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

Sistema de Detecção de Intrusão baseado em Métodos Estatísticos para Análise de Comportamento

por

ANA CRISTINA BENSO DA SILVA

Tese submetida à avaliação, como requisito
parcial para obtenção do grau de Doutor
em Ciência da Computação

Profa. Dra. Liane Margarida Rockenbach Tarouco
Orientadora

Porto Alegre, junho de 2003.

CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Silva, Ana Cristina Benso da

Sistema de Detecção de Intrusão Baseado em Métodos Estatísticos para Análise de Comportamento / por Ana Cristina Benso da Silva. – Porto Alegre: PPGC da UFRGS, 2003.

121p.: il.

Tese (doutorado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-graduação em Computação, BR – RS, 2003. Orientador: Tarouco, Liane M. R.

1. Redes de Computadores. 2. Gerência de Redes de Computadores. 3. Gerenciamento de Segurança. 4. Sistema de Detecção de Intrusão. I. Tarouco, Liane Margarida Rockenbach. II. Título.

Agradecimentos

Agradeço ao meu pai e à minha mãe, *in memorian*, pelo carinho e dedicação com que construíram e cuidaram de nossa família. Agradeço a eles a educação que me deram e a oportunidade e o incentivo para estudar.

Agradeço em especial ao meu esposo, Fábio, por seu apoio, por sua paciência, pelo seu contínuo incentivo e por sua incansável dedicação.

Agradeço à minha avó e a minha irmã o carinho para comigo.

Agradeço à minha orientadora o seu apoio para a realização deste trabalho.

Agradeço aos meus amigos João Batista e Cristina Nunes pelo seu inestimável apoio e amizade.

Agradeço à família de meu esposo à compreensão pelos momentos de convívio roubados pelo dever com este trabalho.

Agradeço à PUCRS o suporte para realização deste trabalho.

Agradeço à Profa. Vera Lima, ao Prof. Bernardo Copstein e ao Sr. Ricardo Pianta, da HP, o apoio e compreensão recebidos ao longo da execução deste trabalho.

Agradeço aos meus amigos do projeto CPSE, Paulo, Daniel e Fernando pela grande colaboração neste trabalho. E, também, aos demais, Felipe, Andrei, Fabrício e Eugênio, Juliana e Leonardo pelo seu incentivo.

Agradeço às minhas amigas “Lulus” pela amizade, pelo incentivo e pelos ótimos momentos de descontração.

Agradeço a todos que de uma forma ou de outra contribuíram, direta ou indiretamente, durante a execução deste trabalho.

Enfim, agradeço a Deus.

Sumário

Lista de Abreviaturas

API	Application Program Interface
CPSE	Centro de Pesquisa em Sistemas Embarcados
CPTS	Centro de Pesquisa em Teste de Software
CPU	Central Processing Unit
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
DoS	Denial of Service
HIDS	Host Intrusion Detection System
HP	Hewlett-Packard
I/O	Input/Output
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineering
IETF	Internet Engineering Task Force
IP	Internet Protocol
JNI	Java Native Interface
LDAP	Lightweight Directory Access Protocol
LVQ	Learning Vector Quantization
MAC	Medium Access Control
MIB	Management Information Base
NIDS	Network Intrusion Detection System
OSI	Open System Interconnection
PDA	Portable Devices Adapter
PDP	Policy Decision Point

PEP Policy Enforcement Points

PIB Policy Information Base

POP Postal Office Protocol

PPP Point-to-Point Protocol

PUCRS Pontifícia Universidade Católica do Rio Grande do Sul

RFC Request for Comments

RMON Remote Monitoring MIB

SNMP Simple Network Management Protocol

TCP Transmission Control Protocol

UDP User Data Protocol

UPnP Universal Plug and Play

Lista de Figuras

Lista de Tabelas

Resumo

A segurança no ambiente de redes de computadores é um elemento essencial para a proteção dos recursos da rede, dos sistemas e das informações. Os mecanismos de segurança normalmente empregados são criptografia de dados, *firewalls*, mecanismos de controle de acesso e sistemas de detecção de intrusão. Os sistemas de detecção de intrusão têm sido alvo de várias pesquisas, pois é um mecanismo muito importante para monitoração e detecção de eventos suspeitos em um ambiente de redes de computadores. As pesquisas nessa área visam aprimorar os mecanismos de detecção de forma a aumentar a sua eficiência.

Este trabalho está focado na área de detecção de anomalias baseada na utilização de métodos estatísticos para identificar desvios de comportamento e controlar o acesso aos recursos da rede. O principal objetivo é criar um mecanismo de controle de usuários da rede, de forma a reconhecer a legitimidade do usuário através de suas ações.

O sistema proposto utilizou média e desvio padrão para detecção de desvios no comportamento dos usuários. Os resultados obtidos através da monitoração do comportamento dos usuários e aplicação das medidas estatísticas, permitiram verificar a sua validade para o reconhecimento dos desvios de comportamento dos usuários. Portanto, confirmou-se a hipótese de que estas medidas podem ser utilizadas para determinar a legitimidade de um usuário, bem como detectar anomalias de comportamento.

As análises dos resultados de média e desvio padrão permitiram concluir que, além de observar os seus valores estanques, é necessário observar o seu comportamento, ou seja, verificar se os valores de média e desvio crescem ou decrescem. Além da média e do desvio padrão, identificou-se também a necessidade de utilização de outra medida para refletir o quanto não se sabe sobre o comportamento de um usuário. Esta medida é necessária, pois a média e o desvio padrão são calculados com base apenas nas informações conhecidas, ou seja, informações registradas no perfil do usuário. Quando o usuário faz acessos a *hosts* e serviços desconhecidos, ou seja, não registrados, eles não são representados através destas medidas. Assim sendo, este trabalho propõe a utilização de uma medida denominada de grau de desconhecimento, utilizada para medir quantos acessos diferentes do seu perfil o usuário está realizando.

O sistema de detecção de anomalias necessita combinar as medidas acima descritas e decidir se deve tomar uma ação no sistema. Pra este fim, propõe-se a utilização de sistemas de regras de produção e lógica *fuzzy*, que permitem a análise das medidas resultantes e execução do processo de decisão que irá desencadear uma ação no sistema.

O trabalho também discute a integração do sistema de detecção de intrusão proposto à aplicação de gerenciamento SNMP e ao gerenciamento baseado em políticas.

Palavras-chave: Redes de computadores, Gerência de redes de computadores, Gerência de Segurança, Sistemas de detecção de intrusão.

Title: “Intrusion Detection System based on Statistical Methods for Behavior Analysis”

Abstract

The security in the computer network environment is an essential element for the protection of the net resources, systems and information. The applied security mechanisms are normally data cryptography, firewalls, access control mechanisms and intrusion detection systems. The intrusion detection systems have been largely researched because they are an important mechanism for monitoring and detecting suspected events in a computer network environment. The research in this area aims at improving the detection mechanisms in order to improve its efficiency.

This work is focused in the area of anomaly detection and is based on the use of statistical methods to identify abnormal behavior and to control the access to the net resources. The main objective is to create a mechanism to control the network users, with the goal of recognizing their legitimacy by their activities. The considered system uses average and standard deviation for detention of abnormal behavior. The results obtained through the monitoring of the users behavior and the application of the statistical measures proved the validity of this method for the recognition of the users abnormal behavior.

The analysis of the average and deviation standard results permitted to argue that, besides observing the average and deviation standard values, it is necessary to observe its behavior by verifying if the values grow or decrease. The analysis also pointed the necessity of using another measure to reflect how much it is unknown about the user behavior. This measure is necessary because the average and the standard deviation are calculated based only in the known information, that is, the registered information in the user profile. Unknown hosts and services are not registered, so they are not represented by these measures. Therefore, this work proposes the use of a measure called *degree of unfamiliarity* or *unknown degree,* which is used to measure how many accesses the user is carrying through that are different of his/her profile.

The intrusion detection system has to combine the measures described above and decide if it is necessary to take an action on the system. It is then proposed the use of rule production systems and fuzzy logic for the analysis of the resultant measures and the execution of the decision process that will result in an action in the system.

This work also discusses the integration of the proposed intrusion detection system to the SNMP management application and to the network management based on politics.

Keywords: Computer Networks, Network Management, Security Management, Intrusion Detection Systems.

1 Introdução

Segurança é uma questão em aberto ainda hoje. Muitos pesquisadores têm desenvolvido trabalhos na área de segurança e estão buscando sempre por novos mecanismos ou métodos para controlar a invasão dos sistemas por usuários maliciosos.

Os problemas de segurança, dos sistemas atuais, são causados principalmente por erros de implementação de aplicações e protocolos e pelas vulnerabilidades dos sistemas operacionais. No campo das aplicações, as vulnerabilidades aparecem continuamente, pois com o advento da Internet, o número de aplicações tem crescido rapidamente e estão disponíveis a uma extensa comunidade de usuários. Atualmente, acompanha-se também o crescimento rápido da utilização de dispositivos móveis e da utilização de redes *wireless*, que por sua vez introduzem uma outra gama de problemas de segurança, dadas as características especificas de ausência de cabo e de mobilidade de equipamentos e usuários. Estes ambientes exigem maior controle sobre os usuários e suas ações, bem como sobre suas credenciais, a fim de evitar a utilização dos recursos do ambiente e das credenciais dos usuários por usuários maliciosos e não autorizados.

Os mecanismos de segurança adotados atualmente, em geral, compreendem a utilização de métodos criptografia para proteção e autenticação dos dados e dos usuários, mecanismos de controle de acesso, e mecanismos de detecção de intrusão [YUE 03] [SHE 02]. Em especial, os sistemas de detecção de intrusão são utilizados para detectar as ocorrências de situações suspeitas, ou ataques reais, e também para prevenir os sistemas contra possíveis ataques.

Muitas pesquisas têm sido realizadas na área de sistemas de detecção de intrusão [BRO 01] [BUS 02] [CAB 01] [LEC 02] [MAN 02] [YE 02], de forma a otimizar a eficiência dos mesmos [KEM 02], sendo a eficiência relacionada tanto ao número e qualidade das detecções, quanto ao desempenho computacional dos mesmos. Vários mecanismos têm sido estudados como a utilização de métodos de *data mining* [LEE 98], redes neurais [MAR 01], métodos estatísticos [LEC 02] [MAN 02] [YE 02] [BRO 01] [JAV 91], e outros. Esses mecanismos têm sido bastante utilizados na área de detecção por anomalia, que representa dos maiores desafios atualmente na área de sistemas de detecção de intrusão, pois deve identificar situações que fogem a um padrão de comportamento considerado normal.

Este trabalho está focado na área de detecção por anomalia baseada na utilização de métodos estatísticos para identificar desvios de comportamento e controlar o acesso aos recursos da rede. O principal objetivo é criar um mecanismo de controle de usuários da rede de forma a reconhecer a legitimidade do usuário através de suas ações. A escolha por métodos estatísticos baseia-se no fato destes métodos serem descritos pela literatura como métodos de bom desempenho computacional, com bom grau de detecção de intrusões e serem mais flexíveis e assim apresentarem uma menor sensibilidade a falsos eventos [LEC 02].

A utilização de um sistema de controle de usuário pode ser convenientemente empregada em redes *wireless* para acompanhamento dos usuários na rede e validação de suas atividades, de forma a proteger a rede e os usuários do uso indevido dos recursos. Em redes tradicionais, ou seja, cabeadas, também há a possibilidade de utilização desse sistema de detecção, mas nestas redes normalmente os *hosts* utilizam sistemas multiusuário, que permitem a conexão remota de vários usuários, o que impede a associação de ações provenientes de um determinado *host* a um usuário. Em redes *wireless*, com a utilização de PDA´s (*Portable Device Adapter*) a associação de usuários a esses dispositivos é facilitada por serem normalmente utilizados por um único usuário. Isto permite que as ações do usuário sejam comparadas com o comportamento esperado (conhecido), a fim de determinar sua legitimidade.

A análise do comportamento do usuário pressupõe a construção do conhecimento a respeito de usas ações, ou seja, da construção de um perfil do usuário. Perfis de comportamento são bastante utilizados em sistemas de detecção de anomalias [MAR 01], pois a idéia de anômalo é de algo que se desvia de um padrão conhecido. Os dados que devem compor o perfil estão estritamente relacionados ao objeto de proteção dos sistemas de detecção de intrusões [WAR 99]. Neste sistema, o que deseja-se observar é a atividade do usuário em um ambiente de rede de computadores.

