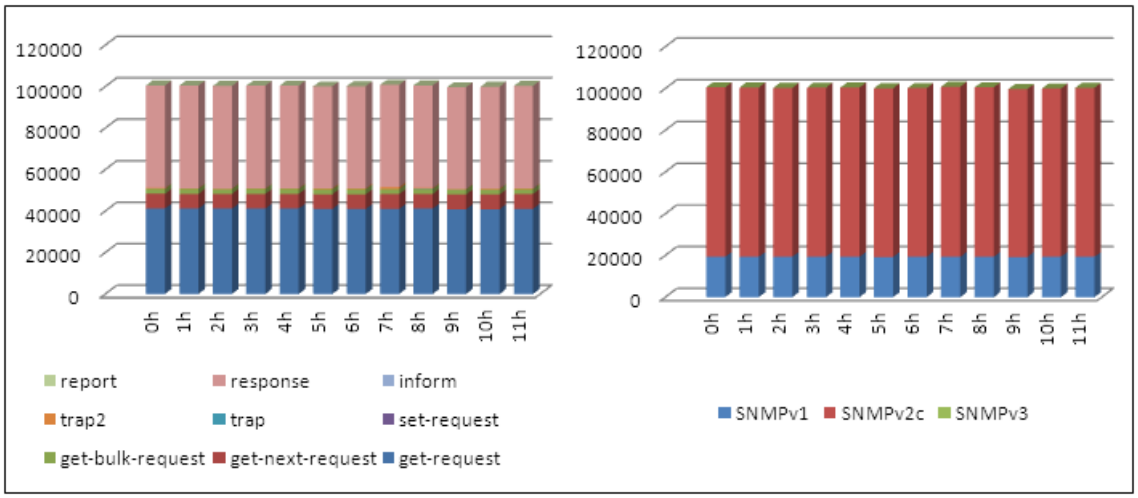

Figura 2.2: Mensagens agrupadas por tipo e versão do SNMP

A dificuldade acima mencionada pode ser dirimida através de uma visualização de histograma de barras seccionado. Neste caso, as abstrações visuais são retângulos, cuja cor diferencia as mensagens SNMP e o tamanho representa a quantidade daquele tipo de mensagem encontrada no tráfego. A partir dessa abstração, renderiza-se o histograma, sendo que o resultado obtido é mostrado na Figura 2.2. Nela as mensagens SNMP são agrupadas de duas formas: por tipo de mensagem e por versão do protocolo. As barras são seccionadas, sendo que cada secção representa um tipo de mensagem (esquerda) ou

versão do protocolo (direita). Neste exemplo pode-se verificar facilmente que as mensagens do tipo **response** são maioria no tráfego, e que a versão **v2c** é a mais utilizada. Estes são apenas alguns exemplos de como o uso de visualizações pode ajudar no tipo de estudo proposto pela metodologia, sendo que além desta outras técnicas são abordadas com maiores detalhes no decorrer deste trabalho.

2.2.2 Mecanismos de Interação com o Usuário

Como denotado na Figura 2.1, visualizações também podem receber comandos do usuário, através de mecanismos de interação. Esta pode ser no sentido de controlar a quantidade de dados na tela ou de mudar a forma com que os dados são apresentados visualmente. Yi *et al.* (YI et al., 2007) classificam as técnicas de interação mais utilizadas em visualização de informação em 7 categorias, sendo que cada uma delas expressa a vontade do usuário ao realizar determinado comando de interação em um sistema. As mesmas são descritas a seguir.

Técnicas de **seleção** disponibilizam para o usuário formas de marcar os itens que são de seu maior interesse na visualização. Quando muitos elementos são apresentados em uma visualização, ou mesmo quando as representações visuais são modificadas, é difícil para o usuário conseguir identificar e memorizar os itens que lhe despertaram maior atenção. Ao permitir a distinção desses itens de maneira visual, uma visualização possibilita que o usuário siga os itens mais relevantes de uma forma intuitiva. Outra característica das técnicas de seleção é que elas geralmente precedem o uso das técnicas subsequentes, ao invés de atuarem de forma independente.

Técnicas de **exploração** permitem aos usuários examinar os diferentes subconjuntos dos dados apresentados. Devido à combinação de limitação do tamanho das telas, grande escala do conjunto de dados e características da cognição humana, os usuários de sistemas de visualização de informação conseguem ver apenas um numero limitado de itens de uma só vez. Para solucionar estas limitações, eles tipicamente utilizam técnicas de exploração, examinando um subconjunto dos dados apresentados para ganhar conhecimento sobre os mesmos, e depois modificando a visualização para ver outros subconjuntos. A técnica mais comum de exploração é o *panning*, que é o movimento da câmera dentro dos limites do espaço de visualização.

Técnicas de **reconfiguração** disponibilizam aos usuários diferentes perspectivas em relação aos dados analisados, mudando o arranjo espacial das representações visuais. Através dessa categoria de técnicas os usuários podem mudar a forma que os itens são dispostos na tela ou o alinhamento dos mesmos, de forma a disponibilizar diferentes perspectivas dos conjuntos de dados. A possibilidade de mudar os atributos apresentados no eixo de um gráfico é um exemplo de técnica de reconfiguração, pois as mudanças nas variáveis a serem examinadas muda os relacionamentos entre os itens e consequentemente sua disposição no espaço de visualização.

Os mecanismos interativos de **codificação** permitem aos usuários alterar a representação visual dos dados, ou seja, sua aparência visual (cor, tamanho e forma). A mudança da forma como os dados são visualizados é outro exemplo de técnica de codificação (*e.g.*, de um *scatterplot* para um diagrama de barras) , sendo que através dela os usuários procuram descobrir novos relacionamentos entre os dados analisados.

As técnicas de **abstração** tem por objetivo prover aos usuários a possibilidade de ajustar o nível de abstração de uma visualização. Este pode variar entre uma visão geral dos dados (*overview*) até a visualização de poucos itens com um nível maior de detalhamento. Uma técnica bastante comum de mudança de abstração é o *zooming*, que muda a escala

de uma representação visual, de forma a apresentar na tela uma maior quantidade de itens com menos detalhe ou focar em um conjunto reduzido de itens, com a apresentação de um maior grau de detalhamento das informações apresentadas para o usuário.

As técnicas de **filtragem** permitem aos usuários mudar o conjunto de dados que está sendo apresentado na visualização, baseadas em algumas condições definidas pelos mesmos. Neste tipo de interação, podem ser especificados intervalos ou condições, para que então apenas os itens que estejam em conformidade com esses critérios sejam apresentados. Os dados que não satisfazem as condições selecionadas não aparecem ou são mostrados de forma diferente, bastando o usuário desligar o filtro para que eles voltem a ser visualizados.

O grupo de técnicas de **conexão** engloba as interações utilizadas para destacar associações e relacionamentos entre itens que já estão sendo representados e mostrar itens escondidos que são relevantes para um determinado item. Quando vários *displays* de visualização são utilizados para mostrar diferentes representações do mesmo conjunto de dados (*e.g.*, uma combinação entre visualização de grafos e *scatterplot*), pode ser difícil identificar os itens visuais que estão relacionados nas duas visualizações. Para resolver esse problema, a técnica de *brushing* (BUJA et al., 1991) é utilizada para destacar a representação de um item selecionado em um determinado *display* nos demais *displays* que estão sendo mostrados para o usuário.

Na área de gerenciamento de redes, o uso de técnicas de visualização de informação interativas ainda é incipiente. Os trabalhos de Mansmann e Vinnik (MANSMANN; VINNIK, 2006), Keim *et al.* (KEIM et al., 2006) e Oberheide *et al.* (OBERHEIDE; GOFF; KARIR, 2006) lidam com tráfego de rede de maneira geral, se levar em consideração as particularidades dos tráfegos de gerenciamento. Isso se reflete também no uso de mecanismos de interação não adaptados a essas particularidades.

Salvador *et al.* (SALVADOR; GRANVILLE, 2008a) propuseram um conjunto de três técnicas de visualização de informação adaptadas para visualizar informações geradas pela aplicação da metodologia de captura e análise de tráfego SNMP proposta pelo IRTF. No entanto, este trabalho apresentou apenas resultados preliminares sobre o uso de técnicas de visualização de informação para o estudo de tráfegos SNMP. Além disso, as visualizações apresentadas disponibilizam poucas possibilidades de interação com usuário, o que em algumas situações dificulta a obtenção de inferências sobre os tráfegos.

O presente trabalho visa dar um passo à frente em relação aos outros esforços existentes na área, mostrando como técnicas de visualização interativas podem levar a um melhor entendimento em relação aos padrões de funcionamento do SNMP. Um conjunto de técnicas de visualização interativas adaptadas ao estudo de tráfegos SNMP é descrito no próximo capítulo.

3 VISUALIZAÇÕES INTERATIVAS PARA O ESTUDO DE TRÁFEGOS SNMP

Neste capítulo é apresentado um conjunto de técnicas de visualização de informação interativas, adaptadas para visualizar os resultados da aplicação de *scripts* de análise criados seguindo a metodologia de captura e análise de tráfego SNMP proposta pelo IRTF. Estas técnicas foram desenvolvidas a partir dos estudos que permearam esta dissertação de mestrado, e constituem parte da contribuição deste trabalho. Todas elas foram implementadas e integradas na ferramenta *Management Traffic Analyzer* (SALVADOR; GRANVILLE, 2008b), que integra em um ambiente Web todos as etapas da metodologia supracitada. Na descrição das mesmas são enfatizados os mecanismos de interação que um operador de rede pode utilizar para ajustar as visualizações, de forma a atender melhor às suas necessidades.

3.1 Topologia de Rede de Gerenciamento

O primeiro passo para a geração de uma topologia de rede de gerenciamento é identificar, dentro do conjunto de mensagens presentes em um tráfego SNMP, os dispositivos que desempenham função de agentes, gerentes, ou ambas. Através da execução de um *script* de análise para separação do tráfego em fluxos (mensagens trocadas entre um par de endereços de origem e destino que pertençam a um relacionamento CG/CR *(Command Generator/Command Responder)* ou a um relacionamento NO/NR *(Notification Originator/Notification Receiver)* (SCHOENWAELDER et al., 2007)), chega-se à coleção de todos os fluxos de mensagem SNMP presentes no tráfego. Nos relacionamentos CG/CR, os endereços fonte agem como gerentes, enquanto os endereços destino podem ser considerados agentes. Por outro lado, nos relacionamentos NO/NR os endereços fontes são os agentes, enquanto os endereços destinos atuam como gerentes.

A próxima etapa é apresentar visualmente agentes, gerentes, e os relacionamentos existentes entre eles. Para tanto, pode-se utilizar um grafo como abstração visual, sendo que os dispositivos correspondem aos nodos do grafo, e as arestas mapeiam os fluxos de mensagens existentes entre os nodos.

Na visualização proposta, os agentes e gerentes foram representados por círculos, sendo que os representativos dos gerentes possuem maior raio. Existem nodos que atuam como gerentes e agentes, sendo estes representados por círculos de maior raio em relação aos supracitados. A cor dos nodos varia entre tons de azul (elementos com menor carga de tráfego) e vermelho (elementos com maior carga de tráfego). Quando um determinado nodo é focado pelo mouse, todos os elementos relacionados a ele são destacados, para facilitar a visualização de seus vizinhos na topologia. Este destaque é dado através da

mudança gradual da cor dos mesmos para amarelo. As arestas do grafo representam a troca de informação entre gerentes e agentes. A cor da aresta foi utilizada para diferenciar a carga de tráfego dos vários relacionamentos entre gerentes e agentes, variando entre verde (tráfegos menores) e azul (tráfegos maiores).

Para representar estes elementos na visualização, foi utilizado um algoritmo radial para exibição de grafos. Este dispõe os nodos em círculos concêntricos em relação a um nodo central. Quando a visualização inicia, todos os nodos que atuam como gerentes em algum fluxo de mensagens são posicionados na circunferência mais próxima do nodo central, este um nodo fictício (em relação a topologia de gerenciamento) introduzido apenas para organizar o *layout* inicial do grafo. Assim, todos os nodos conectados a este nodo central invisível são gerentes. Esta é a disposição mostrada na Figura 3.1.