Assim sendo, o objetivo geral do sistema proposto é identificar através dos mecanismos estatísticos propostos, quando o comportamento de usuário desvia-se de seu comportamento habitual. Os objetivos específicos são apresentados a seguir.

1.1 Objetivos do Trabalho

O trabalho tem por objetivo detectar situações anômalas ao comportamento de um usuário, através da utilização de métodos estatísticos, e assim definir a legitimidade de acessos daquele usuário. Para alcançar este objetivo é necessário que:

- Identifiquem-se as medidas estatísticas a serem utilizadas para análise de comportamento;
- Identifiquem-se as informações específicas a respeito do usuário que são relevantes para análise de comportamento.

Em relação às medidas estatísticas, observa-se pela literatura [YE 02], que para reconhecimento de desvios de comportamento são normalmente utilizados a média e o desvio padrão.

Em relação às informações a serem observadas, deseja-se observar o que o usuário faz de acordo com o ambiente em que se encontra, buscando a partir disso a legitimidade do usuário através do padrão de comportamento tal como estudado em [FIO 00].

Neste sentido, este trabalho virá investigar que a utilização de medidas simples como média e desvio padrão podem ser empregadas e são suficientes para o reconhecimento de desvios de conduta de usuários, de forma a comprovar a sua legitimidade. Também se busca averiguar-se o comportamento do usuário pode ser monitorado e através da observação do volume de acessos a destinos e serviços da rede, deriva-se a hipótese sobre a autenticidade do usuário.

Além disso, outra contribuição do trabalho é uma proposta quanto à forma de interpretar as medidas e associar regras que identifiquem determinadas condições, a fim de restringir ou liberar o acesso dos usuários aos recursos da rede.

1.2 Organização do Texto

O Capítulo 2 apresenta uma visão geral sobre sistema de detecção de intrusão, que é a área na qual este trabalho está inserido. O capítulo 3 apresenta o mecanismo de detecção de intrusões para análise de anomalias no comportamento do usuário proposto

neste trabalho. O capítulo 4 apresenta os sistema de regras que podem ser utilizados para análise das informações estatísticas obtidas. O capítulo 5 apresenta uma visão do sistema de detecção de intrusões associado à aplicação de gerenciamento SNMP. O capítulo 6 apresenta as conclusões e trabalhos futuros.

2 Sistema de Detecção de Intrusão

Os sistemas de detecção de intrusão foram inicialmente propostos em 1980 [BUS 02] [SHE 02], sendo um dos marcos principais o modelo proposto por Denning em 1987 [DEN 87] que apresentou o primeiro modelo compreensivo para sistemas de detecção de intrusão. Desde então, várias pesquisas vêm sendo desenvolvidas nesta área visando explorar diferentes técnicas e conceitos aplicados à detecção de intrusão [AXE 99].

A detecção de Intrusão pode ser conceituada como a tecnologia de segurança que auxilia na identificação e isolamento de intrusões contra sistemas de computadores [PTA 98]. A tentativa de intrusão ou ameaça ao sistema é definida como a possibilidade de ter acesso ou manipular informações, ou ainda de tornar o sistema inutilizável ou instável. Em [BUS 02], o autor apresenta a seguinte definição para detecção de intrusão:

"Detecção de Intrusão é o ato de identificar indivíduos que estão utilizando um sistema computacional sem autorização e também indivíduos legítimos, ou seja, autenticados, que abusam de seus privilégios".

Neste caso, a intrusão caracteriza-se pela utilização sem autorização de um recurso e pelo abuso de direitos por parte de usuários conhecidos e autorizados, portanto, legítimos. Em ambas as situações, o evento é uma intrusão que deve ser identificada para garantir a segurança dos sistemas.

A identificação de tais eventos não é uma tarefa simples. Os sistemas atuais, incluindo-se no conceito de sistemas os ambientes de redes de computadores, são extremamente complexos, e a velocidade com novas aplicações e protocolos surgem e são adotados torna a função de detecção de intrusão uma tarefa complexa. Os principais problemas encontrados com estes sistemas estão relacionados aos mecanismos de identificação dos eventos do sistema, pois o mecanismo deve adaptar-se ao ambiente monitorado de forma que não gere alarmes para situações normais, ou deixe de gerar alarmes para situações de intrusão. Além disso, o tempo envolvido na análise, identificação e envio de alertas ao sistema também é um problema. O ideal para um sistema de detecção de intrusão é que o reconhecimento seja em tempo real para que ações de contenção e identificação de envolvidos possam ser realizadas, evitando que este ocorra, ou possa ser contido a tempo.

O sistema de detecção de intrusão é um dos mecanismos complementares à segurança de um sistema. Existem vários métodos disponíveis para proteger um sistema de computadores ou uma rede de um ataque. Em [AXE 98] são listadas seis abordagens gerais antiintrusivas, as quais são apresentadas a seguir:

- Prevenção: prever ou coibir severamente uma intrusão;
- Preempção: agir contra o possível atacante antes que ele ataque o seu sistema;
- Persuasão: persuadir o atacante a não executar o ataque ou mesmo suspender um possível ataque em andamento;
- Ilusão: iludir o intruso, fazendo-o pensar que o ataque foi bem sucedido;
- Detecção: identificar tentativas de invasão do sistema e acionar os mecanismos apropriados; e,
- Ação: executar contra-medidas para conter ativamente e autonomamente uma intrusão em andamento, que não foi necessariamente detectada.

Segundo [AXE 98] os sistemas de detecção de intrusão encaixam-se exclusivamente na categoria de detecção, de acordo com as técnicas acima apresentadas.

2.1 Tipos de sistemas de detecção de intrusão

Um sistema de detecção de intrusão pode ser um software ou hardware, que automatize o processo de detecção através de técnicas de monitoramento, visando identificar possíveis alterações nos padrões ou atividades previamente definidas como maliciosas.

Estes sistemas podem ser classificados quanto ao tipo da informação analisada e também em relação ao modo como os sistemas analisam as informações coletadas. Quanto às informações analisadas, os sistemas são classificados em:

- NIDS (*Network Intrusion Detection System*): monitoram os pacotes que trafegam na rede;
- HIDS (*Host Intrusion Detection System*): monitoram o comportamento dos sistemas, analisando dados tais como arquivos de *log*, chamadas de sistema, dados de equipamentos como *firewalls* e roteadores, etc; e,

- Híbridos: sistemas que monitoram tanto os pacotes da rede, quanto às informações dos sistemas.

Estes sistemas são aplicáveis de acordo com o tipo de intrusão que se deseja monitorar e em que nível consegue-se obter informações sobre elas. Os sistemas baseados em rede costumam trabalhar com as informações de endereçamento, protocolo e portas de aplicação para a identificação de tentativas de ataques. Essas informações são obtidas do *header* dos protocolos contidos no pacote e são mais rápidas de analisar. No entanto, alguns sistemas de detecção também executam a verificação do conteúdo do *payload* do pacote para detectar outros tipos de ataque. Os sistemas baseados em *host* estudam os eventos internos ao *host*, analisando as informações geradas pela execução de operações no sistema.

No sistema híbrido, as duas abordagens são utilizadas, pois ambas são importantes e não exclusivas. Uma tentativa de ataque identificada por NIDS, poderá não ocorrer efetivamente, dependendo do sistema alvo. Enquanto que situações não detectadas na monitoração da rede podem constituir-se de ataques ao sistema alvo.

2.2 Formas de Detecção de Intrusão

A detecção de intrusões torna-se possível a partir da coleta de dados da entidade a ser protegida. Esses dados podem ser coletados na rede ou em estruturas de controle do sistema como *logs*, tabelas de processos e outros. As técnicas aplicadas na identificação de uma invasão analisam as informações coletas na busca de desvios de comportamento ou por padrões de ataques conhecidos.

Na classificação por modelo de análise das informações, os sistemas são classificados em:

- Detecção por assinatura: baseia-se na identificação de um padrão de ataque, já conhecido, chamado de assinatura; e,
- Detecção por anomalia: baseia-se no desvio de comportamento de um sistema de uma rede.

Os sistemas baseados em assinatura têm como vantagem a detenção do "conhecimento" sobre o comportamento normal ou suspeito, podendo identificar de

uma forma mais simples a ocorrência de um ataque e também diminuir o número de falsos positivos.

A desvantagem deste sistema é que a especificação das assinaturas tem de ser altamente qualificada para a identificação correta dos ataques em diferentes situações. Outra desvantagem é a falta de dinamicidade no reconhecimento de novos ataques, pois estes precisam ser previamente especificados no sistema.

O sistema baseado na identificação de anomalias normalmente possui uma base de conhecimento e mecanismos que o ajudam a identificar se o evento é efetivamente um ataque, se é uma variação de um ataque conhecido, ou se é apenas uma situação suspeita. Esse tipo de detecção é modelado para ser flexível, permitindo a identificação de situações que fogem ao padrão de comportamento da rede.

A desvantagem de sistemas baseados em anomalias é que ele aprende sobre comportamentos não usuais, que não são necessariamente ilícitos. E assim, poderá gerar alarmes do tipo falso positivo. Se o sistema aprende a aceitar comportamentos perigosos como normal, poderá não sinalizar um ataque real quando ele ocorrer.

Segundo [AXE 98], existem outras classificações de sistemas de detecção de intrusão referentes ao processamento das informações e características gerais do sistema, que são:

- Tempo de detecção: as técnicas são agrupadas por sua eficiência em detectar a intrusão, dividindo-se em *real-time*, *near real-time* e *non real-time;*
- Granularidade do processamento dos dados: esta classificação leva em conta a freqüência com que os dados são analisados, constantemente ou em intervalos de tempo regulares. A granularidade pode afetar a detecção das falhas;
- Processamento de dados: os dados podem ser processados de forma distribuída ou centralizada;
- Coleta de dados: os dados coletados podem ser de uma fonte centralizada ou de fontes distribuídas;
- Segurança: habilidade de contornar intrusões ao próprio sistema de detecção, contornando ataques de evasão e inserção;

- Grau de interoperabilidade: indica o quanto um determinado sistema é capaz de operar em conjunto com outras ferramentas de segurança de administração da rede;
- Grau de resposta a intrusões: um IDS pode responder a um ataque de forma passiva ou ativa. A maioria dos IDS oferece apenas mecanismos para geração de alertas aos responsáveis pelas redes e/ou sistemas sobre os possíveis ataques. No entanto, poderiam responder aos ataques de forma ativa, por exemplo, finalizando sessões de usuários, conexões de rede, configurando *firewalls*, entre outras [ANT 02].

As características acima apontadas não são exclusivas em um sistema de detecção de intrusão. E dentre elas uma característica muito importante é a segurança do sistema de detecção, pois a segurança do ambiente depende do grau de correção e integridade da informação por ele fornecida.

2.2.1 Detecção por Assinatura

O método de detecção por assinatura consiste em representar um ataque conhecido através de um padrão ou assinatura para que os ataques descritos e variações do mesmo possam ser identificados [AXE 98] [PTA 98]. Exemplos, de intrusões reconhecidas através da utilização deste método, são tentativas de conexão com um endereço IP reservado; pacotes TCP (*Transmission Control* Protocol) com combinações de *flags* ilegais; tentativas de estouro de pilha do *buffer* de DNS (*Domain Name System*); DoS (*Denial of Service*) em um servidor POP3 (*Post Office Protocol*); ataques de acesso a arquivos em um servidor de ftp; e-*mails* que possuam um vírus em particular; ataques de *SYN Flooding*; entre outros.

A maior dificuldade encontrada no desenvolvimento deste tipo de IDS é definir uma assinatura que englobe as variações de um ataque, mas não englobe as atividades normais. Outra dificuldade encontrada é a definição de uma referência sobre o protocolo a ser utilizada para definição das regras de comportamento e possíveis violações. As fontes utilizadas são a RFC (*Request for Comments*) do protocolo e a análise do comportamento do mesmo, pois nem sempre através da RFC é possível prever a ocorrências de falhas decorrentes da implementação do protocolo, e evitando assim a ocorrência de alarmes falso negativos ou falso positivos.

Além destes fatores, se observa que este tipo de abordagem exige a atualização dos padrões de ataque para que o sistema não fique obsoleto. Em comparação, o método anteriormente abordado, detecção por anomalia, é capaz de aprender novos padrões de comportamento de acordo com a sua ocorrência na rede.

2.2.2 Detecção por anomalia

A detecção por anomalia, conforme [AXE 98] [PTA 98] [WAR 99], baseia-se em caracterizar o comportamento de programas, protocolos e usuários através da construção ou treinamento de um modelo (perfil), utilizando métricas tais como número de chamadas de sistema, tempo de uso da CPU, número de conexões de rede em um determinado período de tempo, tamanho dos pacotes, etc. Este perfil pode também ser pré-determinado, por exemplo, tipo de usuários, tipo de rede, embora isto reduza as chances do IDS se adaptar aos diferentes estados do sistema.

A idéia utilizada para investigar anomalias é executar a comparação do estado do sistema ou de pacotes capturados com os dados do perfil estabelecido. Quando ocorrem variações significativas entre estes dados, considera-se como uma tentativa de intrusão.

Os problemas encontrados no desenvolvimento de sistemas de detecção por anomalias, de acordo com [COO 02], são:

- A descrição do comportamento de um sistema de maneira efetiva e eficiente, por motivos tais como o reconhecimento do comportamento do usuário final;
- A definição dos limites aceitáveis de variação entre o dado analisado e o perfil estabelecido, pois, na dependência destes, atividades normais podem ser interpretadas como intrusões, gerando alarmes falso-positivos; ou em situações piores, as intrusões não são detectadas, gerando alarmes falso-negativos.

A dificuldade em descrever o comportamento e definir limites aceitáveis tem limitado o desenvolvimento de sistemas de detecção de intrusão baseados na identificação de anomalias, sendo que as ferramentas existentes são desenvolvidas em nível de pesquisa. Várias técnicas estão sendo estudadas e podem ser aplicadas às detecções de anomalias envolvendo diversas métricas para elaboração de perfis de

comportamento [WAR 99]. Algumas das técnicas utilizadas estão descritas a seguir e, como exemplo, utilizam as chamadas de sistema como métrica, são elas:

- Enumeração de seqüências: para cada uma das chamadas de sistema ocorridas durante a execução normal de um programa, gera-se uma lista contendo as chamadas que a seguem com uma separação de até *n* chamadas. No entanto, existem relatos de que seqüências contínuas podem caracterizar melhor o comportamento;
- Métodos baseados em freqüências: modelam a distribuição de freqüência de seqüências de chamadas de sistemas. As seqüências que, durante o monitoramento, ocorrerem em freqüências distantes em relação ao modelo serão consideradas intrusões;
- *Data Mining*: estes métodos são utilizados para extrair as informações mais relevantes de grandes volumes de dados. A intenção é obter uma caracterização mais compacta de um comportamento normal, generalizando-o de forma a incluir padrões que não puderam ser observados durante a fase de treinamento;
- Máquina de Estados Finita: baseia-se na idéia de que uma chamada de sistema possui estados anteriores e posteriores à sua execução. Através da análise dos dados determina-se a freqüência com que cada estado ocorre. Os caminhos na execução do programa que não correspondem a estados e transições previstas, ou ocorram em freqüências diferentes da observada, são considerados intrusões;
- Redes Neurais: a rede é treinada de forma a predizer a próxima ação do usuário com base em seus *n* comandos anteriores. Conforme o desvio em relação a esta predição, é possível identificar um ataque.

O problema presente nestes métodos é que os mesmos podem ser treinados pelos invasores, fazendo com que intrusões sejam consideradas estados normais do sistema ou da rede. Com isto, a facilidade de atualização de um sistema de detecção através da utilização destas técnicas é prejudicada, pois torna-se necessário garantir que o comportamento do sistema ou da rede seja normal durante o período de coleta de dados, para fins de treinamento. Deve-se, com isso, utilizar métodos auxiliares para a redução e

normalização dos dados, fazendo com que apenas comportamentos considerados normais e relevantes estejam presentes no perfil.

Outra grande dificuldade, apontada por [GHO 99], é conseguir generalizar o comportamento anterior de forma a predizer ações futuras. Embora esta dificuldade também exista na fase de definição das assinaturas, é mais acentuada na detecção por anomalia, uma vez que o comportamento futuro pode não ser idêntico ao comportamento passado.

2.2.3 Métodos Estatísticos para Sistema de Detecção de Anomalias

Os métodos estatísticos são empregados nos sistemas de detecção de intrusões, principalmente baseados na detecção de anomalias, para determinar a ocorrência de intrusões ou para o pré-processamento dos dados que serão utilizados por outros métodos como, por exemplo, redes neurais.

Os primeiros trabalhos relevantes nesta área foram apresentados por Javitz [JAV 91] em 1991 e Helman [HEL 93] em 1993. A vantagem destes métodos, de acordo com [YE 02], é a sua capacidade de tratar e representar explicitamente as variações e ruídos envolvidos nas atividades dos sistemas computacionais. Além disso, eles apresentam um bom desempenho computacional, bons índices de reconhecimento e boa escalabilidade, minimizando o tempo de resposta dos sistemas de detecção, aumentando a confiança no resultado do sistema e reduzindo gargalos de processamento.

Mas ainda assim continua existindo um dos principais problemas dos sistemas de detecção de anomalias que é a construção dos perfis de comportamento os quais são utilizados para a comparação com as ações atuais, na tentativa de detecção de desvios do comportamento considerado normal. A manutenção dos perfis é igualmente importante nestes sistemas, pois elas devem refletir a alteração de comportamento dos sistemas observado como forma de aprender as mudanças que ocorrem e não invalidar o processo por utilizar dados que não refletem corretamente os comportamento real.

2.2.4 Trabalhos Relacionados à Aplicação de Métodos Estatísticos para Detecção de Anomalia

Recentemente, os métodos estatísticos passam a serem empregados nos sistemas de detecção de anomalia. Alguns trabalhos apresentam variações do método baseado em distribuição normal, como em [LEC 02] e [POR 98]. Enquanto, uma grande quantidade de trabalhos tem apresentado a utilização da probabilidade condicional, mais especificamente do Teorema de Bayes, tanto para sistemas de segurança quanto para sistemas de gerenciamento de falhas [STE 00] [MAN 02] [MAR 01] [BRO 01]. De forma a alcançar melhores índices de reconhecimento de eventos verdadeiros e com bom desempenho, pesquisadores utilizam alguma destas técnicas combinadas com sistemas especialistas, redes neurais, lógica *fuzzy*, entre outros, como apresentado em [LUO 01] [HEL 00] [DIC 01] [DIC 00] [LEE 98].

Os sistemas de detecção de intrusão baseados em métodos estatísticos, puros ou combinados com outros métodos, têm sido aplicados com objetivos variados como detecção de intrusão em sistemas, através da verificação das seqüências de comandos utilizadas por um usuário; detecção da legitimidade do usuário através da monitoração de suas ações, tanto em um *host* quanto na rede; detecção de intrusões em sistemas de telefonia celular; detecção de intrusões em serviços específicos, etc. Esses sistemas têm em comum o objetivo de detectar um evento ou uma seqüência de eventos que se desviam do comportamento considerado normal e, portanto caracterizam uma intrusão.

Em [JAV 91], é apresentado um sistema baseado em métodos estatísticos que observa o comportamento de sistema computacional e aprende de forma adaptativa o que é um comportamento normal para um usuário ou para um grupo de usuários, bem como identifica situações potenciais de ocorrência de intrusões. Este sistema utiliza uma base de conhecimento que consiste de perfis de comportamento. Os perfis armazenam informações sobre distribuições de freqüência, médias e covariâncias ao invés de armazenar todos os dados de forma bruta, para minimizar os requisitos de memória. A manutenção dos perfis é realizada diariamente, de forma a refletir nos perfis as alterações naturais de comportamento dos usuários. Os dados armazenados anteriormente também são processados de forma que as informações mais novas tenham maior peso nas decisões do que informações antigas. O método estatístico aplicado é

bastante complexo, pois ele utiliza vários métodos para refinar as informações até concluir se o evento caracteriza uma intrusão.

É importante ressaltar algumas considerações feitas pelo autor e que também foram identificadas no decorrer deste trabalho. Em primeiro lugar, o autor define níveis de alarmes de acordo com o nível de suspeita em relação à atividade, e os limiares e ações a serem realizadas são configuradas dinamicamente, de acordo com a política de cada sistema. Em segundo lugar, o autor identifica que a análise das variáveis deve ser feita de forma contínua no tempo, para que se possa determinar a variação das medidas e suas tendências. Desta forma, pode-se determinar se o comportamento tende a desviar-se do comportamento considerado normal, se ele permanece como normal ou anormal, e, se for anormal, verificar se ele retorna a um nível de normalidade.

Em [BUS 02], o autor apresenta um sistema de detecção de intrusão para sistemas de usuários móveis. O perfil é construído utilizando informações como a localização do usuário, a movimentação do usuário entre células em redes de transmissão de rádio-freqüência baseadas em células, e o tempo de permanência do usuário nestes ambientes. A probabilidade condicional é utilizada para identificar a probabilidade das ações dos usuários e então detectar os desvios de comportamento. O trabalho apresenta ainda a preocupação quanto à privacidade dos usuários.

Em [LEC 02], o autor aplica uma abordagem estatística para detectar varreduras de rede (*network scans*) em tempo real. O mecanismo está baseado em dois fatores: o quanto incomum é um sistema de origem s_i ter acesso a um destino ou porta deste destino; e a quantos destinos e portas um sistema de origem s_i teve acesso. Segundo o autor, seu método é capaz de detectar intrusões em tempo real, além disso, ele combina uma forma eficiente de indexar os acessos com uma abordagem probabilística para detectar os acessos que caracterizam as varreduras de rede. No entanto, este método não é capaz de detectar varreduras coordenadas realizadas por origens distribuídas.

Em [MAR 01], o autor apresenta um sistema de detecção de anomalias voltado a detecção de intrusões em *hosts*. O trabalho baseia-se na premissa de que usuários legítimos podem ser classificados em categorias, de acordo com o percentual de comandos que eles usam em um período específico. Isto é, um usuário legítimo, durante o tempo de permanência no sistema, irá gerar uma quantidade de informação suficiente para definir o seu perfil. Logo, quando o comportamento do usuário afastar-se do seu

perfil, o sistema poderá considerar que pode estar ocorrendo utilização indevida das credenciais do usuário. Os principais pontos para o autor são a seleção das informações que compõe o perfil, de forma a eliminar um conjunto potencial de comandos com erro de digitação, com utilização inexpressiva e também os casos que não correspondem a uma situação normal de uso. A seleção dos dados permite também minimizar os requisitos de memória e processador, melhorando o desempenho do sistema. O autor apresenta um método que utiliza lógica *fuzzy*, medidas como média e desvio padrão e algoritmos genéticos para o tratamento dos dados do perfil, de forma a selecionar as informações relevantes. Os dados resultantes são submetidos a uma rede neural que determina a ocorrência de uma intrusão. O algoritmo empregado neste passo é uma variação do LVQ (*Learning Vector Quantization*) [KOH 86].

Em [MAN 02] é apresentado um sistema para detecção de anomalias e falhas generalizadas. Esse sistema emprega métodos estatísticos para o pré-processamento dos dados e redes neurais para a classificação das falhas e intrusões. O sistema é constituído por uma hierarquia multiníveis com vários níveis de monitoração destinados à observação de vários parâmetros de tráfego. Esses parâmetros são usados para calcular a similaridade dos dados para então combiná-los de forma inteligente em um vetor de anomalias que é classificado por uma rede neural. Os valores numéricos demonstraram que esta metodologia detecta de forma confiável intrusões e faltas leves.

Em [BRO 01], o autor apresenta um sistema para detecção de intrusões em serviços Internet. O autor propõe a utilização de medidas como média e desvio padrão para obter informações sobre os eventos coletados e a utilização de redes bayesianas para determinar o grau de anormalidade dos eventos da aplicação. Nesta solução, a inteligência do sistema é alcançada pela utilização e medidas como média e desvio padrão e probabilidade condicional.