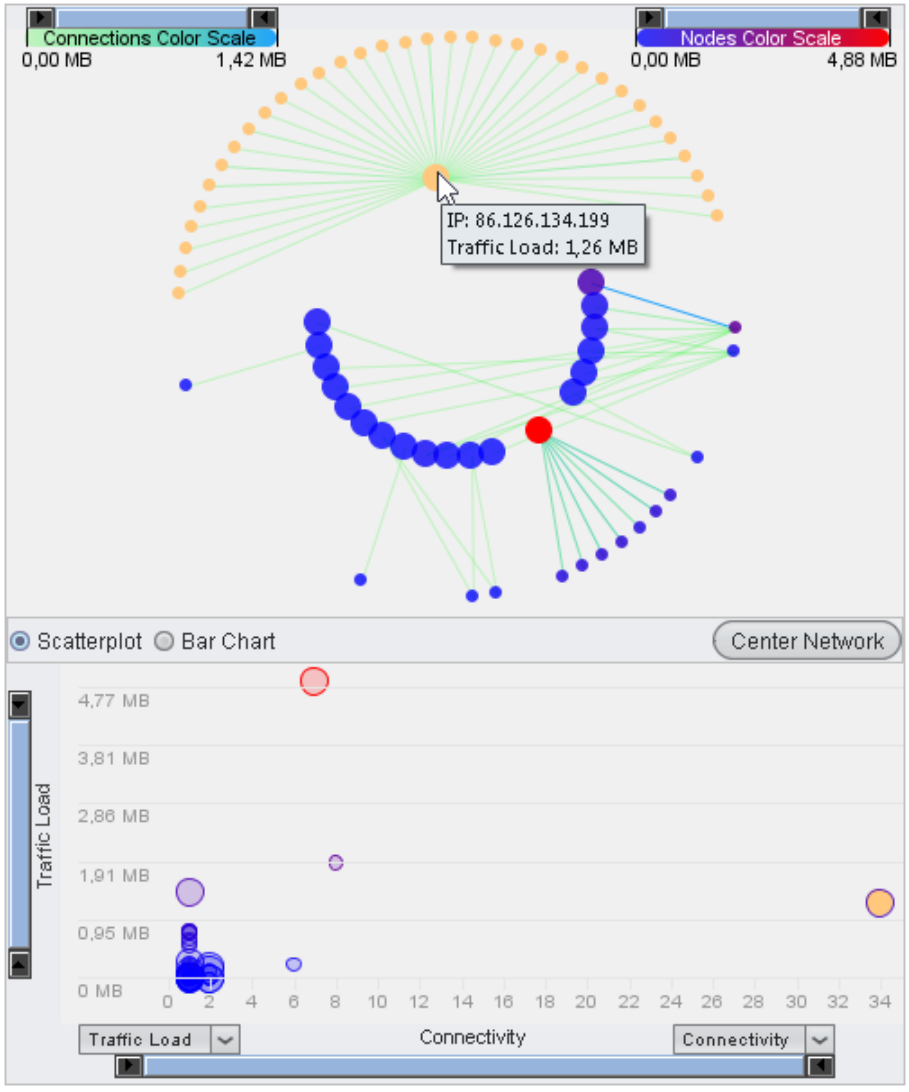

Figura 3.1: Topologia de Rede de Gerenciamento

A visualização provê um mecanismo de interação que permite mudar o nodo central de acordo com comandos do usuário. Nodos gerentes ou agentes podem ser centralizados no espaço de visualização através de um clique do mouse, operação que permite uma melhor compreensão do papel que uma determinada entidade exerce na rede de gerenciamento. A Figura 3.2 mostra um exemplo de tal interação, onde um nodo agente é centralizado e todos os gerentes que possuem relacionamentos com ele aparecem mais próximos.

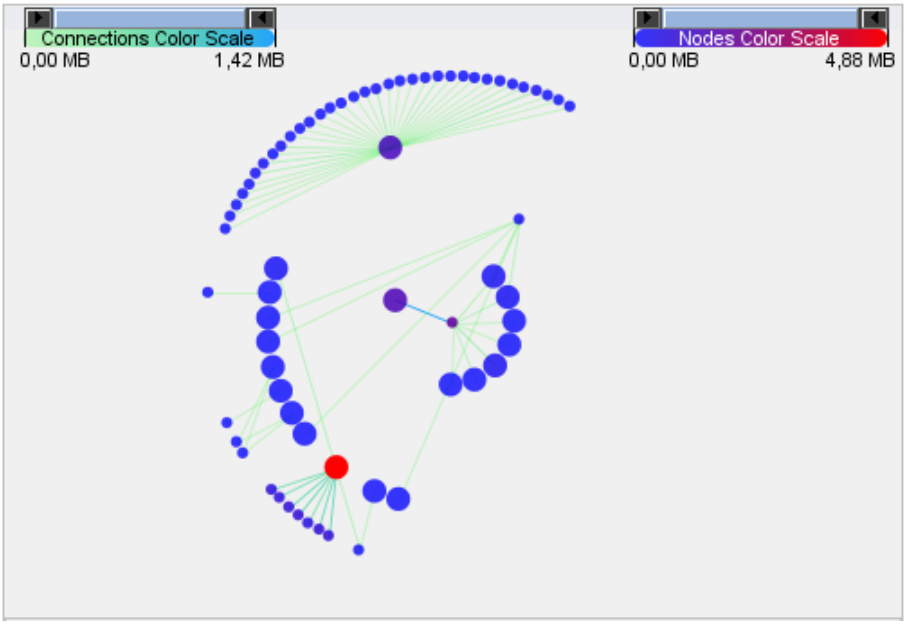

Figura 3.2: Exemplo de Centralização de Agente

Como mecanismos de interação implementados também pode-se citar o uso de *tooltips* (legendas que aparecem quando o mouse é posto em cima de um elemento visual) nos nodos e vértices (no primeiro caso informando o IP e carga de tráfego dos terminais e no segundo informando o tráfego total correspondente ao relacionamento em Bytes e qual o tipo de relacionamento); mecanismos de *zooming* e *panning* da visualização; possibilidade de mover os nodos pelo espaço da visualização, de forma a permitir ao usuário modificar a disposição proposta pelo algoritmo de *layout*; e um botão colocado na parte inferior da visualização, que reorganiza a rede para o seu estado inicial, depois de possíveis interações do usuário.

Acima da visualização localizam-se dois filtros, responsáveis por formar novas topologias de rede de acordo com o interesse do operador. Um deles modifica a topologia de acordo com o tamanho de suas conexões, e a outra de acordo com a carga de tráfego dos nodos, apresentando novos arranjos de acordo com novos valores definidos. Essa possibilidade é interessante para que o usuário tenha a possibilidade de focalizar sua análise apenas nos nodos e conexões que seguem as restrições do filtro.

Para facilitar a visualização de algumas nuances da topologia de rede de gerenciamento, foi implementada uma visualização complementar, que pode ser alternada entre um *scatterplot* e um histograma de barras. As duas visualizações tem a capacidade de interagir uma com a outra, fazendo uso de uma técnica bem difundida em visualização de informação para a visualização de dados multidimensionais (como é o caso da topologia), denominada "*brushing*" (BUJA et al., 1991). Exemplos do uso desta técnica nas visualizações é o destaque dos nodos focados pelo mouse nas duas visualizações, e a possibilidade de centralizar um nodo na topologia através de um comando aplicado na visualização inferior.

No *scatterplot* são plotados os gerentes e agentes da topologia, com a mesma cor e tamanho relativo que possuem na mesma. Os parâmetros dos eixos podem ser alterados de forma dinâmica, possibilitando qualquer combinação entre os parâmetros carga de tráfego, conectividade e ordenação de tráfego (que denota de forma ordenada o tráfego recebido por cada nodo). Existem filtros localizados ao lado dos eixos da visualização que

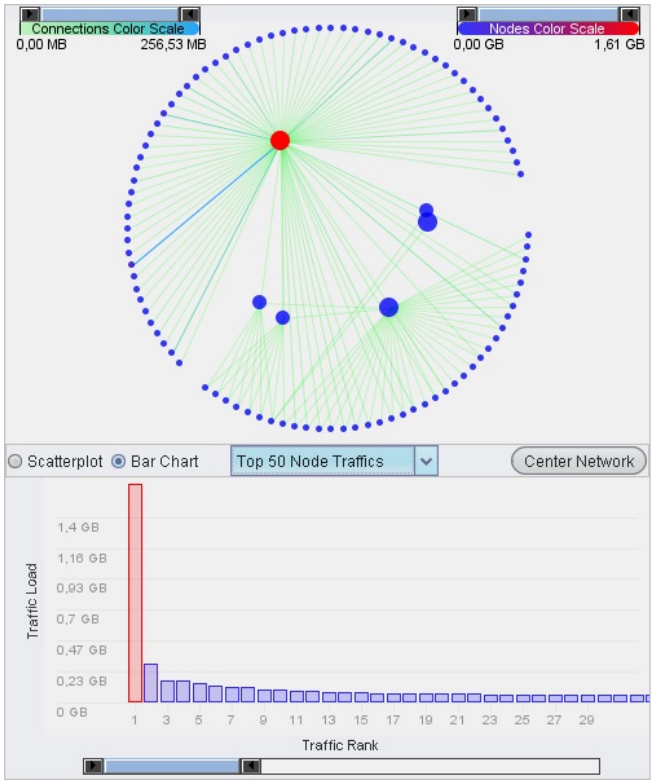

Figura 3.3: Histograma de Barras como Visualização Complementar

possibilitam que o domínio (eixo x) e contradomínio (eixo y) da mesma sejam alterados, de acordo com o interesse do operador. Já o histograma de barras (exibido na Figura 3.3) mostra os top-N elementos da rede com maior carga de tráfego, para facilitar possíveis análises com relação a proporção do tráfego gerado por agentes e gerentes, por exemplo. A quantidade de dispositivos visualizada pode ser regulada por um filtro localizado abaixo da visualização.

3.2 Visualização de Número de Mensagens SNMP por Período

Uma das possíveis análises a ser feita em tráfegos SNMP é a da quantidade de mensagens trocada entre gerentes e agentes em um determinado período. Esse tipo de análise é útil para se identificar o comportamento da quantidade dos diversos tipos de mensagens de gerenciamento trocadas na rede ao longo de um dia, e pode ser um bom ponto de partida para responder algumas perguntas levantadas na metodologia do IRTF, como a relação existente entre tráfego periódico e aperiódico e se as notificações do SNMP levam a mudanças no padrão de *polling* das estações de gerenciamento.

Uma abordagem eficiente para visualizar os resultados desse tipo de análise é utilizar um histograma de barras, onde o tamanho de cada barra corresponde ao número de mensagens trocadas durante uma janela de tempo do tráfego. As barras são seccionadas, sendo que cada secção corresponde aos tipos de mensagem ou versões do SNMP, de acordo com a escolha do usuário. Existem legendas na parte inferior da visualização que identificam cada divisão de acordo, respectivamente, com as mensagens ou versões do SNMP representados.

A visualização inicial mostra todo o período de análise, disponibilizando uma visão geral a respeito das mensagens trocadas no tráfego. O período pode ser representado por

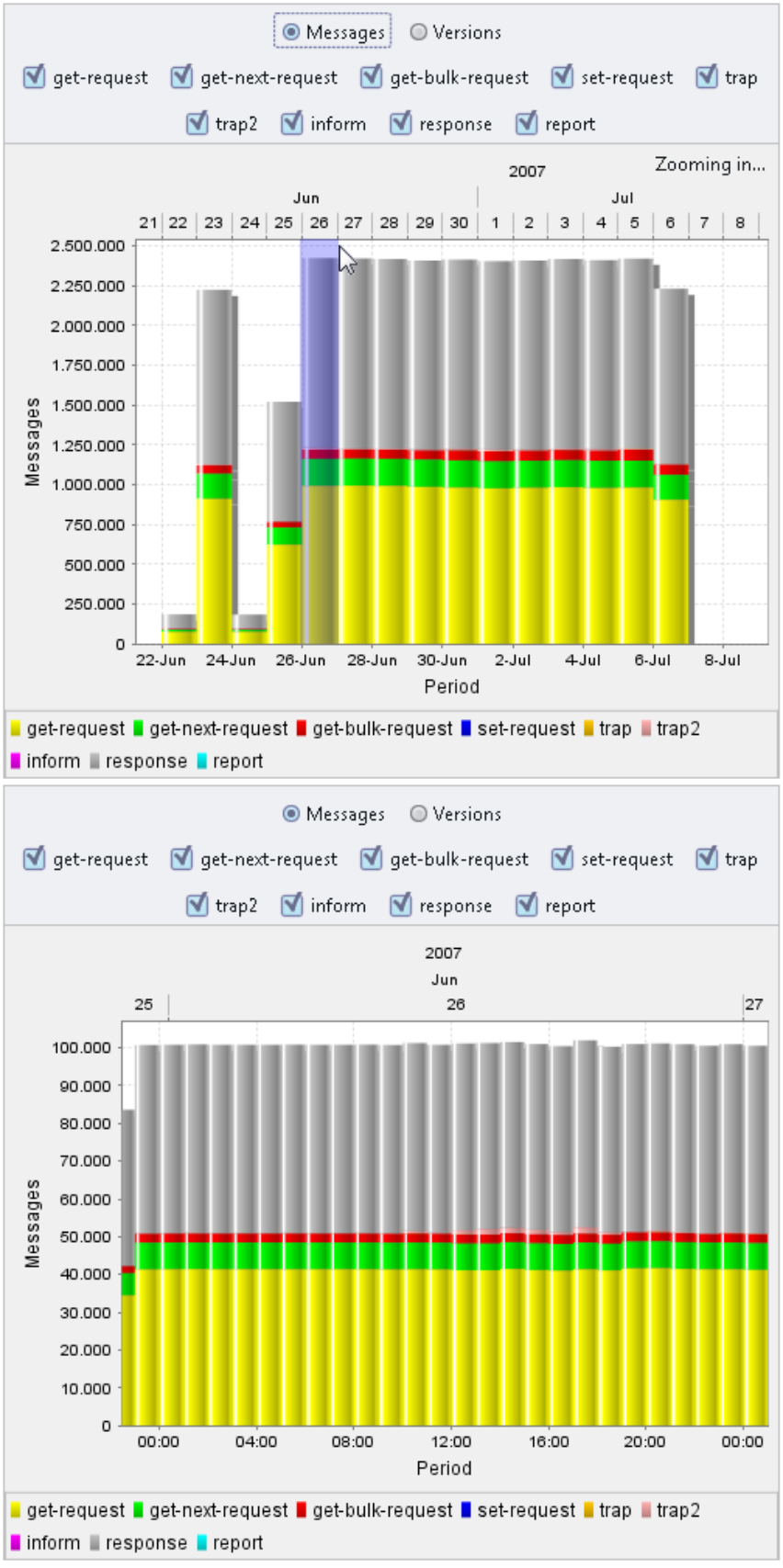

Figura 3.4: Mensagens por Período: exemplo de operação de zoom

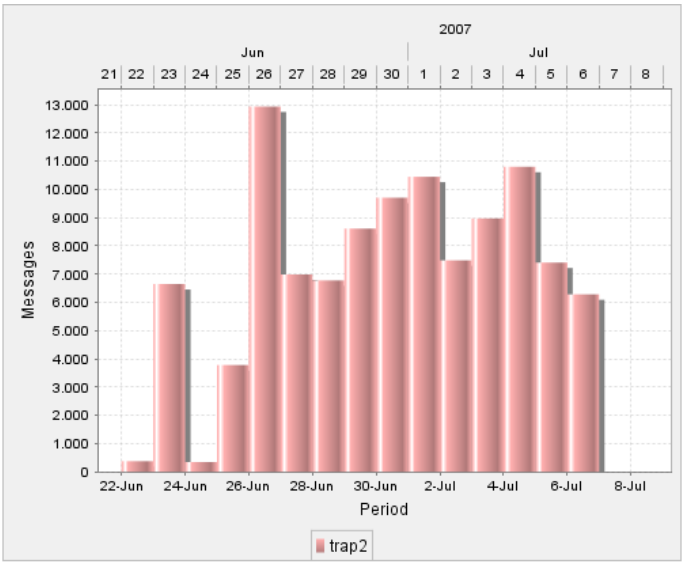

Figura 3.5: Operações trap2

horas, dias, meses ou anos, dependendo da duração da captura. O operador pode interagir com a visualização selecionando subintervalos do tráfego através do mouse. Este mecanismo de interação dispara uma operação de *zooming* semântico que adapta o conjunto de dados visualizado de acordo com o período selecionado. Esta operação é denotada na Figura 3.4, onde o dia 26 de junho de 2007 de um determinado tráfego capturado é selecionado através do *zooming*, o que resulta na exibição do conjunto de horas correspondente a este dia. Vale mencionar que a ocorrência de operações do tipo **response** não é diferenciada por corresponder a uma determinada operação de requisição (get, getnext, getbulk, etc.). Por conseguinte, todas as operações **response** são denotadas pela mesma secção no gráfico.

Nos tráfegos SNMP, algumas mensagens costumam aparecer com frequência muito pequena em relação às demais. Em alguns casos, este fato impedia a visualização de tais mensagens nas barras. Esta situação é mostrada na Figura 3.5, onde as operações do tipo **trap2** presentes no tráfego são mostradas de maneira solitária. Pode-se observar claramente qual o padrão de troca deste tipo de mensagem após a operação de filtro, o que não é possível ao observar-se apenas a visão geral da troca de mensagens mostrada na Figura 3.4. Além disso, a possibilidade de visualizar apenas certas operações ou versões do SNMP faz com que novas inferências à respeito do tráfego possam ser conseguidas, em comparação à visualização de todas as mensagens de uma vez. Para lidar com esses requisitos, foram implementados filtros capazes de mudar a visualização através da seleção de quais operações ou versões do protocolo devem ser mostradas. Ademais, para visualizar a quantidade de mensagens correspondente a uma determinada secção do gráfico, *tooltips* aparecem quando uma barra é focada pelo mouse.

3.3 Visualização de Árvore de Objetos SNMP

Outra análise que pode ser feita nos tráfegos do SNMP é o cálculo do número de vezes em que cada um dos objetos está presente em um tráfego. Através desta análise, é possível elaborar uma série de estatísticas sobre os objetos SNMP presentes no tráfego, como o conjunto de objetos mais acessados, os menos acessados, as MIBs mais importantes, etc.

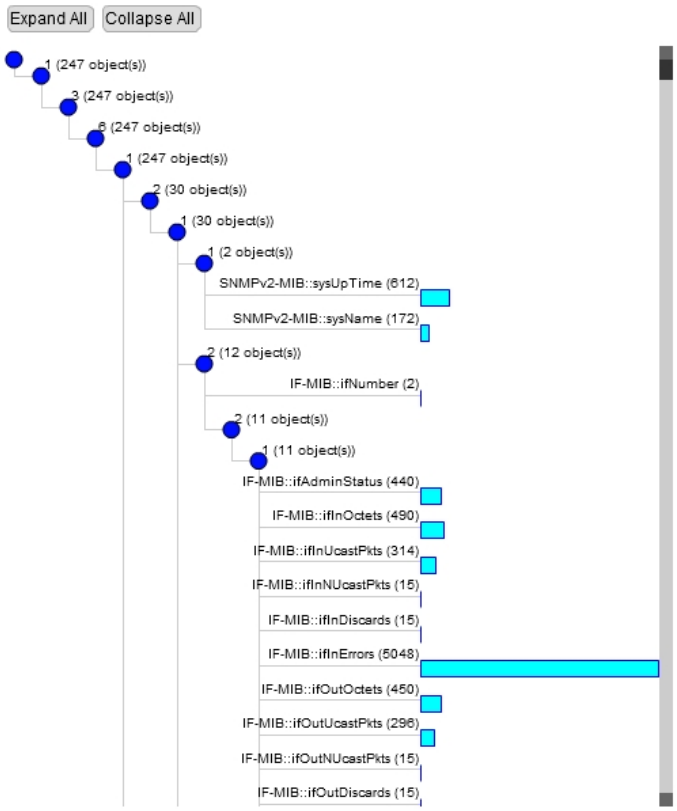

Figura 3.6: Visualização da Árvore de Objetos SNMP

Uma vez que os objetos SNMP são organizados em uma árvore conhecida como *MIB Tree*, é desejável que o resultado desse tipo de análise também apresente o conjunto de objetos encontrados no tráfego nesse tipo de estrutura.

A visualização proposta utiliza um algoritmo de *layout* de árvore identada, onde cada nodo não-folha corresponde a um dos diretórios de uma MIB, e é representado visualmente por um círculo. As folhas da árvore, que correspondem aos objetos SNMP, foram representadas por barras, com o tamanho de cada barra sendo proporcional a sua quantidade no tráfego analisado. Isso é feito de forma que o conjunto de folhas da árvore forma um histograma, com o conjunto de barras disposto de maneira horizontal. Com a combinação dessas duas técnicas de visualização, foi possível representar tanto a hierarquia de objetos SNMP quanto a incidência de cada objeto no tráfego. O resultado desta abordagem pode ser visualizado na Figura 3.6.

Ao lado dos nodos da árvore são apresentados legendas, com informações úteis para a navegação. Se o nodo for folha, é apresentado o nome do objeto e o número de vezes que este foi encontrado. Caso contrário, é apresentada a parte do número OID correspondente aquele determinado nodo, que atua então como um diretório contenedor de outros diretórios ou de objetos.

Para a navegação da árvore, é utilizado um mecanismo de interação para mostrar ou esconder os nodos da árvore, de acordo com cliques de mouse executados pelo usuário, de forma a que este visualize apenas as MIBs sobre as quais possui interesse. Transições animadas são utilizadas para este processo. Acima da visualização existem botões para expandir ou esconder todos os nodos da árvore, úteis quando se deseja ter uma visão global dos objetos. Por fim, é disponibilizada uma barra de arraste vertical, para mostrar os objetos que eventualmente não sejam desenhados no espaço de visualização.

3.4 Visualização do Relacionamento entre Objetos SNMP

Por definição, no SNMP uma operação pode carregar um ou mais objetos em uma determinada operação. No entanto, pouco se sabe sobre quais agrupamentos de objetos costumam aparecer com maior frequência dentro de uma mesma operação, ou mesmo quais objetos são usualmente requisitados de maneira solitária. O esclarecimento dessa questão ajudaria a estabelecer padrões de interação do SNMP mais realísticos do que os utilizados atualmente no estudo do protocolo.