Em [YE 02], o autor apresenta uma comparação entre o método de Hottellings, o T^2 [YE 02], para uma análise multivariável com correlação de dados. O objetivo do trabalho é realizar a detecção de anomalias através da análise das chamadas de sistema realizadas pelos usuários. O autor apresenta também uma comparação deste método com o método X^2, que é um método de análise multivariável baseado na análise de média e desvio padrão. O autor concluiu que as intrusões manifestam-se basicamente pelas alterações de média da distribuição de intensidade de vários tipos de eventos.

Além de verificar que o teste X^2 é mais eficiente e eficaz na detecção das alterações de média e, por conseguinte, na detecção de intrusões. Enquanto que o T^2 apresentou maior sensibilidade a ruídos, gerando uma taxa maior de falso-positivos, e também pior desempenho computacional.

Esses trabalhos em geral apresentam um método estatístico para avaliar a variação de comportamento e para determinar a probabilidade de ocorrência de eventos a partir da monitoração de comportamento. Todos eles utilizam perfis previamente definidos como histórico para a comparação com eventos amostrados a cada momento e observação dos desvios de comportamento, bem como avaliação da probabilidade de ocorrência de um evento. A construção e manutenção dos perfis variam de trabalho para trabalho, mas todos são unânimes quanto à complexidade envolvida na modelagem, construção e manutenção dos mesmos, pois a confiabilidade do sistema depende da confiabilidade dos dados armazenados no perfil.

Além disso, alguns trabalhos apresentam uma forma um tanto complexa para a obtenção de medidas que sinalizem a ocorrência de intrusões, enquanto que experiências como apresentadas em [LEC 02] [BUS 02] [BRO 01] apresentam métodos simples e eficientes, pois as intrusões normalmente manifestam-se principalmente pelas alterações de média e desvio padrão [YE 02].

3 Modelo Estatístico para Detecção de Intrusão

Este trabalho propõe a construção de um sistema de detecção de intrusão para análise de comportamento de usuário, com o intuito de determinar a legitimidade dos mesmos e prevenir a utilização dos sistemas por usuários não autorizados, os quais, possivelmente, adquiriram credenciais de outros usuários de forma ilícita.

A aplicação deste sistema pode ocorrer tanto em redes tradicionais, ou seja, redes cabeadas (*wired*), quanto em redes sem fio (*wireless*). A principal motivação para a criação e utilização destes sistemas é o crescente avanço de ambientes que provêm conexão a diversos tipos de dispositivos e usuários para acesso aos serviços providos na rede local ou na Internet. Na visão futurista, ou nem tanto, os usuários com dispositivos portáteis com capacidade de conexão a uma rede, poderão mover-se entre redes, mantendo a conexão e o acesso aos serviços durante o seu deslocamento físico, ou poderão ter acesso aos serviços da Internet e da rede local através da conexão à rede *wireless* existente no ambiente onde eles estão, com métodos apropriados para garantir a segurança [BAL 02] [ZHA 00]. E nesses casos, precisa-se de mecanismos de monitoração e controle de usuários e serviços, tanto para o gerenciamento da segurança do ambiente, quanto para o gerenciamento de contabilização dos recursos utilizados pelos usuários.

Em redes tradicionais, o sistema pode ser aplicado, pois é conhecido que o maior número de intrusões têm origem dentro da rede atacada, que um grande número de ataques são originados por usuários legítimos, ou seja, registrados e autorizados a utilizar a rede em questão, e um grande número é gerado por intrusos que roubam as credenciais de usuários legítimos. Portanto, mecanismos de segurança devem auxiliar a identificar comportamentos maliciosos de forma a garantir a segurança da rede, bem como a segurança dos usuários que tenham tido suas credenciais roubadas. No caso específico da mobilidade de usuários e dispositivos, torna-se cada vez mais normal um usuário levar seu computador portátil e conectar-se a diferentes redes, desde que estas provenham um ponto de acesso, e a ampla adoção de redes sem fio torna mais fácil proporcionar a conexão destes usuários.

Assim sendo, considera-se que algumas medidas importantes devam ser adotas para garantir a segurança dos ambientes, tais como:

- Implementar mecanismos de controle de acesso para todo e qualquer usuário;
- Estabelecer políticas de segurança, especialmente para determinar:
    - O nível de segurança desejado para o ambiente;
    - Os direitos de acesso dos usuários na rede;
    - O nível de periculosidade dos eventos, de forma a identificar situações mais ou menos graves; e,
    - As contramedidas que devem ser adotadas em cada situação.
- Implementar diversos mecanismos de monitoração da rede para detectar situações de intrusão; e,
- Adotar a utilização de *firewalls* para isolar as redes que oferecem pontos de acesso da rede da organização, e também para proteger a rede da organização em relação à Internet.

Quanto aos sistemas de detecção de intrusão, podem ser empregados diferentes módulos, com objetivos específicos de detecção em conjunto com um sistema de correlação de dados, para que se alcance um maior conhecimento e compreensão sobre os eventos que ocorrem no ambiente e verificar suas correlações.

Neste trabalho a proposta concentra-se na implementação e utilização de um sistema de detecção de anomalias para análise do comportamento dos usuários. No sistema de detecção são empregados uma abordagem estatística para análise das medidas coletadas e um sistema de regras para análise da variação dos resultados estatísticos. A utilização de um sistema de regras torna mais flexível o tratamento dessas medidas, permitindo ao administrador do sistema realizar alterações de limiares de comparação, bem como alterações das regras e ações adotadas de acordo com a política de segurança local.

Os métodos estatísticos, conforme visto no capítulo 2, são utilizados em sistemas de detecção de intrusão, resumidamente, por serem eficientes tanto para detecção de intrusões, quanto em termos computacionais, ou seja, apresentam bom desempenho; e são mais flexíveis e sensíveis a ruídos que os demais métodos.

Vários trabalhos investigados apresentaram mecanismos que envolvem a aplicação de vários métodos estatísticos. Neste trabalho o objetivo é utilizar um método que seja capaz de detectar variações de comportamento que permita identificar se as

variações fogem dos parâmetros considerados normais para a situação analisada. Logo, dentro da classificação de sistemas de detecção de intrusão este é um sistema de detecção de anomalias.

Estes sistemas baseiam-se, normalmente, conforme apresentado anteriormente, na comparação de fatos atuais com fatos históricos, a fim de determinar sua semelhança. Os fatos históricos são coletados ou construídos de forma a representar um padrão de conduta para o objeto em questão, constituindo os chamados perfis. Inúmeras questões estão relacionadas à construção destes perfis como a manutenção de informações atualizadas, o volume de dados armazenados e, principalmente, a modelagem destes, de forma que eles reflitam comportamentos ditos normais.

Neste trabalho o histórico do usuário, ou seja, o seu perfil, armazena informações sobre suas ações em um ambiente de rede. Isto é, são armazenadas as suas ações na rede, que são traduzidas pelos endereços de destinos, serviços e protocolos que usuário usa. Esses dados são utilizados em um modelo estatístico, baseado em média e desvio padrão, para identificação de possíveis anomalias. Neste caso, as anomalias são desvios de conduta, o que gera as suspeitas sobre a legitimidade do usuário.

A seguir são apresentadas as variáveis que constituem o perfil do usuário, de forma a facilitar o entendimento do sistema, e o método estatístico utilizado.

3.1 Perfil

O perfil mantém uma descrição do comportamento normal de cada usuário. Ele foi projetado para manter informações históricas em quantidade razoável e que possam ser facilmente armazenadas e processadas por um sistema de detecção de anomalias. Além do que, o sistema implementa um mecanismo de manutenção, que envolve o envelhecimento das informações e o armazenamento de novos dados, de forma a acompanhar a evolução do comportamento de cada usuário e garantir a atualidade das informações para o sistema de detecção.

O primeiro passo é definir quais são as informações necessárias para identificar um usuário e quais são as informações necessárias para identificar a similaridade entre comportamentos. Esta definição depende do objeto em questão no sistema de detecção de intrusão e do ambiente em que ele está localizado. Por exemplo, em um HIDS, o

perfil do usuário deve conter dados sobre chamadas de sistemas individuais, seqüências de comandos, horários de acesso, tempo de permanência, entre outros. Em sistemas de telefonia móvel pode-se construir um perfil com dados sobre as chamadas do usuário, a localização usual do usuário, o padrão de movimentação do usuário entre estações rádio transmissoras, os horários de utilização, etc. A diversidade das informações armazenadas exige a utilização de métodos mais ou menos complexos para avaliação de todas as variáveis, além de possibilitarem uma análise mais detalhada dos perfis e o reconhecimento com maior segurança dos comportamentos monitorados. Mas em alguns casos, a diversidade de informações pode ser apenas um fator de complexidade, sendo que o nível de satisfação necessário para a detecção de intrusão pode ser alcançado com um conjunto reduzido de variáveis, minimizando a utilização de recursos de memória, processamento e a complexidade do sistema.

O perfil utilizado neste trabalho foi projetado para conter um conjunto mínimo, mas suficiente de variáveis que descrevam o comportamento de usuários em um ambiente de rede de computadores. Neste ambiente, pode-se observar as ações do usuário na rede, observando-se o tráfego gerado e recebido pelo mesmo, em função dos endereços de origem e destino e dos serviços aos quais ele está utilizando. A monitoração do tráfego, especificamente, permite observar:

- Os endereços de rede de origem e destino;
- Os endereços de aplicações;
- Os protocolos envolvidos;
- O volume de dados transferidos;
- O número de acessos a um destino ou serviço;
- O número de pacotes gerados entre origem e destino; e,
- As informações de controle dos protocolos.

Estes dados são facilmente obtidos do *header* dos protocolos contidos em cada pacote de dados que trafega na rede, sem necessidade de análise de dados de aplicação, ou seja, do conteúdo dos pacotes. A análise de informações de conteúdo representa uma sobrecarga maior de processamento e também a adoção de mecanismos mais sofisticados para identificação das possíveis variações da informação observada. Além disso, uma grande parte dos ataques existentes, que causam situações variadas de negação de serviço, varredura de rede, etc, são identificados basicamente pelas

informações contidas no *header* dos protocolos e pela freqüência de acesso a destinos e serviços [OLI 02].

Outra informação relevante, para sistemas que aceitam usuários móveis, é a localização destes usuários. No caso de redes de computadores, a localização pode ser traduzida pelo domínio da rede na qual o usuário está conectado. O domínio pode ser utilizado para verificar se, para um usuário, é comum estar conectado naquele domínio ou não. Não ser comum, faz com que o nível de desconfiança sobre um determinado usuário aumente e/ou sejam aplicadas restrições mais sensíveis às atividades do usuário na rede. A identificação da localização de um usuário é importante em um sistema de autenticação globalizado, por exemplo, em telefonia móvel, para identificar telefones clonados que aprecem simultaneamente em localidades diferentes.

Outras informações podem ser obtidas a respeito de um usuário na rede, tais como:

- Os horários de conexão do usuário; e
- O tempo de permanência do usuário na rede.

Essas informações podem ser obtidas através do controle dos eventos de *loggin* e *logout* dos usuários na rede, ou seja, através da monitoração do sistema de autenticação de usuários. A monitoração do processo de autenticação dos usuários e a monitoração do sistema de distribuição dinâmica de endereços de rede são importantes para que se possam associar as informações entre identidade do usuário e endereço de rede associado ao dispositivo do usuário, uma vez que, após esta fase somente o endereço estará presente nas informações que trafegam pela rede.

A partir da identificação do conjunto de variáveis que se pode obter a respeito do comportamento de um usuário em um ambiente de rede local, fez-se uma análise das informações básicas que podem descrever o comportamento de um usuário. Essa análise tem como premissa que um usuário pode ser identificado pelo que faz, ou seja, pelas suas ações na rede, e assim é necessário identificar dentre as variáveis acima descritas quais descrevem o comportamento do usuário. Além disso, a análise tem por objetivo selecionar o conjunto mais simples possível de informações para a construção de um modelo estatístico simples, mas satisfatório. O resultado da análise levou à identificação das seguintes variáveis:

- O endereço de rede do destino;
- O endereço do serviço (porta) do destino;
- O protocolo encapsulado no protocolo de rede; e,
- O número de acessos ao destino/serviço.

As demais informações não foram utilizadas inicialmente, pois se considerou que acrescentariam uma complexidade maior ao modelo, sem necessariamente contribuírem para a identificação do usuário de forma relevante, de acordo com os objetivos deste trabalho. Por exemplo: informações como volume de tráfego são extremamente variáveis, pois o usuário nem sempre irá fazer grandes transferências de arquivos; tempos de conexão e horários podem variar muito para usuários que viajam constantemente.

Essas variáveis foram escolhidas por permitirem mapear o comportamento do usuário através da observação dos destinos e serviços que ele utiliza. Os destinos são traduzidos por endereços de rede, isto é, em redes TCP/IP por endereços IP. E os serviços são traduzidos pelos endereços de aplicação, isto é, em redes TCP/IP, por endereços de porta. Além de mapear o que o usuário está utilizando, o sistema observa o número de acessos do usuário ao serviço. Um acesso é considerado uma conexão TCP ou UDP entre um cliente e um servidor. Isto é, o sistema contabiliza um acesso sempre que observar a comunicação entre a mesma origem e o mesmo destino e a instanciação de um novo cliente. No caso do protocolo TCP, não é necessário detectar inicio e fim de uma conexão TCP exatamente, apenas detectar o número de acessos que ocorrem entre uma origem e um destino. No caso do protocolo UDP, observe que o protocolo não é orientado à conexão, mas mesmo assim origem e destino de uma comunicação são reconhecidos pela tupla <IP, Porta>, permitindo a identificação dos acessos entre uma origem e um destino.

Em alguns casos, o usuário pode utilizar protocolos de aplicação de nível três, que não são encapsulados em um protocolo de transporte, mas são encapsuladas diretamente no protocolo IP, por exemplo, aplicações que utilizam ICMP. Neste caso, é necessário identificar os endereços de origem e destino, o protocolo em questão e o número de pacotes transmitidos entre origem e destino.

3.1.1 Tipos de Perfil

O perfil constitui o histórico do usuário com o qual pode-se confrontar as suas ações atuais e então observar as similaridades e discrepâncias da sua conduta em momentos diferenciados. A análise, neste caso, é intra-sujeito, pois avalia o comportamento do usuário com seu próprio comportamento passado. Mas também é necessário considerar que o usuário está exposto a influências externas que o levam a alterações de comportamento, devendo-se então observar também o que ocorre no ambiente em que o usuário está presente.

Então é necessário utilizar-se diferentes perfis para armazenar as informações necessárias ao sistema de análise de comportamento. Nesse trabalho inicialmente utilizou-se dois perfis diferenciados:

- O perfil do usuário, denominado perfil histórico (PH); e,
- O perfil da rede, denominado simplesmente perfil da rede (PR).

Toda a discussão até o momento refere-se ao PH, pois reflete o comportamento do próprio usuário no passado. O PR apresenta as mesmas informações que o PH, mas em relação ao conjunto de usuário que utilizam a rede. Esse perfil tem a tendência de refletir quais são as ações comuns aos usuários naquele ambiente e, portanto, captar as ações que são realizadas pelo grupo e também as ações que são estimuladas por existirem incentivos externos, como propagandas, etc.

O perfil histórico do usuário é utilizado com prioridade para a observação e identificação de sua autenticidade. O perfil da rede está em segundo lugar, pois se uma ação não pertence ao perfil do usuário, mas pertence ao perfil da rede, isto não define a autenticidade do usuário, apenas pode diminuir a suspeita sobre ele.

Além destes perfis, pode-se criar outros perfis para comparação de comportamento, como por exemplo, perfis que descrevam situações indesejáveis. Isto é, perfis que contenham a descrição de ações consideradas intrusões, suspeitas de intrusão, ou simplesmente são indesejáveis para aquele ambiente, de acordo com a política local.

O sistema deve empregar, além dos perfis do usuário e da rede, um perfil de situações indesejáveis. O administrador da rede é responsável por construir esse perfil, de acordo com a política de segurança local. Esse perfil é utilizado para detectar acessos do usuário que são ataques conhecidos ou mesmo acessos suspeitos e indesejáveis,

como forma de garantir a integridade da rede. Ele não é utilizado para identificar a legitimidade de um usuário, apenas para determinar se o padrão de uma ação é indesejável.

Uma característica importante do perfil de situações indesejáveis ou de intrusões é que ao invés de armazenar o número de acessos a um destino e serviço, deve ser armazenada a freqüência de acessos a um destino e serviço. Isto se diferencia do perfil do usuário, pois para reconhecimento do usuário é necessário saber o que ele normalmente faz, mas o padrão de conduta do usuário não apresenta a freqüência de acessos a um serviço tão regular quanto um ataque efetivo. Como o perfil de intrusões é utilizado para identificar estas situações, é necessário que utilize-se as informações de freqüência.

3.1.2 Utilização, Construção e Manutenção de Perfis

Inicialmente, os usuários não têm um perfil próprio, de forma que o sistema adota, nestes casos, uma política diferenciada. O sistema não tem como montar um perfil inicial para o usuário sem ter qualquer conhecimento sobre o mesmo. Logo, ao verificar que o usuário é novo, solicita imediatamente uma nova autenticação e então passa a observar o comportamento do usuário para aprender sobre ele e para construir o primeiro perfil. O sistema, neste caso, irá comparar as ações do novo usuário com o perfil de situações indesejáveis para garantir a integridade do ambiente.

Após a primeira utilização do sistema pelo usuário, o sistema utiliza as informações monitoradas para criar o seu perfil. Inicialmente, o sistema passa por um período de adaptação, pois necessitará aprender o suficiente sobre o usuário para ter um maior grau de conhecimento sobre o mesmo.

Os dados coletados durante o uso do sistema pelo usuário são armazenados e, somente se forem considerados válidos para fazer parte do seu perfil, vão ser incluídos no perfil do usuário. Desta forma, o perfil do usuário não é atualizado constantemente, mas a cada período determinado de utilização do sistema. A cada período, o perfil do usuário irá evoluir, pois irá conter mais informações relevantes sobre como o usuário se comporta no sistema.

A periodicidade de manutenção dos perfis definida neste trabalho é diária, sendo que os dados sobre a utilização de cada usuário irão sendo armazenados no sistema de monitoração durante o dia e, uma vez ao dia, são tratados e utilizados para atualizar o perfil do usuário. A periodicidade de manutenção também pode variar de acordo com a política local. Um dos fatores para a definição inicial da manutenção diária é que o servidor LDAP [HAR 03], escolhido para armazenar o perfil neste trabalho, não apresenta um ótimo desempenho para alterações constantes na base de dados. No entanto, apresenta um mecanismo de consulta eficiente.

As informações mantidas no perfil, tanto do usuário quanto da rede, devem retratar o comportamento normal, bem como devem ser atualizadas periodicamente para que se possa acompanhar a evolução do comportamento dos usuários. Um ponto muito importante está relacionado à identificação de comportamentos considerados normais. Neste trabalho, considera-se um comportamento normal para o usuário o conjunto de ações que não definem ações indesejáveis para o sistema, ataques conhecidos ou que sejam consideradas suspeitas e tenham levado ao bloqueio dos serviços para aquele usuário. Se o comportamento do usuário observado não se classifica em uma destas categorias ele é considerado válido e utilizado para realimentar seu perfil.

Os trabalhos na área de detecção de anomalias aplicam, normalmente, procedimentos específicos para minimizar a quantidade de informação que é armazenada nos perfis, principalmente para eliminar dados com erros sintáticos e dados mais ou menos relevantes [COH 95] [HEL 00]. Neste trabalho, as informações são coletadas da rede, diminuindo a possibilidade de erro nas informações do perfil. Por exemplo, um *host* não envia para a rede pacotes com endereços IP, ou endereços de portas de serviço e protocolos sintaticamente errados. Assim, elimina-se a necessidade de utilização de algoritmos para a eliminação de dados errados. Um procedimento necessário seria a identificação de pacotes falsificados com informações sobre protocolos ou serviços fora de escopo, que podem ser forjados por usuários mal intencionados. Mas este procedimento de validação não está sendo considerado e nem implementado neste trabalho.

Os perfis são armazenados em um servidor LDAP, também utilizado para a autenticação dos usuários. A escolha do LDAP deve-se à sua estrutura hierárquica para armazenamento de dados, bem como a possibilidade de integrar vários servidores

LDAP, de forma a criar um sistema de autenticação globalizado, conforme proposto em [MIS 01]. A utilização do LDAP deve-se principalmente a ele ser amplamente utilizado para sistemas de autenticação de usuários e permitir a integração do processo de autenticação com o processo de recuperação do perfil do sistema para a alimentação do sistema de monitoração de usuários. A utilização de outro servidor de autenticação implicaria na possível utilização de outro servidor da banco de dados para armazenamento dos perfis. Enquanto que o LDAP implementa um serviço de diretórios e permite o armazenamento de várias informações e atributos, além de implementar mecanismos de consulta eficientes.

A manutenção do perfil é necessária para que seja possível atualizar o conhecimento sobre as ações do usuário, conforme ele muda seu comportamento. O processo de manutenção envolve a adição, a remoção e também a atualização dos dados já presentes no perfil. O processo de adição permite a inclusão de novas informações ao perfil. O processo de remoção permite que dados "envelhecidos", ou seja, destinos e serviços os quais o usuário não tem mais realizado acesso, sejam retirados do perfil.

O processo de atualização envolve a renovação do número de acessos para destinos e serviços que estão presentes no perfil. O número de acessos será alterado para maior ou menor de acordo com o volume de utilização do usuário. Os destinos e serviços que não forem utilizados pelo usuário serão "envelhecidos", isto significa que, o número de acessos será reduzido de acordo com um fator de envelhecimento. Os destinos e serviços aos quais o usuário realiza o acesso são atualizados, de forma a manter no perfil o maior número de acessos conhecido, isto é, o maior número entre o perfil histórico e o comportamento amostrado.

O processo de manutenção, em especial relacionado à atualização do número de acessos existentes, deve ser cuidadosamente planejado, pois o fator de envelhecimento utilizado irá determinar o período de validade das informações no perfil. Assim, se o usuário deseja manter no perfil os dados sobre as atividades durante um mês, o fator de envelhecimento tem de ser compatível com este período. Por exemplo, se o fator de atualização for 0.2, os dados tem um período de vida curto, pois o número de acessos é reduzido em 80% a cada dia, para aqueles destinos não utilizados. O intervalo de valores do fator de envelhecimento varia entre [0,1]. Quanto mais próximo de zero este fator se encontra, mais rápida é alteração do perfil para destinos e serviços que o usuário

utiliza como menor freqüência. E quanto mais próximo de um se encontrar, mais lenta é alteração dos valores do perfil.

O sistema utiliza um valor padrão de 0.9 para o envelhecimento, pois a cada dia serão diminuídos apenas 10% do valor do número de acessos para destinos e serviços que não têm sido utilizados. Esse percentual só fará sentido em relação ao tempo, se a amplitude por destinos e serviços for ajustada para a mesma faixa de valores para todos os elementos do perfil. Assim pode-se estimar que todos os valores terão o mesmo período de validade. Caso não ocorra este ajuste, o período de validade das informações depende do valor do número de acessos, ou seja, quanto maior o número de acessos, maior o tempo de validade. Por exemplo, se o número de acessos a um destino e serviço for 10, utilizando-se o fator de envelhecimento de 0.9, a informação permanecerá no perfil por um período inferior a 10 dias. Enquanto que se o número de acessos for de 100, a informação permanecerá pelo dobro do tempo no perfil.

3.1.3 Coleta de Dados

A observação destes valores é feita através de um monitor de rede que captura o tráfego do segmento e monta uma matriz de tráfego, baseada na tabela *alMatrixTable* da RMON II [STA 99]. O monitor é alimentado por um agente SNMP que monitora os usuários que executaram o processo de autenticação, e automaticamente configura o monitor, provendo o endereço IP do dispositivo associado ao usuário e iniciando a análise dos dados para o IP fornecido. Neste momento o monitor de tráfego (*sniffer*) passa a capturar da rede todos os pacotes referentes ao IP do usuário.

É importante observar que não é utilizado um agente que implementa a RMON, mas sim que utiliza-se a idéia da matriz de tráfego que existe nesta MIB. O agente que captura os dados e os organiza na matriz não é o responsável pela identificação dos processos de *loggin* ou *logout* do usuário.