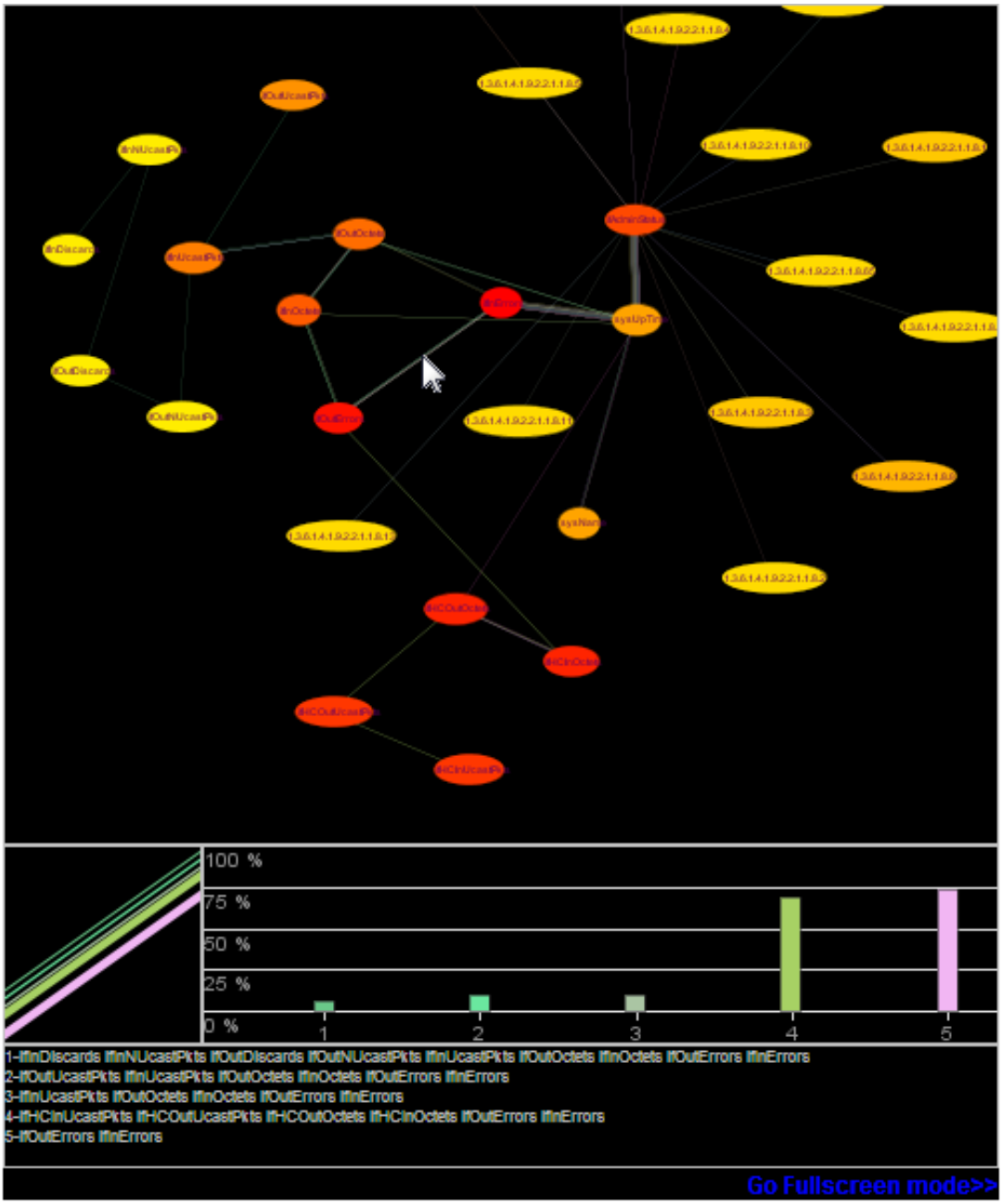

Figura 3.7: Visualização do Relacionamento entre Objetos SNMP

Uma dificuldade inicial para isso é a quantidade de conjunto de objetos a ser visualizado em cada tráfego, pois o número de objetos N pode ser potencialmente muito grande, e o número de agrupamento de objetos cresce de maneira exponencial, seguindo a fórmula 2^N. Para um tráfego com apenas 20 objetos presentes, seria necessário visualizar

1.048.576 conjuntos, o que tornaria o estudo inviável. No entanto, através do uso de técnicas de mineração de dados pode-se restringir o número de conjuntos de objetos a ser analisado, para que se observe apenas aqueles com maior incidência, por exemplo.

Uma das abordagens possíveis é o algoritmo Apriori (AGRAWAL; SRIKANT, 1994), geralmente utilizado para encontrar regularidades nos padrões de compra em supermercados, lojas online e outros, em um processo chamado de *Market Basket Analysis*. Posteriormente esta abordagem foi estendida para o estudo de vários outros domínios em que o relacionamento entre objetos pode prover conhecimento útil, como medicina clínica, dinâmica de fluidos, astrofísica, prevenção de crimes, e combate ao terrorismo (CEGLAR; RODDICK, 2006).

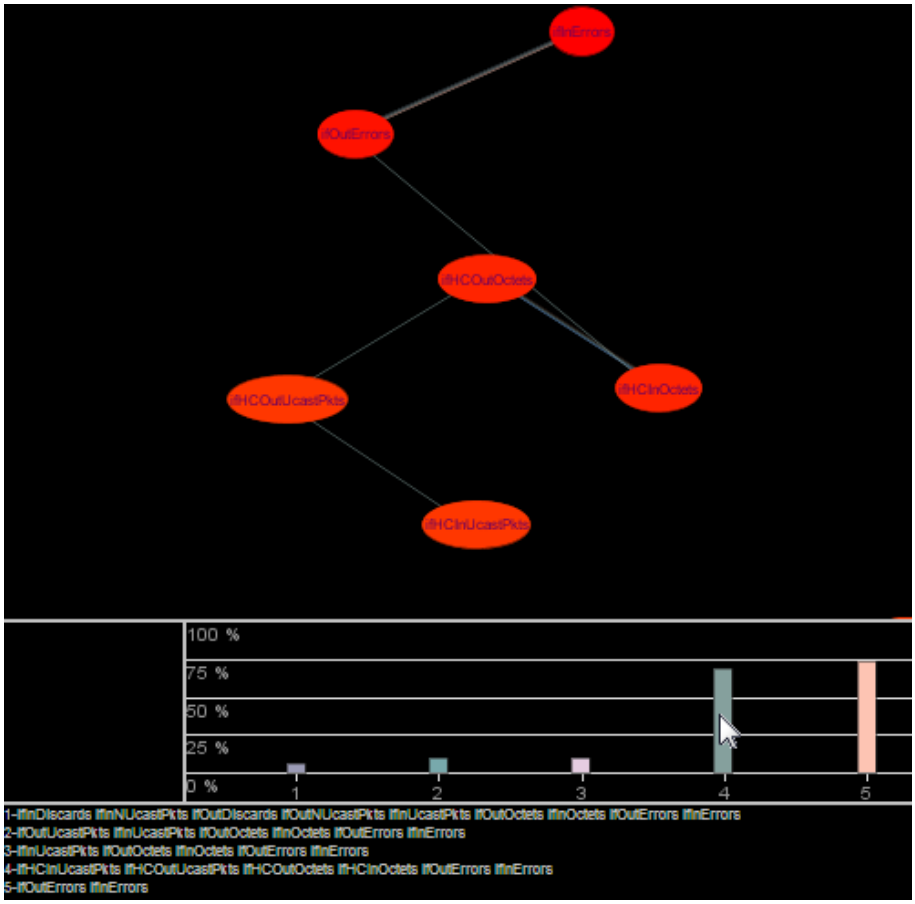

Figura 3.8: *Brushing* entre displays

Depois de encontrados os conjuntos de objetos de maior interesse através da aplicação do algoritmo Apriori, os mesmos são apresentados em uma visualização que representa cada um dos objetos e seus relacionamentos. As abstrações visuais utilizadas para denotar os objetos são elipses, enquanto os seus relacionamentos são representados por linhas que os conectam. Podem haver até N linhas conectando dois objetos, sendo que N é igual ao número de conjuntos de mensagens nos quais esses objetos aparecem juntos. A cor das elipses representa a frequência que um objeto é visto em todos os conjuntos de objetos, e varia entre tons de amarelo (frequência menor) e vermelho (frequência maior). Já a cor de uma linha identifica cada conjunto de objetos que foi encontrado nas amostras de tráfego. Por exemplo, se três objetos SNMP são conectados por linhas de mesma cor, significa que estes objetos foram transportados dentro de uma mesma mensagem ao menos uma vez. A grossura das linhas representa a frequência que um conjunto de objetos é visto

em todo o tráfego, sendo que as linhas mais grossas representam os conjuntos de objetos mais vistos no tráfego. O resultado da visualização proposta é mostrado na Figura 3.7. Os objetos **ifDescr, ifAdminStatus, ifPhysAddress, ifType** e **ifName** são conectados por linhas mais grossas que os demais, o que indica que eles aparecem juntos em mensagens SNMP com mais frequência do que os outros objetos visualizados.

Na visualização proposta, os elementos visuais são dispostos através da aplicação de um algoritmo de *layout* baseado em forças, no qual os objetos que possuem maior afinidade tendem a aparecer mais próximos, enquanto os que tem menor afinidade ou mesmo não aparecem juntos em nenhuma mensagem tendem a repelir uns aos outros. Por sua vez, os relacionamentos são molas, que são comprimidas ou distendidas de acordo com a proximidade entre os dois objetos que estão ligando. O usuário pode interagir na visualização do relacionamento entre objetos SNMP através de *zooming* e *panning*. Quando um objeto é focalizado, *tooltips* mostram a frequência em que ele é visto no tráfego, e os objetos que não possuem nenhum tipo de relacionamento com ele são filtrados da visualização, para facilitar inferências sobre a vizinhança do objeto.

Para facilitar a visualização dos conjuntos de objetos SNMP, uma visualização complementar foi implementada. Ela representa qualquer relacionamento entre dois objetos SNMP selecionado, mapeando os conjuntos representados pelas linhas para um diagrama de barras. Caso um conjunto seja selecionando no diagrama, a visualização da proximidade de objetos passa a mostrar apenas os objetos pertencentes àquele conjunto, em mais um exemplo de uso de técnica de "*brushing*". Essa é a possibilidade de interação ilustrada na Figura 3.8. Abaixo da visualização complementar aparecem legendas, onde pode-se visualizar cada um dos conjuntos que está sendo representado.

4 IMPLEMENTAÇÃO

Neste capítulo são descritos detalhes de implementação dos protótipos de visualização de informação apresentados no capítulo anterior. A arquitetura da ferramenta *Management Traffic Analyzer* é revisada brevemente, para denotar os requisitos necessários à implementação das visualizações. Em seguida, as APIs de visualização de informação utilizadas, bem como os *scripts* de análise e os principais componentes dos protótipos de visualização implementados, são apresentados.

4.1 Arquitetura do *Management Traffic Analyzer*

Salvador et al. propuseram uma ferramenta que automatiza o processo de execução da metodologia de medições sobre tráfegos SNMP, integrando todos os passos da mesma em uma ferramenta Web chamada *Management Traffic Analyzer* (SALVADOR; GRANVILLE, 2008a). A arquitetura desta ferramenta é brevemente revisada na Figura 4.1.

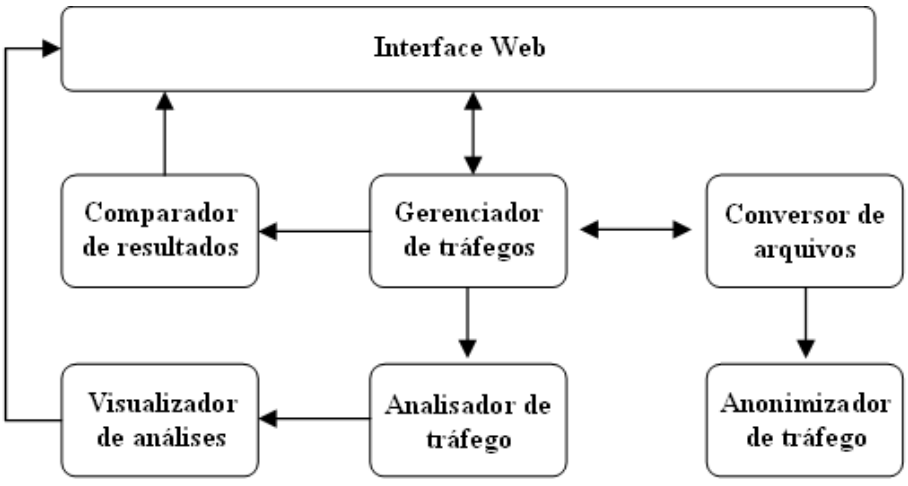

Figura 4.1: Arquitetura da ferramenta *Management Traffic Analyzer*

O módulo **analisador de tráfego** compreende à execução de *scripts* de análise para extrair e agregar informações sobre amostras de tráfego SNMP. Os dados resultantes das análises são armazenados em tabelas de uma base de dados MySQL, para serem utilizados posteriormente em visualizações implementadas no módulo **visualizador de análises**. As técnicas de visualização devem ser desenvolvidas de forma a recuperar os dados resultantes de uma análise diretamente do banco de dados, processar esses dados e exibir a visualização. Para dinamizar o processo de criação da visualizações propostas nesta dissertação, APIs de visualização de informação foram utilizadas na implementação dos

protótipos. Estas concentram interfaces para funções típicas utilizadas para construção de visualizações e acesso a bases de dados, evitando o esforço de ter que programá-las do início. As API utilizadas neste trabalho são apresentadas na próxima seção.

4.2 APIs Web de Visualização de Informação

Dentre as APIs de visualização de informação disponíveis na Internet, foi escolhido um subconjunto que atendesse os requisitos de integração com a ferramenta *Management Traffic Analyzer*. Como requisitos que permearam esta seleção, pode-se destacar a possibilidade de integração das visualizações com páginas Web (HTML), suporte ao acesso a base de dados relacionais e código-fonte aberto. As APIs selecionadas são descritas nas subseções seguintes.

4.2.1 prefuse

O prefuse (HEER; CARD; LANDAY, 2005) é uma API baseada em Java de livre uso, que utiliza Java 2D para tornar simples tarefas complicadas na implementação de visualizações, como renderizar grafos de maneira visualmente agradável e animada, permitindo vários tipos de interação com o usuário. Para tanto, a API provê estruturas específicas para manipulação de tabelas, grafos e árvores. As tabelas possuem métodos de consulta por campo, similar a de uma consulta a sistemas de banco de dados. Os grafos e árvores possuem diversos algoritmos de *layout* disponíveis para utilização, de forma a tornar sua exibição mais compreensível para o usuário, de acordo com a aplicação.