Quando um usuário executa o processo de *logout*, ou permanece por um período inativo, o agente SNMP deve sinalizar o monitor, que encerra a captura e análise de dados para aquele endereço. Uma dificuldade neste caso está associada ao processo de *logout* do usuário, pois ele nem sempre ocorre. Então é necessário monitorar o usuário de outras formas para perceber sua saída da rede. Uma das formas é monitorando a alocação dos endereços IP no servidor de endereços, por exemplo, um DHCP. Neste

servidor, os endereços são associados aos endereços MAC dos dispositivos da rede e periodicamente há o processo de renovação dessas associações, para identificar quais endereços ainda estão ativos. Através da monitoração destas operações pode-se identificar estações que não estão mais presentes no ambiente e então desativar a monitoração para um IP associado a um usuário.

Em relação a esta abordagem, existe um problema principal: o tamanho do intervalo de tempo entre as atualizações de endereços. Se o intervalo for muito grande o sistema poderia ser ludibriado por outro usuário que assume o mesmo endereço IP do dispositivo anterior.

3.1.4 Formalização do Perfil

O perfil contém o número de acessos a cada destino e serviço. Formalmente ele é descrito como um vetor que contém 2^T posições, onde $T \in N$, e $T = 2^{56}$. O *iésimo* elemento do vetor representa o número de acessos a um endereço IP destino, $IP \in [0, 2^{32}–1]$, a uma porta $P \in [0, 2^{16}\text{-}1]$ e um protocolo $p \in [0, 2^8–1]$. Esse elemento é indexado por:

$$i = IP * 2^{24} + P * 2^8 + p$$

Então, os vetores de perfil são genericamente representados como:

$$V = (a_1, a_2, ..., a_T)$$

Conforme definido anteriormente, utiliza-se dois vetores de perfil, um para o histórico do usuário, denominado PH, e um para o perfil da rede, denominado PR. Além desses, também são utilizados os seguintes vetores pelo sistema de detecção proposto:

- Perfil local histórico, denominado PLH, no qual são armazenadas as informações coletadas enquanto observa-se as atividades do usuário na rede e que coincidem com o perfil histórico do usuário;
- Perfil local da rede, denominado PLR, no qual são armazenadas as informações coletadas enquanto observa-se as atividades do usuário na rede e que coincidem com o perfil histórico da rede;

- Perfil de acessos desconhecidos, denominado O, no qual são armazenadas as informações coletadas que não coincidem nem com o perfil do usuário, nem com o perfil da rede, ou seja, são desconhecidas;

Assim sendo, os perfis são representados na forma genérica como:

$$PH = (a_1, a_2, a_3, \mathrm{K} , a_T)$$

$$PR = (a_1, a_2, a_3, \mathrm{K} , a_T)$$

$$PLH = (a_1, a_2, a_3, \mathrm{K} , a_T)$$

$$PLR = (a_1, a_2, a_3, \mathrm{K} , a_T)$$

$$O = (a_1, a_2, a_3, \mathrm{K} , a_T)$$

A representação por vetores foi escolhida por apresentar maior facilidade para representação das operações a serem realizadas. A utilização formal de um vetor de 2^T posições facilita a visualização da ordenação e também a realização das operações entre vetores, garantindo que a posição a_i tem os mesmos valores da tupla *< IP, Porta, Protocolo>* para todos os vetores.

A implementação prática destas estruturas não exige a utilização de vetores de 2^T posições, pois em primeiro lugar eles consumiriam uma grande quantidade de memória e não seriam passíveis de utilização para a observação de um conjunto de usuários. Em segundo lugar, mesmo que se deseje armazenar o comportamento do usuário, resultante de vários dias de observação, as 2^T posições não seriam utilizadas, pois dificilmente o usuário irá fazer acesso a todas as combinações de endereços e serviços possíveis.

Então resumindo, formalmente define-se um vetor de 2^T, mas na prática pode-se implementar uma estrutura de dados adequada às necessidades da aplicação, mantendo a características da definição formal.

3.1.5 Exemplos de Perfis

O perfil histórico do usuário é construído a partir da monitoração do próprio usuário ao longo do tempo. Nas primeiras monitorações, pouco se sabe a respeito do usuário, porém, após o período inicial de monitoração, já é possível identificar atividades características do usuário. Mas o processo de construção do perfil é contínuo, pois o usuário pode alterar constantemente o seu comportamento. Essa alteração pode ser motivada por inúmeros fatores, entre eles a diversidade de serviços existentes na Internet atualmente.

Um exemplo de construção do perfil e de observação do comportamento do usuário ao longo do tempo é apresentado a seguir. A tabela 1 mostra as informações referentes a um dia de monitoração de um usuário. As informações foram armazenadas no seu perfil e serão utilizadas como seu histórico para comparação de seu comportamento quando ele estiver novamente conectado à rede. O perfil em questão apresenta um conjunto parcial de entradas de forma a minimizar no texto sua apresentação.

Tabela 1 – Perfil Histórico do Usuário

	IP Destino	Porta Destino	Protocolo	No. Acessos
1	192.168.100.2	80	TCP	40
2	192.168.100.3	25	TCP	35
3	www.inf.pucrs.br	80	TCP	50
4	www.cnn.com	80	TCP	120
5	www.google.com	80	TCP	89
6	www.banrisul.com.br	80	TCP	60
7	www.pucrs.br	80	TCP	20
8	www.pocket.com	80	TCP	20
9	www.bluetooth.com	80	TCP	50
10	www.bancodobrasil.com.br	80	TCP	100
11	verum.pucrs.br	4040	TCP	67

Conforme descrito anteriormente, além do perfil histórico do usuário, também é construído o perfil histórico da rede, o qual armazena os acessos feitos por todos os usuários que estiveram ativos na rede. A tabela 2 apresenta o perfil da rede após um dia de monitoração. Da mesma forma, a tabela apresentada contém informações parciais para minimizar a apresentação da mesma no texto.

Tabela 2 – Perfil Histórico da Rede

	IP Destino	Porta Destino	Protocolo	No. Acessos
1	192.168.100.2	80	TCP	120
2	192.168.100.3	25	TCP	105
3	www.inf.pucrs.br	80	TCP	150
4	www.cnn.com	80	TCP	360
5	www.google.com	80	TCP	267
6	www.banrisul.com.br	80	TCP	180
7	www.pucrs.br	80	TCP	60
8	www.pocket.com	80	TCP	60
9	www.bluetooth.com	80	TCP	150
10	www.bancodobrasil.com.br	80	TCP	300
11	verum.pucrs.br	4040	TCP	201
12	www.hp.com	80	TCP	120
13	wacken.inf.pucrs.br	22	TCP	12
14	limnos.inf.pucrs.br	21	TCP	7
15	192.168.100.45	21	TCP	11
16	192.168.100.31	761	UDP	69
17	www.3com.com	80	TCP	12
18	192.168.100.69	21	TCP	62

Após o período da primeira monitoração, o usuário volta à atividade na rede, sendo que o seu perfil monitorado nesse período é apresentado na tabela 3. A comparação entre os perfis é realizada através do cálculo da média e do desvio padrão, para medir a proximidade entre os comportamentos.

Tabela 3 – Perfil Histórico do Usuário no 2o. Dia de monitoração

	IP Destino	Porta Destino	Protocolo	No. Acessos
1	192.168.100.2	80	TCP	10
2	192.168.100.3	25	TCP	16
3	www.inf.pucrs.br	80	TCP	0
4	www.cnn.com	80	TCP	30
5	www.google.com	80	TCP	51
6	www.banrisul.com.br	80	TCP	0
7	www.pucrs.br	80	TCP	0
8	www.pocket.com	80	TCP	0
9	www.bluetooth.com	80	TCP	10
10	www.bancodobrasil.com.br	80	TCP	15
11	verum.pucrs.br	4040	TCP	0
12	www.linux.org	80	TCP	24
13	muster.inf.pucrs.br	22	TCP	23
14	samos.inf.pucrs.br	21	TCP	3
15	192.168.100.69	21	TCP	17

Pode-se observar a similaridade entre os comportamentos comparando quantas atividades coincidiram com o seu perfil histórico ou com o da rede e quantas são desconhecidas. A figura 1 apresenta um gráfico que permite visualizar o número de

acessos presentes no perfil histórico e o número de acessos a esses destinos feitos no segundo período de atividade do usuário.

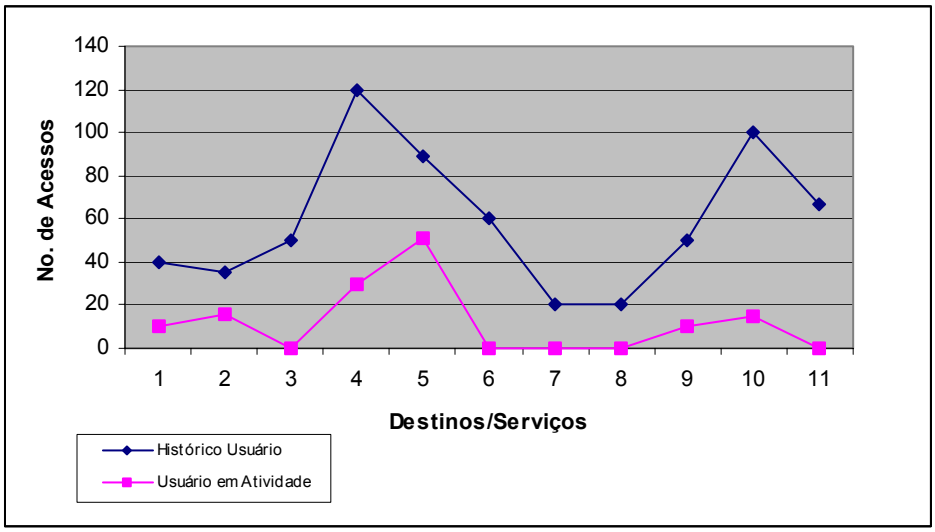


Figura 1 – Comparação do perfil histórico com o comportamento do 2º dia.

Neste exemplo, pode-se verificar que o comportamento observado tende ao comportamento do histórico do usuário. Enquanto que, se comparado o comportamento do usuário em relação ao perfil da rede, excluindo-se os destinos e serviços do seu perfil histórico, o usuário acessa em comum com os demais usuários da rede o destino 192.168.100.69 na porta 21. Neste caso, pode-se observar que o comportamento do usuário é similar ao seu comportamento histórico, bem como, está dentro do comportamento conhecido da rede.

A análise completa-se com a observação do número de destinos e serviços que eram desconhecidos. Se forem observados os destinos ainda não conhecidos, temos um total de seis destinos desconhecidos. Isto poderá fazer com que o grau de desconfiança sobre o usuário cresça. Se no segundo dia o usuário ainda é bastante desconhecido para o sistema, será executada alguma ação preventiva para certificar-se da identidade do usuário. Futuramente, o sistema já haverá incorporado essas informações ao perfil histórico do usuário e da rede.

No caso de ocorrências de desvio de comportamento em relação ao perfil histórico, pode-se observar duas situações:

- O número de acessos a um destino conhecido supera o valor do contido no perfil. Ainda neste caso, há duas situações possíveis:

- O número de acessos a um único destino excede o número de acessos do perfil; e,
- O número de acessos aos demais destinos é muito baixo ou não existe, apresentado na figura 2.

- O número de acessos aos destinos é similar ao perfil, mas excede o número conhecido, figura 3.

Em ambos os casos, haverá um desvio de conduta, e o sistema deverá agir de forma a ter maior certeza sobre a identidade do usuário.

O segundo caso do desvio de comportamento observado é aquele em que o desconhecimento sobre as ações do usuário é alto, isto é, os acessos que ele está executando não constam de seu perfil ou do perfil da rede.

Essas informações utilizadas como exemplo, foram obtidas a partir da monitoração da rede real, mas sintetizadas apenas para uso como exemplo.

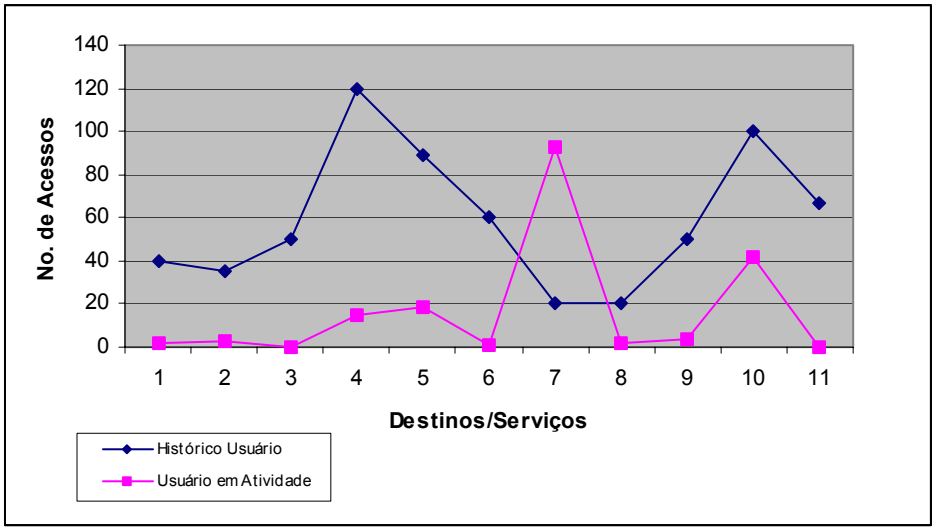


Figura 2 – Número de acesso a um destino específico excedente

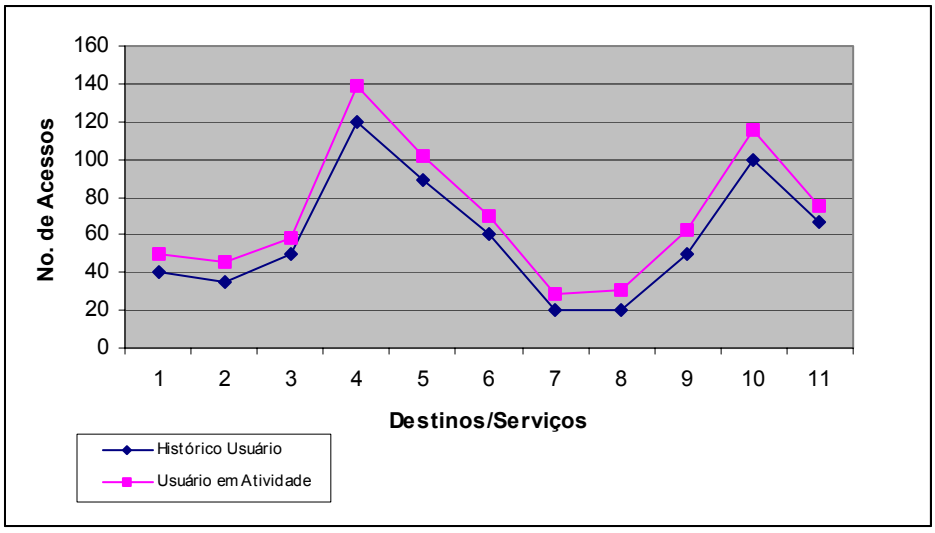


Figura 3 – Número de acesso superam o perfil do usuário

3.2 Medidas Utilizadas no Método Estatístico

As medidas estatísticas são utilizadas para a detecção de desvios de comportamento do usuário. As principais medidas utilizadas são a média, o desvio padrão e o grau de desconhecimento, este último proposto neste trabalho. Essas medidas são analisadas, observando a tendência de comportamento de um usuário ao longo do tempo, ao invés da observação em momentos estanques no tempo.

As medidas utilizadas são combinadas a um sistema de regras que permite a execução da análise de seus valores e de suas tendências de comportamento. A utilização de um sistema de regras agrega a vantagem da utilização de políticas para definição das ações, ou seja, contramedidas a serem executadas em casos de suspeição e/ou detecção real de usuários não legítimos.

A seguir são apresentadas as medidas utilizadas, a forma de análise das mesmas através de sistemas de regras e o sistema baseado em políticas para a especificação das contramedidas.

3.2.1 Grau de Desconhecimento

O grau de desconhecimento é a medida utilizada para determinar o quão diferente, ou seja, desconhecido é o comportamento do usuário, de acordo com o seu perfil e o perfil da rede.

Os acessos realizados pelos usuários são contabilizados como pertencentes ao perfil histórico do usuário, ao perfil da rede ou como desconhecidos. Os acessos desconhecidos são armazenados no vetor O, enquanto que os demais são armazenados no PLH ou no PLR.

O grau de desconhecimento é calculado por

$$D = \frac{\sum_{i=1}^{T} O_i}{\sum_{i=1}^{T} PLH_i + \sum_{i=1}^{T} PLR_i + \sum_{i=1}^{T} O_i}$$

onde D assume valores no intervalo de [0;1]. Quanto mais próximo de 1, maior é o grau de desconhecimento em relação às atividades do usuário. E quanto mais próximo de 0, menor é o grau de desconhecimento.

Essa medida, por ser utilizada como uma medida específica para o sistema, é capaz de determinar uma política de ação independente do valor de outras medidas, como média e desvio padrão. Por exemplo, se o grau de desconhecimento é alto, isso pode determinar a execução de ações como solicitação de novas senhas, bloqueio de serviço, etc. Entretanto essa medida também pode ser utilizada em um sistema de regras *fuzzy*, sendo utilizada junto com as demais variáveis para determinar o grau de suspeição. Nesse caso, o valor elevado do grau de desconhecimento seria refletido por um peso alto no sistema *fuzzy,* contribuindo decisivamente na definição da política a ser adotada.

O grau de desconhecimento sobre as atividades do usuário irá elevar-se no momento em que o usuário faz alterações no seu comportamento, ou em casos de uso indevido da identificação de um usuário por usuários intrusos. Por exemplo, em um sistema de telefonia celular, o grau de desconhecimento seria alto para telefones clonados, pois a probabilidade das ligações do usuário original e do usuário clonado serem similares é muito baixa. [BUS 02]

No caso de alterações de comportamento do usuário legítimo, o grau de desconhecimento será alto e irá disparar ações como solicitação de novas senhas. Se o usuário for realmente legítimo ele será capaz de responder à solicitação do sistema seja qual for. Uma vez que a reposta é válida, o sistema continua permitindo que o usuário

utilize os recursos disponíveis. As alterações de comportamento serão posteriormente registradas no perfil, no momento de sua atualização e, em um próximo acesso, essas ações já não serão desconhecidas para o sistema. Em caso de insucesso da verificação, o serviço será bloqueado e as ações monitoradas não serão utilizadas para a atualização do perfil e, nestas situações, são executadas contramedidas como bloqueio dos serviços e alarmes de acordo com a política de segurança local.

3.2.2 Classificação de Usuário

Uma informação adicional que pode ser extraída a partir da fórmula do grau de desconhecimento é a identificação do comportamento do usuário com um dos três perfis, pela proximidade de seu comportamento com um deles.

O cálculo extraído do grau de desconhecimento permite calcular o grau de proximidade do perfil histórico da seguinte forma:

$$SH = \frac{\sum_{i=1}^{T} PLH_i}{\sum_{i=1}^{T} PLH_i + \sum_{i=1}^{T} PLR_i + \sum_{i=1}^{T} O_i}$$

A proximidade do perfil da rede pode ser calculada de forma similar, apenas alterando a parcela de dividendo pelo somatório de PLR, conforme apresentado abaixo:

$$SR = \frac{\sum_{i=1}^{T} PLR_i}{\sum_{i=1}^{T} PLH_i + \sum_{i=1}^{T} PLR_i + \sum_{i=1}^{T} O_i}$$

É importante observar que, caso um usuário faça um número de acessos a um destino e serviço superior ao número de acessos de seu perfil histórico, ou mesmo do perfil da rede, ainda assim a similaridade não é afetada. Isto é, apesar de exceder o número de acessos, ele está utilizando destinos e serviços contidos nestes perfis. Outras medidas irão determinar se ele excedeu ou não este número, e de acordo com as contramedidas, a legitimidade do usuário será comprovada ou não. Assim, essa classificação ajuda a identificar quando usuários com um comportamento similar a um ou outro perfil, ou a ambos, são ou não usuários legítimos.

3.2.3 Medidas Estatísticas Utilizadas no Sistema

Média e desvio padrão são as medidas estatísticas escolhidas para este trabalho a fim de detectar variações de comportamento. Outras medidas foram estudadas como correlação numérica, distribuição normal e outras, mas não apresentaram resultados expressivos e torna mais complexa a modelagem. Então, com o objetivo de manter o sistema simples e eficiente, optou-se pela utilização apenas da média e do desvio padrão. Segundo [YE 02], esta escolha é justificável, pois as intrusões manifestam-se principalmente por variações de média e desvio padrão, devendo estas medidas ser suficientes para a detecção de variações do comportamento dos usuários.

Resumidamente, o método empregado calcula a média e o desvio padrão em relação à diferença de acessos entre o perfil histórico e o perfil atual, ou seja, em função da amplitude entre os perfis. O cálculo destas medidas permitiu observar que elas não são medidas estanques no tempo e devem ser observadas ao longo deste, para que se observe a tendência de crescimento ou decrescimento. Em uma situação de comportamento normal, observa-se que média e desvio padrão devem tender a zero, ou seja, a tendência é que as medidas decresçam, conforme a utilização de um usuário legítimo. Quando essas medidas apresentam a tendência de crescimento, então poderá estar ocorrendo uma situação de intrusão, ou seja, o comportamento de um usuário desvia-se de seu comportamento habitual, o que eleva o nível de suspeição sobre sua legitimidade.

3.2.3.1 Amplitude

A comparação entre os perfis do usuário e da rede com as ações observadas, ou seja, é feita através comparação entre o número de acessos de cada perfil. Inicialmente, o perfil local do usuário não contém acessos a qualquer destino e serviço. Conforme o usuário tem acessos aos serviços e utiliza serviços contidos no seu perfil ou no perfil da rede, o número de acessos do perfil local aumenta, e diminui a amplitude entre perfil histórico e perfil local, conforme demonstrado nas figuras 4 e 5.

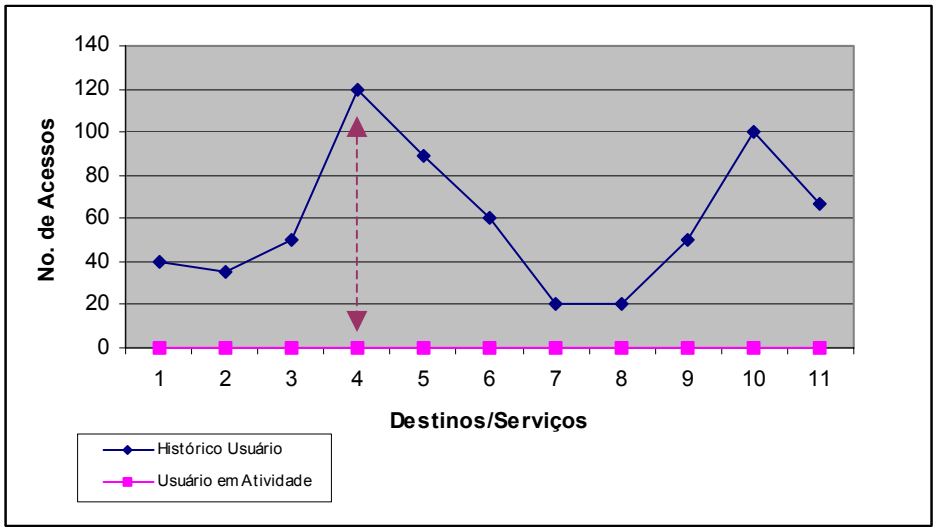


Figura 4- Perfil local na inicialização

A figura 4 apresenta a visualização do perfil histórico do usuário e o perfil local do usuário. Neste caso, obtém-se a amplitude máxima entre os vetores, pois o perfil local não contém nenhum acesso. A figura 5 apresenta a visualização do perfil histórico do usuário e do perfil local no momento em que o usuário já fez um conjunto de acessos a destinos e serviços contidos no perfil histórico. Neste caso, pode-se observar que a amplitude entre os vetores é menor. Conforme o usuário reproduz seu comportamento habitual, a tendência é que a amplitude diminua.