Outra facilidade provida pelo prefuse é o suporte integrado à leitura de arquivos formatados, como CSV (*Comma Separated Value*), XML (*eXtendible Markup Language*) e GraphML (*Graph Modeling Language*), uma formato baseado em XML para a representação de grafos. Outro destaque vai para as bibliotecas de *display* e animações, que provêem uma interface simples para a criação de visualizações com um conjunto significativo de possibilidades de interação. Abaixo estão listados os principais pacotes que a API disponibiliza:

- **prefuse** - contém as classes Visualization e Display, que representam respectivamente instâncias de abstrações visuais e visualizações (*views*);
- **prefuse.data** - disponibiliza estruturas para construção de tabelas, grafos e árvores;
- **prefuse.data.io** - classes de entrada/saída para arquivos de dados;
- **prefuse.data.io.sql** - conectividade com base de dados que utilizam linguagem SQL;
- **prefuse.action** - módulo para a criação de animações baseadas em operações de filtro, *layout*, cor, forma e tamanho;
- **prefuse.visual** - representa instâncias de itens visuais;
- **prefuse.render** - módulos de renderização para o desenho de itens visuais;
- **prefuse.control** - provê controles interativos para a manipulação de itens visuais e operações de *zooming* e *panning*;
- **prefuse.data.query** - filtra dados a partir de comandos do usuário.

4.2.2 JFreeChart

O JFreeChart (JFREECHART, 2010) é uma API específica para a criação de gráficos, baseada em Java. Ela pode ser utilizada para gerar gráficos de pizza, gráficos de barra, gráficos de linha, gráficos combinados, dentre outros. Algumas das principais funcionalidades do JFreeChart incluem: suporte à exportação para os formatos de imagem PNG e JPEG; suporte à exportação para os formatos PDF e SVG; possibilidade de inclusão de *tooltips* nos gráficos; *zooming* interativo; possibilidade de fazer anotações nos gráficos; e possibilidade de criação de gráficos e eixos customizados.

Os pacotes disponibilizados pela API são:

- **org.jfree.chart** - contém as classes do núcleo da API, como as que definem os tipos de gráficos e a visualização;
- **org.jfree.chart.annotations** - provê um mecanismo para adicionar pequenos textos (anotações) aos gráficos, comumente para destacar um item de dados em específico;
- **org.jfree.chart.axis** - possui classes para definir os eixos de um gráfico. A API permite que se defina mais do que um eixo por dimensão em um mesmo gráfico;
- **org.jfree.chart.labels** - gerar rótulos para itens em um gráfico;
- **org.jfree.chart.renderer** - classes utilizadas para a implementação dos renderizadores dos gráficos;
- **org.jfree.data** - contém as classes que representam os conjuntos de dados na API;
- **org.jfree.data.jdbc** - provê uma interface para leitura de uma base de dados utilizando JDBC (*Java Database Connectivity*);
- **org.jfree.data.xml** - classes para a leitura de conjunto de dados a partir de arquivos XML.

4.2.3 flare

O flare (FLARE, 2010) é uma coleção de classes do ActionScript 3.0 voltadas para a construção de visualizações interativas. A API pode ser utilizada para a criação de vários tipos de gráfico, animações complexas, diagramas de rede, e outros. Através do flare pode-se construir visualizações interativas acessíveis pela Web através do Macromedia Flash Player.

A API é composta por diversas bibliotecas, dentre elas:

- **flare.data** - provê classes para a importação de conjuntos de dados externos à aplicação, como arquivos formatados;
- **flare.display** - provê classes para mostrar as visualizações, que automaticamente se atualizam;
- **flare.physics** - provê classes para simulações físicas;
- **flare.vis** - pacote para a criação de visualizações interativas;
- **flare.animate** - provê classes para a criação de animações.

4.3 *Scripts* de Análise

Para a aplicação de técnicas de visualização ao estudo de tráfegos SNMP, foi utilizado o resultado da execução de alguns *scripts* de análise, que procuram agregar os dados dos tráfegos de forma a permitir a identificação de predominâncias e tendências na utilização do protocolo. São eles:

- **snmp_flows** - Os tráfegos capturados podem conter mensagens SNMP trocadas entre várias terminações de linha da rede. Uma maneira de fazer uma separação destes tráfegos em entidades mais gerenciáveis é separar as mensagens em fluxos. Um fluxo de mensagem SNMP é definido como todas as mensagens trocadas entre um par de endereços de origem e destino que pertençam a um relacionamento CG/CR *(Command Generator/Command Responder)* ou a um relacionamento NO/NR *(Notification Originator/Notification Receiver)* (SCHOENWAELDER et al., 2007).

- **messages_per_hour** - Uma forma de estudar a distribuição das mensagens em função do tempo é computar o número de vezes que as mesmas aparecem em intervalos de 1 hora. Com essa abordagem pode-se verificar padrões de trocas de mensagem, e possíveis anomalias que tenham ocorrido durante o período da captura, denotadas por modificação abrupta do número de mensagens trocadas em uma determinada hora. Para uma análise mais eficiente dos fluxos, as mensagens são classificadas de acordo com o tipo e versão do SNMP.

- **snmp_objects** - O cômputo de quais objetos SNMP estão em um determinado tráfego é útil para esclarecer dúvidas sobre quais os objetos mais utilizados, quais as MIBs mais utilizadas, a proporção de MIBs proprietárias no tráfego, além do uso de objetos considerados obsoletos.

- **snmp_objects_proximity** - Mensagens SNMP podem carregar vários objetos, mas pouco se sabe sobre quais objetos costumam aparecer com maior frequência nas mesmas mensagens. Essa informação é útil para que se possa inferir otimizações na utilização do protocolo.

Análise	**Visualização**
snmp_flows	Topologia de Rede de Gerenciamento
messages_per_hour	Visualização de Número de Mensagens SNMP por Período
snmp_objects	Visualização de Árvore de Objetos SNMP
snmp_objects_proximity	Visualização do Relacionamento entre Objetos SNMP

Tabela 4.1: Relação entre Análises e Visualizações

Os dados gerados por tais *scripts* serviram como base para a implementação das quatro técnicas de visualização apresentadas. A Tabela 4.1 mostra o relacionamento entre *scripts* e visualizações. A implementação dos protótipos de visualização será descrita a seguir.

4.4 Protótipos Implementados

Como mencionado anteriormente, as APIs de visualização de informação apresentadas foram utilizadas para a construção dos protótipos de visualização de tráfego SNMP.

A relação entre as APIs de visualização de informação e os protótipos implementados é mostrada na Tabela 4.2. A Visualização de Árvore de Objetos SNMP foi implementada utilizando a linguagem Actionscript 3.0 do Macromedia Flash. Já as outras visualizações foram implementadas como *applets* Java.

Protótipo	**API**
Visualização de Topologia de Rede de Gerenciamento	prefuse
Visualização de Número de Mensagens SNMP por Período	JFreeChart
Visualização de Árvore de Objetos SNMP	flare
Visualização do Relacionamento entre Objetos SNMP	prefuse

Tabela 4.2: Protótipos Implementados

Os protótipos de visualização foram implementados de forma modular, para assegurar um baixo acoplamento e facilitar a implementação de novas visualizações. A descrição desses módulos e do papel que cada API desempenhou na construção dos mesmos é mostrada nas próximas subseções.

4.4.1 Conexão com bases de dados

A ferramenta *Management Traffic Analyzer* armazena o resultado das análises realizadas sobre tráfegos SNMP em uma base de dados MySQL. Para que o resultado das análises pudesse ser visualizado, componentes responsáveis pela conexão com esse banco de dados tiveram que ser implementados. Como as visualizações foram programadas em duas tecnologias diferentes (Java e Flash), duas abordagens de acesso aos dados tiveram que ser utilizadas.

A primeira abordagem, utilizada pelas visualizações implementadas em Java, faz uso do modelo de comunicação entre *applets* e *servlets* dessa linguagem. Este modelo é ilustrado na Figura 4.2. A consulta SQL é enviada através da classe DatabaseDataSource do *applet* para o *servlet*, que se encarrega de comunicar-se com a base de dados e retornar o resultado da consulta para o protótipo de visualização.

O resultado das consultas é tratado de maneira distinta nos protótipos. Como o prefuse disponibiliza classes específicas para a aquisição dos dados, as tabelas retornadas pelo *servlet* puderam ser mapeadas diretamente para estruturas internas da API. Isso tornou a implementação do módulo de acesso a dados das Visualizações de Topologia de Rede de Gerenciamento e Proximidade entre Objetos mais simples. Já no caso da Visualização de Número de Mensagens SNMP por Período, houve um maior trabalho para que os dados fossem adquiridos para visualização. Isto ocorreu porque, apesar de o JFreeChart possuir classes específicas para a conexão com bases de dados, estas são bastante limitadas. No que concerne à leitura dos *Datasets* (estruturas de dados que contêm os valores a serem representados em um gráfico) a partir de uma base de dados, por exemplo, a classe provida (JDBCXYDataset) limita bastante o esquema no qual os conjuntos de dados devem ser representados em um banco de dados. Isto representou um esforço extra na construção das visualizações, ao demandar que a conectividade com o banco de dados tivesse que ser programada diretamente na API Java, e o mapeamento dos resultados para estruturas de dados internas da API também tivesse que ser modelado.

Já a Visualização de Árvore de Objetos SNMP, implementada em Flash, teve que utilizar uma solução diferenciada para a conexão com o banco MySQL. Como o ActionScript 3.0 não provê classes para a conexão com bancos de dados, e a API flare também não oferece nenhuma facilidade para tanto, foi necessário utilizar a biblioteca AMFPHP

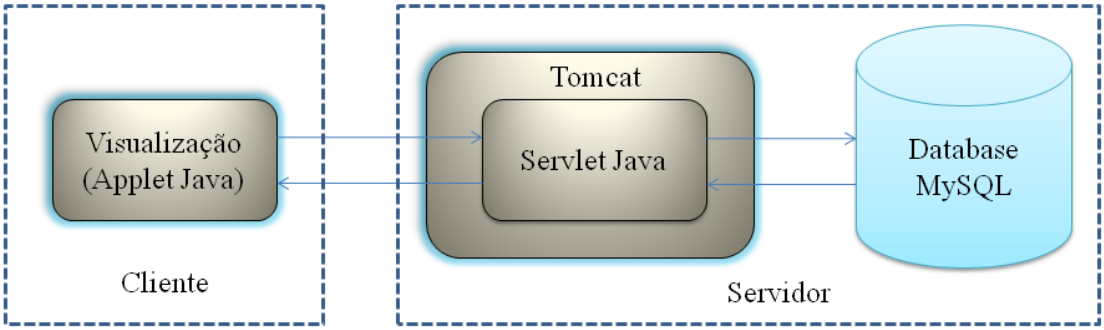

Figura 4.2: Conexão com base de dados das implementações em Java

(AMFPHP, 2008), que faz uma ponte entre os objetos suportados pelo ActionScript e a linguagem PHP. A partir disso, torna-se possível fazer consultas na base de dados através do PHP, sendo que o resultado de tais consultas é retornado para a visualização através de um mapeamento para estruturas de dados nativas do ActionScript. Tal abordagem é mostrada na Figura 4.3.

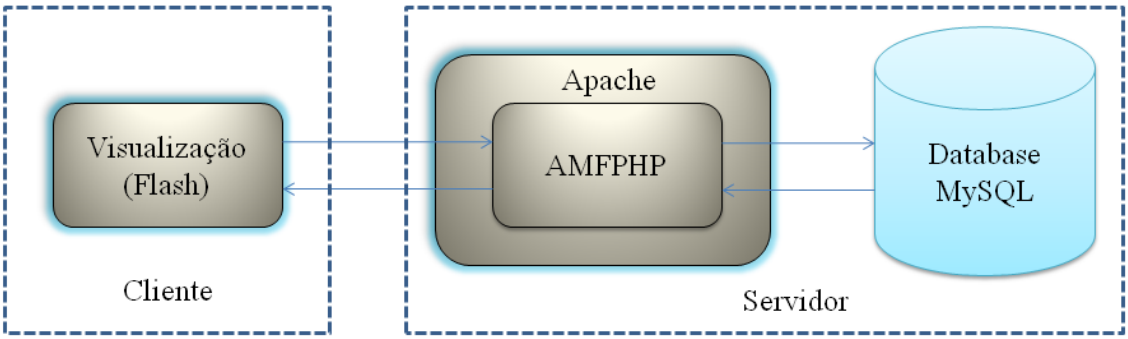

Figura 4.3: Conexão com base de dados da implementação em Flash

4.4.2 Estruturas de dados

Para a construção da Topologia de Rede de Gerenciamento, foi necessário utilizar duas das estruturas providas pela API prefuse, as classes Table e Graph. Ambas ofereceram um conjunto de métodos e classes de apoio satisfatórias para o propósito da visualização. A classe Table, por exemplo, suporta um tipo de consulta similar ao da linguagem SQL para o retorno de dados, o que facilita as leituras feitas nas tabelas. O resultado das consultas à base de dados é armazenado em objetos Table. Este resultado é composto por todos os fluxos de mensagem SNMP presentes no tráfego, conseguidos através da execução do *script* **snmp_flows**. Como já mencionado anteriormente, a partir dos fluxos é montada a topologia de gerenciamento, que é então armazenada em objetos Graph.

Como a Visualização do Relacionamento entre Objetos SNMP utiliza uma abordagem inovadora para a visualização de conjuntos, foi necessário desenvolver classes específicas para o armazenamento dessa estrutura. Da mesma forma que a visualização anterior, o resultado das consultas à base MySQL é armazenado em objetos Table. Este resultado corresponde a todos os conjuntos de objetos vistos em um determinado tráfego, apurados através da execução do *script* **obj_proximity**. Para que os conjuntos pudessem ser mapeados para a abstração visual proposta, foi criada uma nova classe, ObjectProximitySet,

capaz de armazenar todos os objetos presentes em um tráfego e todos os relacionamentos existentes entre os objetos.

No caso da Visualização de Número de Mensagens SNMP por Período, o resultado da consulta à base de dados retorna o número de mensagens SNMP classificadas por tipo de mensagem ou versão do protocolo, resultados da execução do *script* **messages_per_hour**. Neste caso a própria tabela retornada serve para a criação da abstração visual, sem necessidade da criação de objetos intermediários, sendo mapeada para a estrutura TimeTableXYDataset, disponibilizada pela JFreeChart. Essa estrutura apresenta uma boa facilidade de uso, com algumas restrições. Após um valor ser colocado na estrutura, a API não permite que este seja retirado ou substituído, o que complica operações de atualização, por exemplo. Para que estas sejam feitas, é necessário uma chamada ao método *clear()*, que faz a remoção de todos os valores previamente armazenados na estrutura, para que então sejam adicionados novamente todos os valores atualizados, operação que pode se mostrar bastante ineficiente para *datasets* muito grandes.

Já na Visualização de Árvore de Objetos SNMP, o resultado da consulta à base de dados é representado pela quantidade de cada um dos objetos SNMP presentes no tráfego, apurada através do *script* **snmp_objects**. A *MIB Tree* então é montada, através do mapeamento dos OIDs para uma estrutura de árvore, e armazenada na classe Tree, nativa do flare. Esta estrutura também apresenta uma certa inflexibilidade, já que depois de formada, os elementos da árvore (nodos e arestas) não pode ser manipulados, o que dificulta a execução de alguns processos necessários para a recomputação dos *layouts* providos.

4.4.3 Estruturas Visuais

A Visualização de Topologia de Rede de Gerenciamento foi criada com auxílio de algumas classes de renderização providas pelo prefuse. As classes ShapeRenderer e EdgeRenderer foram utilizadas, respectivamente, para a criação dos nodos e arestas da topologia de gerenciamento. Já as visualizações complementares (diagrama de barras e *scatterplot*) foram criadas com as classes AxisRenderer (responsável por gerar os eixos dos gráficos) e AbstractShapeRenderer, que renderiza as barras do gráfico de barras e os círculos do *scatterplot*.

A Visualização do Relacionamento entre Objetos SNMP demandou o desenvolvimento de uma classe específica para a renderização das linhas representativas dos relacionamentos entre objetos. Esta renderiza retas paralelas entre os objetos carregados juntos em mensagens. O numero de retas corresponde ao número de conjuntos onde as mensagens ligadas aparecem juntas. Já os objetos foram renderizados através de uma extensão da classe LabelRenderer disponibilizada pelo prefuse, para que as elipses representativas dos objetos pudessem ser identificadas através de *labels*. Por sua vez, a visualização complementar foi implementada através das classes AxisRenderer e AbstractShapeRenderer, da mesma forma que na visualização apresentada anteriormente.

Todos os elementos visuais da Visualização do Número de Mensagens SNMP por Período são gerados a partir da classe StackedXYBarRenderer. As barras seccionadas, os eixos do gráfico e as legendas das barras são formadas por métodos presentes nesta classe.

Já a Árvore de Objetos SNMP foi renderizada a partir de três classes nativas do flare: NodeSprite, RectSprite e TextSprite. A primeira renderiza os diretórios da MIB, representados por círculos na visualização. Já objetos RectSprite renderizam tanto as arestas da árvore quanto os objetos SNMP. E a classe TextSprite renderiza os *labels* que identificam os diretórios e os objetos.

4.4.4 Mecanismos de Interação

As implementações feitas com o auxílio do prefuse utilizaram alguns controles de interação disponibilizados nativamente pela API. As classes DragControl, NeighborHighlightControl, PanControl e WheelZoomControl foram utilizadas para disponibilizar o arraste dos nodos na visualização, o destaque dos nodos vizinhos quando um nodo é focalizado, e controles de *panning* e *zooming* da visualização, respectivamente. Já a classe TooltipControl teve de ser estendida, para que mais de um campo possa ser mostrado através de *tooltips* quando determinado elemento visual das visualizações é focalizado. Todas as operações de *brushing* tiveram que ser implementadas do início, já que a API não provê suporte nativo para este tipo de interação.

Na Visualização de Topologia de Rede de Gerenciamento, o controle para centralização de um determinado nodo através de seleção com o mouse é feito através da classe TreeRootAction, também disponibilizada pelo prefuse. Já os filtros da visualização tiveram que ser implementados diretamente na API Java.

A Visualização de Número de Mensagens SNMP por Período utilizou uma modificação no mecanismo de *zooming* do JFreeChart. Nativamente, o *zooming* da biblioteca não funciona de maneira semântica, ou seja, não existe a possibilidade de atualizar o conjunto de dados de acordo com o nível de *zooming* aplicado ao gráfico. Para contornar este problema, foi necessário estender a classe ChartPanel (responsável por exibir a visualização na tela) de forma a adicionar a possibilidade de alterar o conjunto de dados de acordo com a operação. Os filtros tiveram que ser programados sem auxílio da API, já que a mesma não dá suporte a este tipo de operação. Já os *tooltips* foram disponibilizados através da classe StandardXYToolTipGenerator, nativa do JFreeChart.

Já a Visualização de Árvore de Objetos SNMP utiliza um mecanismo de interação para mostrar ou esconder os nodos da árvore, provido pela API flare através da classe ExpandControl. No entanto, a API não provê componentes de *scrolling*, o que demandou a programação dos mesmos diretamente em ActionScript.

Após os esforços de implementação descritos no decorrer deste capítulo, os protótipos de visualização foram submetidos a um processo de validação, de forma a mostrar a efetividade do uso destas técnicas no estudo de tráfegos SNMP, e o papel que os mecanismos de interatividade desempenham no processo. Esta avaliação é desenvolvida no próximo capítulo.

5 AVALIAÇÃO

Neste capítulo uma avaliação dos protótipos de visualização de informação apresentados no decorrer deste trabalho é desenvolvida. Esta avaliação segue um modelo aninhado para o projeto e avaliação de visualizações, que divide o processo em quatro fases: caracterização das tarefas e dados no vocabulário do domínio do problema, abstração destas em operações e tipos de dados, projeto de abstrações visuais e técnicas de interação com o usuário e a criação de algoritmos para executar as técnicas de maneira eficiente.

5.1 Modelo Aninhado para Avaliação de Visualizações

O modelo de avaliação de visualizações proposto por Munzner (MUNZNER, 2009) divide o processo de validação de uma técnica de visualização de informação em quatro níveis. O nível mais externo compreende a caracterização dos problemas e dados no domínio particular a que pertencem os usuários. O resultado desta caracterização então é mapeado para operações e tipos de dados abstratos, para que no próximo nível sejam projetadas visualizações e mecanismos de interação capazes de representá-los. Por fim, o nível mais interno corresponde a criar algoritmos para implementar as visualizações e mecanismos de interação de forma eficiente. Estes níveis são aninhados, o que significa que a saída resultante de um nível acima é a entrada para o nível abaixo. Os quatro níveis de avaliação são detalhados a seguir.

5.1.1 Caracterização do Domínio do Problema

No primeiro nível, o projetista da visualização deve aprender sobre as tarefas e dados dos usuários alvo em algum domínio em particular (*e.g.*, o gerenciamento de redes utilizando SNMP). Cada domínio usualmente possui seu próprio vocabulário para descrever seus dados e problemas, e normalmente existe um fluxo de dados que descreve como os dados são utilizados para resolver os problemas.

A saída da caracterização do fluxo de atividades do domínio é um conjunto detalhado de perguntas sobre as ações executadas pelos usuários na coleção heterogênea de dados. Este conjunto pode ser conseguido através de entrevistas com estes usuários, ou de outras formas. No caso do presente trabalho, as questões são retiradas da metodologia de coleta e análise de tráfego SNMP, ou criadas em conformidade com a mesma.

5.1.2 Abstrações de Dados e Operações

O estágio de abstração corresponde a mapear os problemas e dados do vocabulário específico do domínio estudado em uma descrição mais abstrata e genérica, alinhada com o vocabulário de ciência da computação. Em outras palavras, traduzir o domínio do pro-

blema em termos de visualização de informação. A saída deste nível corresponde à descrição de operações e tipos de dados, necessários para servir de entrada para as decisões de abstração visual presentes no próximo nível.

O aspecto principal deste estágio é a transformação dos dados brutos em tipos de dados que técnicas de visualização de informação possam utilizar. O objetivo é encontrar o tipo de dado mais coerente, para que então uma representação visual do mesmo possa ser criada visando resolver o problema. Isto frequentemente requer a representação dos dados brutos em tipos derivados ou formatos diferentes.

5.1.3 Técnica de Visualização e Mecanismos de Interação

O terceiro nível corresponde à análise das técnicas de visualização e mecanismos de interação utilizados para instanciar as abstrações de dados e operações propostas. Uma das possíveis abordagens de validação é a apresentação e discussão qualitativa dos resultados sob forma de imagens estáticas ou vídeos. Tal discussão pode ser baseada na obtenção de *insights* sobre os dados a partir das visualizações geradas.

A obtenção de *insights* é considerada um dos principais propósitos do uso de técnicas de visualização de informação. Apesar de o conceito de *insight* não possuir uma definição amplamente aceita na comunidade de computação gráfica, existem alguns esforços de pesquisa que apresentam avaliações baseadas em *insights*, como os trabalhos de Yi *et al.* (YI et al., 2008), Saraiya *et al.* (SARAIYA; NORTH; DUCA, 2005) (SARAIYA et al., 2006) e North (NORTH, 2006). O uso de avaliações baseadas em *insights* pode mostrar mais claramente como o uso de técnicas de visualização de informação interativas pode ajudar na identificação de tendências e padrões no funcionamento do SNMP.

5.1.4 Projeto do Algoritmo

O nível mais interno do modelo aninhado para avaliação de visualizações é a validação dos algoritmos que levam a efeito as técnicas de visualização e mecanismos de interação propostos. Uma maneira de alcançar este propósito é mostrar que o algoritmo atende aos requisitos de codificação visual e *design* de interação especificados no nível acima. Como mostrado durante o trabalho, todas as visualizações descritas constituem protótipos implementados e funcionais, o que valida os algoritmos utilizados para a codificação das visualizações e mecanismos de interação.

Nos esforços de desenvolvimento das visualizações, foram utilizadas capturas de tráfego coletadas em vários ambientes acadêmicos e de produção ao redor do mundo. Todos os protótipos de visualização foram capazes de apresentar os resultados das análises destes tráfegos de maneira fluida, mantendo tempos de resposta aceitáveis nas mudanças interativas das visualizações. O maior tráfego utilizado no desenvolvimento possuía 247 nodos, uma duração aproximada de 12 dias e 258.010.521 mensagens trocadas. Mesmo neste caso, nenhum problema de escalabilidade nas visualizações foi detectado. Assim, o desempenho dos algoritmos implementados pode ser considerado satisfatório para o domínio a que se destinam.

5.2 Avaliação da Visualização de Topologia de Rede de Gerenciamento

Uma topologia de rede descreve como é o *layout* de uma rede de computadores através da qual há o tráfego de informações, e também como os dispositivos estão conectados à

mesma. Em particular, uma topologia de rede de gerenciamento mostra o relacionamento entre as entidades responsáveis pelo monitoramento e controle dos sistemas de *hardware* e *software* que compõem a rede (gerentes) e os dispositivos monitorados (agentes). O estudo de uma topologia de gerenciamento pode levar ao esclarecimento de dúvidas sobre os papéis que as entidades estão exercendo na rede de gerenciamento, e do relacionamento existente entre entidades. Algumas destas dúvidas são:

- Quais são os gerentes que apresentam maior carga de tráfego?
- Quais são os agentes que apresentam maior carga de tráfego?
- Quais são os agentes gerenciados por mais de um gerente?
- Existem entidades que atuam como gerente e agente?
- Quais são os relacionamentos mais geradores de tráfego?

  Qual o tipo de relacionamento (cg/cr ou no/nr)?
- Existem hierarquias de gerenciamento? Como fica a distribuição do tráfego gerado?

Para representar gerentes, agentes e o relacionamento entre eles, a abstração utilizada foi a de um grafo, estrutura amplamente utilizada na representação de topologias de rede em geral. No entanto, alguns aspectos do problema não puderam ser denotados adequadamente através de uma estrutura de grafo. Por exemplo, no grafo representativo da topologia é possível visualizar que uma entidade possui um papel importante na rede através da diferença de cor entre ela e os outros nodos, mas é difícil compará-las em termos proporcionais. A partir dessa limitação da estrutura de dados, surgiu a necessidade do uso de uma outra estrutura, mapeada para o *display* de visualização complementar localizado abaixo da topologia original. Este *display* utiliza as mesmas abstrações visuais instanciadas para o grafo (forma, cor e tamanho relativo), o que faz com que ambas possam ser facilmente correlacionadas.

A partir das abstrações mencionadas, foi criada a visualização de topologia de rede de gerenciamento, uma técnica que utiliza a combinação de visualização de grafos e *scatterplot* para visualizar os fluxos de mensagens SNMP. Na sua conformação inicial, a visualização de topologia de rede de gerenciamento provê uma visão geral sobre os gerentes, agentes e fluxos de mensagens vistos entre eles. Através desta visão, identificar as entidades e conexões com maior carga de tráfego é um processo intuitivo. Por outro lado, é difícil identificar a relação entre a conectividade e a carga de tráfego de uma determinada entidade olhando apenas para a topologia de gerenciamento. Ou seja, não é intuitivo identificar se os nodos mais conectados do grafo são aqueles que possuem maior tráfego passando por eles. A visualização de *scatterplot* mostrou-se eficiente para este propósito, ao plotar os nodos no *display* de visualização de acordo com o relacionamento entre carga de tráfego e conectividade. Isso mostra que a visão geral da técnica de visualização proposta facilita a aquisição de alguns *insights* úteis a respeito da rede de gerenciamento, mesmo antes de qualquer interação do usuário.

Após obter uma visão geral de toda a rede de gerenciamento, o usuário pode focar sua atenção em alguns elementos que demandem uma investigação mais profunda (*e.g.*, gerentes que possuem uma grande conectividade e carga de tráfego). Para tanto, ele precisa interagir com a visualização, ajustando-a para satisfazer suas necessidades. Através dos filtros de nodos e conexões, é possível mostrar apenas os nodos e conexões que possuam

carga de tráfego dentro dos limites estabelecidos pelo usuário. Esta operação é particularmente útil em topologias muito grandes, onde a quantidade de elementos apresentados pode tornar difícil a formulação de padrões sobre as trocas de mensagens entre gerentes e agentes. Outra possibilidade de interação disponível é a centralização de qualquer nodo da topologia, operação que faz com que todos os nodos vizinhos sejam posicionados próximos do nodo centralizado. Este processo leva a uma melhor compreensão do papel que a entidade focalizada exerce na rede.

Na visualização de diversos tráfegos SNMP coletados, foi possível detectar a tendência de vários agentes e gerentes possuírem valores similares de carga de tráfego. Comumente esta tendência forçava os nodos a aparecerem muito próximos um dos outros (ou mesmo sobrepondo-se) no *scatterplot*, o que muitas vezes levava a uma identificação imprecisa desses elementos. Este problema foi resolvido através de filtros localizados próximos aos eixos do *scatterplot*, que restringem o intervalo dos eixos e fazem com que a visualização de nodos como características similares seja possível.

5.3 Avaliação da Visualização de Número de Mensagens SNMP por Período

No SNMP, a comunicação entre agentes e gerentes se dá através da troca de mensagens entre eles. O propósito principal de uma mensagem SNMP é controlar ou monitorar parâmetros de um agente SNMP. O cômputo do número de mensagens SNMP trocadas em determinados intervalos de tempo leva a um melhor entendimento sobre a relação existente entre os tipos de mensagem SNMP, e sobre a proporção de cada versão do protocolo vista no tráfego. Este estudo tem por objetivo dirimir as seguintes dúvidas:

- Existem padrões bem definidos na troca de mensagens? Se esses padrões são alterados em determinados intervalos, quais as mensagens responsáveis pela alteração?
- Quais são as mensagens mais enviadas?
- Quais são as versões do SNMP mais utilizadas?
- O protocolo está sendo utilizado com propósitos de configuração dos dispositivos?
- Qual o nível de otimização na troca de mensagens, levando em conta as versões do protocolo utilizadas?
- Predomina o uso de gerenciamento proativo ou reativo?

Para o estudo da distribuição de mensagens SNMP em função do tempo, foi utilizada uma estrutura de série temporal, capaz de armazenar os tipos de mensagem e versões do SNMP em intervalos de tempo de uma hora. A característica mais importante deste tipo de dados é que as observações vizinhas são dependentes, sendo necessário analisar e modelar esta dependência para que padrões nas trocas de mensagens possam ser formulados.

A série temporal é então instanciada em um diagrama de barras seccionado, no qual as secções representam os tipos de mensagens ou versões do SNMP. Quando a visualização de número de mensagens SNMP por período é iniciada, ela exibe todo o conjunto de mensagens trocadas no tráfego, classificadas por tipo de mensagem. A priori, o usuário pode obter *insights* sobre os tipos de mensagens que são mais predominantes no tráfego, e sobre a distribuição das mesmas em função do tempo.

Depois de obter uma visão geral a respeito das trocas de mensagens ocorridas, o operador pode ajustar o escopo de dados que devem ser exibidos. Isto pode ser feito através dos filtros de mensagens/versões do SNMP, ou da operação de *zooming* semântico. A primeira permite ao usuário focar os esforços de análise apenas nos tipos de mensagens ou nas versões do SNMP utilizadas. Após esta primeira seleção, o usuário pode selecionar apenas os mensagens ou versões do protocolo que ele pretende visualizar no histograma de barras, fazendo com que fique mais fácil a comparação entre os tipos de mensagens ou versões de maior interesse, ou mesmo a visualização de padrões de uso de mensagens encontradas com pouca frequência. A operação de *zooming* semântico restringe o período de captura analisado, de forma que apenas um subintervalo da captura de tráfego seja visualizado. Isto leva à identificação de padrões de troca de mensagens que mudam de acordo com a unidade do intervalo de tempo representado pelas barras (anos, meses, dias ou horas).

A abstração visual utilizada (diagrama de barras seccionado) mostrou-se eficiente para analisar a troca de mensagens SNMP em função do tempo. No entanto, este tipo de representação possui uma limitação, relativa a uma característica intrínseca do SNMP. No protótipo implementado, o operador pode visualizar as mensagens SNMP divididas por operação ou versão do protocolo. No entanto, para aquisição de novos *insights*, seria interessante visualizar as divisões de mensagens e versões sendo mostradas na mesma visualização. Esta limitação constitui um dos trabalhos futuros da pesquisa.

5.4 Avaliação da Visualização de Árvore de Objetos SNMP

Um objeto gerenciado SNMP é a visão abstrata de um recurso real do sistema. Assim, todos os recursos da rede que devem ser gerenciados são modelados, e as estruturas de dados resultantes correspondem aos objetos gerenciados. Os objetos gerenciados são armazenados em árvores denominadas MIBs (*Management Information Bases*), que procuram abranger todas as informações necessárias para o gerenciamento de uma rede. No que tange a objetos gerenciados e MIBs, pode-se levantar as seguintes questões:

- Quais são os objetos mais acessados? A que MIB eles pertencem?
- Qual a quantidade de objetos de uma determinada MIB acessados?
- Os objetos de determinada MIB tem número de acessos semelhante?
- Objetos considerados obsoletos continuam sendo utilizados?
- MIBs proprietárias são utilizadas?

Dado que os objetos SNMP são nativamente organizados em uma estrutura de árvore, é desejável que a abstração de dados também armazene o conjunto de objetos encontrados no tráfego nesse tipo de estrutura. No entanto, tal estrutura mostra-se insuficiente para mostrar a proporção de objetos no tráfego, o que leva à necessidade do uso de outra abstração dos dados a ser mapeada para um diagrama de barras.

A abstração acima mencionada é então instanciada para a visualização da árvore de objetos SNMP, uma combinação de duas técnicas de visualização de informação: árvore identada e histograma de barras. Quando a visualização é inicializada, todos os diretórios da MIB encontram-se ocultos, sendo papel do usuário expandi-los de atráves de cliques do mouse. Essa característica faz com que o usuário possa visualizar apenas os objetos

das MIBs nas quais possui interesse. Caso deseje ter uma visão geral do conjunto de objetos, o operador pode utilizar um botão localizado acima da visualização, que expande todos os diretórios da MIB e seus respectivos objetos. Como frequentemente existe um grande número de objetos distintos em um tráfego SNMP, a árvore pode ficar maior do que o espaço de visualização. Para que o usuário possa visualizar todos os objetos, uma barra de rolagem localizada à direita do *display* move a árvore para cima ou para baixo.

5.5 Avaliação da Visualização do Relacionamento entre Objetos SNMP

O SNMP define que uma mensagem pode carregar um ou mais objetos em cada operação. Os conjuntos de objetos que são transportados dentro das mesmas mensagens tendem a se repetir com maior ou menor incidência, dependendo do grau de proximidade existente entre os objetos. Esta característica do protocolo traz a tona as seguintes dúvidas:

- Quais objetos são frequentemente encontrados juntos em atividades de gerenciamento de alto nível?
- Quais objetos são usualmente requisitados de forma solitária?

A noção da teoria de conjuntos foi utilizada como abstração para instanciar o problema do relacionamento entre objetos. De acordo com a mesma, ao passo que o número de objetos vistos em determinado tráfego SNMP cresce, o número de conjuntos de objetos cresce de forma exponencial, seguindo a fórmula 2^N. Para um tráfego com apenas 20 objetos presentes, seria necessário visualizar 1.048.576 conjuntos, o que tornaria o estudo inviável. Para contornar este problema, os objetos foram representados como elementos visuais solitários, e os conjuntos correspondentes foram representados como linhas conectando-os. Esta abstração visual levou a uma representação mais efetiva do relacionamento entre os objetos SNMP.

A visualização inicial do relacionamento entre objetos SNMP mostra todos os conjuntos de objetos que aparecem no tráfego. A medida que o número de objetos presentes em um tráfego cresce, fica mais complicado para identificar visualmente quais objetos formam um dado conjunto, dado que os mesmos ficam cada vez menores para permitir uma visão global do agrupamento de objetos. Por outro lado, é fácil visualizar *clusters* de objetos, que podem ser identificados a seguir, a partir de interações com o usuário.

Zooming e *panning* são exemplos de mecanismos de interação disponibilizados pela visualização. Através do uso deles, o usuário pode navegar através dos *clusters* de objetos e identificar quais conjuntos de objetos formam um *cluster*.

O *layout* baseado em forças que foi empregado para apresentar os objetos pode levar a um reconhecimento de padrões facilitado, ao mostrar os objetos mais relacionados próximos uns aos outros. Se alguns objetos frequentemente aparecem próximos uns aos outros em tráfegos diferentes, é intuitivo assumir que estes são comumente requisitados juntos em mensagens SNMP.

6 CONCLUSÕES E TRABALHOS FUTUROS

Nos últimos anos, alguns trabalhos investigaram a aplicação de técnicas de visualização de informação no estudo de tráfegos de rede. A interatividade tem sido considerada um dos principais fatores que fazem com que técnicas de visualização de informação sejam efetivas, atendendo aos anseios dos usuários na descoberta de novas inferências sobre os dados analisados. No entanto, não existem investigações na área de gerenciamento de redes que tentem definir o papel da interatividade no processo de aquisição de *insights* na visualização de tráfegos. Nesta dissertação de mestrado foram apresentadas e avaliadas quatro técnicas de visualização de informação interativas adaptadas para o estudo de capturas de tráfego SNMP. Através do presente estudo procurou-se demonstrar a eficiência do uso de técnicas de visualização de informação no estudo de tráfegos de gerenciamento. Os resultados obtidos foram publicados no artigo *"Interactive SNMP Traffic Analysis through Information Visualization"* (BARBOSA; GRANVILLE, 2010).

Uma das propostas de visualização apresentadas nessa dissertação de mestrado foi a "Topologia de Rede de Gerenciamento", que permite verificar os padrões de interação entre os agentes e gerentes de uma rede, através do mapeamento dos fluxos de mensagens do tipo CG/CR e NO/NR para um grafo e uma visualização complementar (*scatterplot* ou diagrama de barras). Nesta visualização, a visão geral mostrou-se eficiente para a aquisição de *insights* referentes ao relacionamento entre gerentes e agentes, e sobre a relação entre a carga de tráfego e conectividade de um nodo. É possível ajustar a visualização para satisfazer as necessidades do pesquisador utilizando filtros em ambas as visualizações complementares e ajustes no *layout*, *zooming* e *panning* da visualização do grafo. Padrões existentes nas cargas de tráfego dos nodos e vértices podem ser identificados mais facilmente, e as abstrações visuais utilizadas são coerentes e complementares.

Outra visualização proposta é a de "Número de Mensagens SNMP por período", que mapeia a quantidade de mensagens trocadas entre gerentes e agentes durante o período de captura do tráfego, classificando-as quanto ao tipo de mensagem ou a versão do protocolo utilizada. Para tanto é utilizada uma técnica de visualização chamada histograma de barras seccionado. A visão geral desta visualização apresenta claramente os tipos de mensagem ou versões do SNMP que são mais predominantes em um tráfego. O usuário pode interagir com a visualização através dos filtros de mensagens/versões do SNMP, de forma que apenas as operações desejadas possam ser mostradas, e também através de uma operação de *zooming* semântico, que permite a visualização de padrões de trocas de mensagens que variam em função da unidade de tempo mostrada.

A "Visualização de Árvore de Objetos SNMP" mostra, através de uma disposição similar a de uma *MIB Tree*, a quantidade de vezes que um objeto está presente no tráfego, através da combinação das técnicas de visualização de árvore identada e histograma de barras. Através do mecanismo de navegação da árvore, o usuário possa visualizar apenas

os objetos das MIBs nas quais possui interesse. A visão geral dos objetos é adquirida através de um botão acima da visualização, que expande todos os diretórios e objetos da árvore. A abstração utilizada mostrou-se adequada para o propósito da visualização, ao aliar a visualização de árvore identada, familiar para os operadores de rede, com um histograma indicativo no número de vezes que cada objeto presente no tráfego foi visto.

Por fim, a "Visualização do Relacionamento entre Objetos SNMP" exibe os agrupamentos de objetos que costumam aparecer com maior frequência dentro das mesmas operações. Para tanto, os agrupamentos de objetos são visualizados em uma nova técnica de visualização de conjuntos, na qual o *layout* de disposição dos conjuntos é baseado na proximidade de seus elementos. A visão geral desta visualização mostra os *clusters* de objetos encontrados, que podem ser explorados através de mecanismos de interação como *zooming* e *panning* do *display*. O *layout* baseado em forças utilizado pode levar a um reconhecimento de padrões intuitivo, ao mostrar os objetos mais relacionados próximos uns aos outros. A abstração visual utilizada levou a uma representação satisfatória do relacionamento entre objetos SNMP, ao representá-lo com menos elementos visuais do que a abordagem de visualizar os conjuntos de objetos como elementos visuais independentes.

Como trabalhos futuros, destaca-se o desenvolvimento e avaliação de novas técnicas de visualização, adaptadas para o estudo de outros aspectos dos tráfegos SNMP não contemplados neste trabalho. A visualização de outros tráfegos de gerenciamento (*e.g.*, tráfegos SSH/TELNET e ICMP) também é encorajada, para que se possa alcançar um melhor entendimento de outras tecnologias de gerenciamento de redes. Por fim, os protótipos de visualização criados podem ser utilizados por pesquisadores e operadores de rede para estudos acerca de tráfegos SNMP capturados segundo a metodologia do IRTF, visando a um melhor entendimento sobre os padrões de uso real do protocolo.

REFERÊNCIAS

AGRAWAL, R.; SRIKANT, R. Fast Algorithms for Mining Association Rules. In: INTERNATIONAL CONFERENCE ON VERY LARGE DATA BASES, 20., VLDB, 1994. **Anais...** [S.l.: s.n.], 1994. p.487–499.

AMFPHP. **Flash Remoting for PHP**. Disponível em: <http://www.amfphp.org/>. Acesso em: fev. 2010.

BARBOSA, P. T.; GRANVILLE, L. Z. Interactive SNMP traffic analysis through information visualization. In: IEEE/IFIP NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, 12., NOMS 2010, 2010. **Anais...** [S.l.: s.n.], 2010. p.73–79.

BUJA, A.; MCDONALD, J. A.; MICHALAK, J.; STUETZLE, W. Interactive data visualization using focusing and linking. In: CONFERENCE ON VISUALIZATIONS, 2., VIS '91, 1991, Los Alamitos, CA, USA. **Anais...** [S.l.: s.n.], 1991. p.156–163.

CARD, S. K.; MACKINLAY, J. D.; SHNEIDERMAN, B. (Ed.). **Readings in information visualization**: using vision to think. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1999.

CASE, J.; MCCLOGHRIE, K.; ROSE, M.; WALDBUSSER, S. **Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)**. [S.l.]: IETF, 1996. n.1903. (Request for Comments).

CEGLAR, A.; RODDICK, J. F. Association mining. **ACM Computing Surveys**, New York, NY, USA, v.38, n.2, p.5, 2006.

DOBREV, P.; STANCU-MARA, S.; SCHOENWAELDER, J. Visualization of Node Interaction Dynamics in Network Traces. In: AIMS '09: PROCEEDINGS OF THE 3RD INTERNATIONAL CONFERENCE ON AUTONOMOUS INFRASTRUCTURE, MANAGEMENT AND SECURITY, 2009, Berlin, Heidelberg. **Anais...** [S.l.: s.n.], 2009. p.147–160.

FLARE. **The flare Visualization Toolkit**. Disponível em: <http://flare.prefuse.org/>. Acesso em: fev. 2010.

FREITAS, C. M. D. S. Visualização de informações e a convergência de técnicas de computação gráfica e Interação Humano-Computador. **Atualizações em Informática 2007**, [S.l.], v.9, n.5, p.171–220, 2007.

HARRINGTON, D.; PRESUHN, R.; WIJNEN, B. **An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks**. [S.l.]: IETF, 2002. n.3411. (Request for Comments).

HEER, J.; CARD, S. K.; LANDAY, J. A. prefuse: a toolkit for interactive information visualization. In: CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, 1., CHI '05, 2005, New York, NY, USA. **Anais...** [S.l.: s.n.], 2005. p.421–430.

JACOBSON, V.; LERES, C.; MCCANNE, S. **Tcpdump**. Disponível em <http://www.tcpdump.org>. Acesso em: maio 2009.

JFREECHART. **JFreeChart**: a free java chart library. Disponível em: <http://www.jfree.org/jfreechart>. Acesso em: fev. 2010.

KEIM, D. A.; MANSMANN, F.; SCHNEIDEWIND, J.; SCHRECK, T. Monitoring Network Traffic with Radial Traffic Analyzer. In: IEEE SYMPOSIUM ON VISUAL ANALYTICS SCIENCE AND TECHNOLOGY, 1., VAST 2006, 2006, Baltimore, Maryland, USA. **Anais...** [S.l.: s.n.], 2006. p.123–128.

MANSMANN, F.; VINNIK, S. Interactive Exploration of Data Traffic with Hierarchical Network Maps. **IEEE Transactions on Visualization and Computer Graphics**, Los Alamitos, CA, USA, v.12, n.6, p.1440–1449, 2006.

MCCLOGHRIE, K.; PERKINS, D.; SCHOENWAELDER, J. **Structure of Management Information Version 2 (SMIv2)**. [S.l.]: IETF, 1999. n.2578. (Request for Comments).

MUNZNER, T. A Nested Process Model for Visualization Design and Validation. **IEEE Transactions on Visualization and Computer Graphics**, Piscataway, NJ, USA, v.15, n.6, p.921–928, 2009.

NORTH, C. Toward Measuring Visualization Insight. **IEEE Computer Graphics and Applications**, Los Alamitos, CA, USA, v.26, n.3, p.6–9, 2006.

OBERHEIDE, J.; GOFF, M.; KARIR, M. Flamingo: visualizing internet traffic. In: IEEE/IFIP NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, 10., NOMS, 2006, Vancouver, Canada. **Anais...** [S.l.: s.n.], 2006. p.150–161.

SALVADOR, E. M.; GRANVILLE, L. Z. Using Visualization Techniques for SNMP Traffic Analyses. In: IEEE SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS, 2008. ISCC, 2008. **Anais...** [S.l.: s.n.], 2008. p.806–811.

SALVADOR, E. M.; GRANVILLE, L. Z. Arquitetura de uma Ferramenta e Técnicas de Visualização para Medições sobre Tráfego SNMP. In: SIMPóSIO BRASILEIRO DE REDES DE COMPUTADORES, SBRC, 26., 2008, Rio de Janeiro, Brasil. **Anais...** [S.l.: s.n.], 2008. p.93–106.

SARAIYA, P.; NORTH, C.; DUCA, K. An Insight-Based Methodology for Evaluating Bioinformatics Visualizations. **IEEE Transactions on Visualization and Computer Graphics**, Piscataway, NJ, USA, v.11, n.4, p.443–456, 2005.

SARAIYA, P.; NORTH, C.; LAM, V.; DUCA, K. A. An Insight-Based Longitudinal Study of Visual Analytics. **IEEE Transactions on Visualization and Computer Graphics**, Los Alamitos, CA, USA, v.12, n.6, p.1511–1522, 2006.

SCHOENWAELDER, J. **Simple Network Management Protocol (SNMP) Traffic Measurements and Trace Exchange Formats**. [S.l.]: IETF, 2008. n.5345. (Request for Comments).

SCHOENWAELDER, J.; PRAS, A.; HARVAN, M.; SCHIPPERS, J.; MEENT, R. van de. SNMP Traffic Analysis: approaches, tools, and first results. In: IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT, 10., IM, 2007. **Anais...** [S.l.: s.n.], 2007. p.323–332.

WIRESHARK. **Wireshark**: A network protocol analyzer. Disponível em <http://www.wireshark.org>. Acesso em: maio 2009.

XMLSOFT. **The XSLT C Library for Gnome**. Disponível em: <http://xmlsoft.org>. Acesso em: mar. 2010.

YI, J. S.; KANG, Y. a.; STASKO, J.; JACKO, J. Toward a Deeper Understanding of the Role of Interaction in Information Visualization. **IEEE Transactions on Visualization and Computer Graphics**, Piscataway, NJ, USA, v.13, n.6, p.1224–1231, 2007.

YI, J. S.; KANG, Y.-a.; STASKO, J. T.; JACKO, J. A. Understanding and characterizing insights: how do people gain insights using information visualization? In: CONFERENCE ON BEYOND TIME AND ERRORS, 1., BELIV '08, 2008, New York, NY, USA. **Anais...** [S.l.: s.n.], 2008. p.1–6.