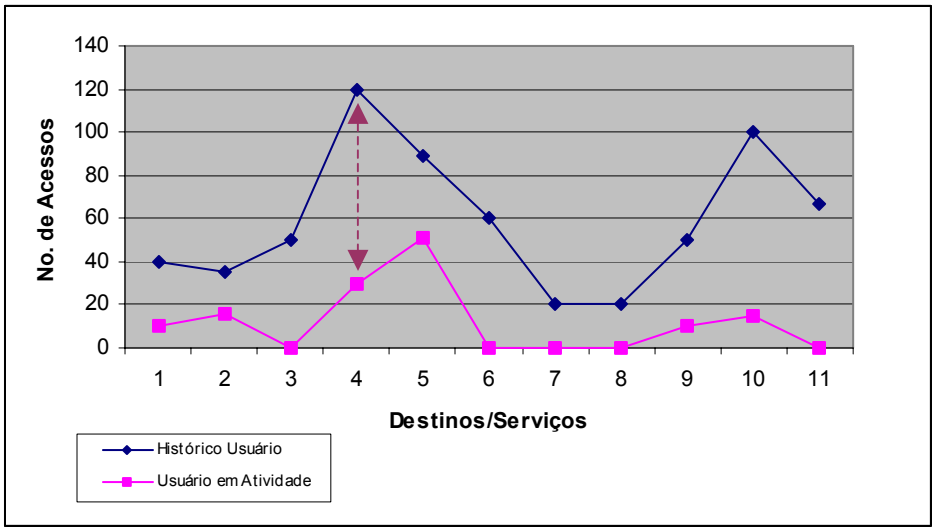


Figura 5 – Perfil local com usuário em atividade

A amplitude entre o perfil histórico do usuário e o perfil local do usuário é definida como:

$$AH = (\,|\,PH_1 - PLH_1\,|, |\,PH_2 - PLH_2\,|, \mathrm{K}\,, |\,PH_T - PLH_T\,|\,)$$

E a amplitude entre o perfil da rede e o perfil local do usuário é definida como:

$$AR = (\,|\,PR_1 - PLR_1\,|, |\,PR_2 - PLR_2\,|, \mathrm{K}\,, |\,PR_T - PLR_T\,|\,)$$

Os valores da amplitude são valores absolutos porque esta é uma medida mais estável do que a utilização de valores positivos e negativos. A utilização de valores polarizados pode ser interessante para determinar se o número de acessos observado é menor ou maior do que o número de acessos do perfil, para cada destino e serviço individualmente. Mas sua utilização torna os valores de média e desvio mais instáveis para a observação dos seus comportamentos e, neste trabalho, optou-se pela utilização do valor absoluto por considerar-se que torna o sistema mais simples.

A amplitude é utilizada para o cálculo da média e do desvio padrão, os quais apresentam o mesmo comportamento da amplitude conforme cresce o número de acessos.

No caso apresentado na figura 4, a média e o desvio padrão calculados são os valores de referência para média e desvio em relação ao comportamento conhecido do usuário, pois são calculados com a amplitude máxima do perfil histórico.

A amplitude foi escolhida como medida para cálculo da média e do desvio, pois, conforme aumenta ou diminui, ela faz com que a média e o desvio aumentem ou diminuam. Por exemplo, observando-se as figuras 4 e 5 vê-se que, conforme o usuário faz acessos a destinos e serviços do seu perfil, a amplitude entre o perfil histórico e o perfil local diminui.

É importante observar que a amplitude tende a zero enquanto o número de acessos é menor ou igual aos acessos registrados no perfil histórico. Caso o usuário permaneça por longo tempo na rede ou tenha uma atividade mais intensa do que o normal registrado no seu perfil, a tendência é que o número de acessos ultrapasse o número de acessos do perfil fazendo com que a amplitude cresça. Se o usuário mantém um comportamento coerente, a média e o desvio, que atingiram o valor zero, voltam a

crescer e podem atingir os valores de referência iniciais, conforme apresentado na figura 6.

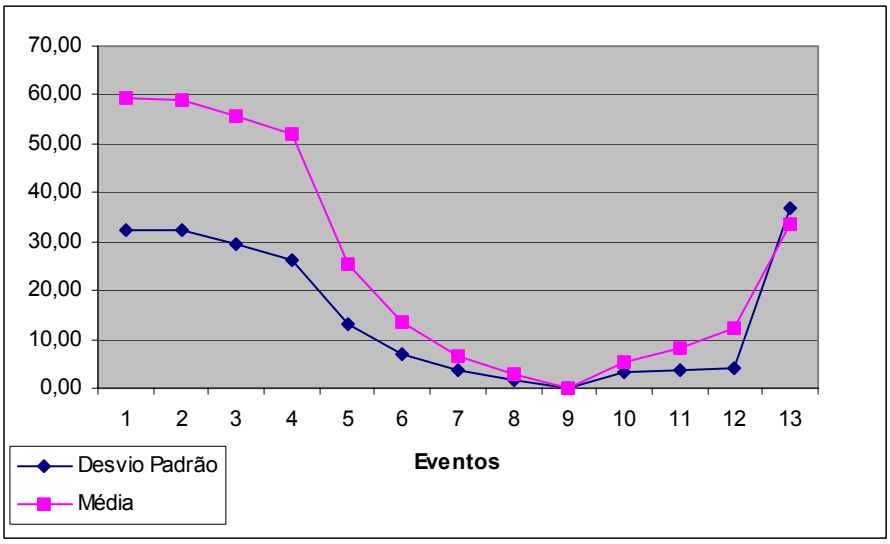


Figura 6 – Comportamento de média e desvio padrão

A figura 6 apresenta um gráfico demonstrativo do comportamento da média e do desvio padrão. Inicialmente uma curva descendente até atingir o valor zero, quando o número de acessos dos perfis se iguala. A seguir as medidas voltam a crescer, no momento em que o número de acessos ultrapassa os valores do perfil histórico.

No entanto, não é possível afirmar que, nestas situações, o usuário não é legítimo, pois ele apenas excede o seu comportamento normal. A questão relacionada a isto é: Até quando se considera o crescimento da média como normal e não se executa qualquer contramedida?

Uma das soluções que se aplica é o acompanhamento do número de incrementos que o desvio sofre e o controle da distância do valor do desvio em relação ao desvio de referência. A cada *n* incrementos sucessivos o sistema pode adotar as contramedidas especificadas de acordo com a política local, ou no caso do desvio distanciar-se k vezes, também se executa uma contramedida. Essa solução é simples, mas tem de ser bem coordenada para que o sistema não execute contramedidas simultâneas em decorrência da satisfação das condições simultaneamente.

A outra solução possível é a observação dos valores de média e desvio através de um sistema *fuzzy*, que é discutido no capítulo 4.

Uma situação especial a ser controlada é quando o número de acessos do usuário supera o número de acessos do seu perfil, mas de forma não coerente, elevando o grau de suspeição sobre sua legitimidade e também sobre suas intenções. A figura 2 do capítulo 3 apresenta uma situação em que o usuário excede o número de acessos a um destino e serviço que faz parte do seu perfil histórico. Nestas situações, claramente observa-se um desvio de comportamento. O desvio pode ser ocasionado por diversos fatores, entre eles a intenção maliciosa do usuário ou simplesmente uma real necessidade de utilização do recurso por parte do usuário. Nesta situação, a amplitude total, $\sum AH$ ou $\sum AR$, pode diminuir, pois o número total de acessos do perfil local ainda poderá ser menor que o número total de acessos do perfil histórico. Em conseqüência, a média poderá diminuir também, mas o desvio padrão, em qualquer caso, irá apresentar um valor superior ao valor inicial, sendo possível então verificar a ocorrência de um desvio de comportamento. O desvio não deve ser observado sozinho, mas em conjunto com a média, pois a situação característica do desvio de comportamento é a diferença no comportamento da média e do desvio, além de seus valores efetivos. Quando o comportamento é normal, as duas medidas tendem a decrescer ou mesmo crescer juntas.

3.2.3.2 Média e Desvio

A média e o desvio padrão são calculados utilizando-se um valor normalizado para a amplitude. Isto é necessário, pois o valor da amplitude varia de acordo os valores de cada perfil. Assim sendo, para considerar que a amplitude é alta, baixa ou média é preciso conhecer os valores reais de cada perfil e ajustá-la a cada intervalo. Uma forma de contornar essa relatividade é normalizar a amplitude da seguinte forma:

$$NH = \frac{\sum_{i=1}^{T} AH_i}{\sum_{i=0}^{T} PH_i}$$

Da mesma forma ocorre para a amplitude em relação ao perfil da rede, onde se considera apenas o uso de AR e PR. A média é calculada como segue:

$$NR = \frac{\sum_{i=1}^{T} AR_i}{\sum_{i=0}^{T} PR_i}$$

Neste trabalho as medidas de média e desvio são calculadas em função da amplitude absoluta, pois não é necessário fazer a comparação entre usuários e, portanto, não é necessário que as amplitudes estejam no mesmo intervalo de valores.

A média do perfil histórico do usuário é calculada por:

$$\overline{X}_H = \frac{\sum_{i=1}^{T} AH_i}{Nz(PH)}$$

A média do perfil da rede é calculada de forma similar à média do perfil histórico do usuário, substituindo-se os valores adequados, conforme apresentado abaixo:

$$\overline{X}_R = \frac{\sum_{i=1}^{T} AR_i}{Nz(PR)}$$

Uma vez que o vetor de T posições é oneroso para a implementação, e na realidade terá uma grande quantidade de zeros, não sendo necessário implementá-lo como tal, define-se o operador E(V,i) com $V \in \mathrm{N}^{\mathrm{T}}$ e $i \in \mathrm{N}$ como:

$$E(V,i) = \begin{cases} 0, V_i = 0 \\ 1, V_i \neq 0 \end{cases}$$

E então, o número de elementos ≠ 0 em um vetor V pode ser definido como:

$$Nz(V) = \sum_{i=1}^{T} E(V,i)$$

O desvio padrão em relação ao perfil histórico do usuário é definido como:

$$\sigma_H = \frac{\sum_{i=1}^{T} (AH - \overline{X}_H)^2}{Nz(PH)}$$

O desvio padrão em relação ao perfil da rede é definido de forma similar, apenas com a substituição dos valores adequadamente, conforme apresentado abaixo:

$$\sigma_R = \frac{\sum_{i=1}^{T} (AR - \overline{X}_R)^2}{Nz(PR)}$$

A variação da média e do desvio padrão indica as variações de comportamento do usuário, conforme discutido anteriormente. As medidas de média e desvio padrão, se observadas de forma estanque, refletem apenas se o usuário está abaixo ou acima da média e do desvio padrão de referência. Mas se observadas seqüencialmente a cada ação do usuário, elas definem a tendência de comportamento, ou seja, mostram se a média e o desvio padrão estão crescendo ou decrescendo continuamente. Essa forma de observação das medidas de média e desvio padrão permite determinar a tendência de comportamento do usuário ao longo do tempo, estabelecendo uma relação entre as medidas amostradas.

Os valores de média e desvio padrão crescem ou decrescem de forma independente, ou seja, eles não seguem necessariamente o mesmo comportamento simultaneamente. Na tabela 4, observa-se a combinação destas duas medidas e os estados de acréscimo ou decréscimo dos valores.

As combinações dos valores apresentam casos em que o usuário pode ser suspeito, casos em que ele é suspeito, e casos em que ele pode não ser suspeito, de acordo com as variações da média e do desvio padrão. Nos casos em que média e desvio crescem, o usuário poderá vir a ser suspeito se o número de incrementos sucessivos destas medidas ultrapassar um limite considerado seguro, ou se os incrementos levam essas medidas a ultrapassar os limites de valores de média e desvio considerados seguros. Enquanto eles não alcançam uma das duas condições, o sistema apenas dá continuidade à monitoração das atividades do usuário.

No caso em que média e desvio apresentam comportamentos diferentes, considera-se que o usuário é suspeito. No primeiro caso, a média cresce e o desvio decresce. Esta situação é matematicamente possível, mas não é observada na prática. Se ocorrer o usuário é considerado suspeito. No segundo caso, a média decresce e o desvio decresce. Esta situação é matematicamente possível, mas não é observada na prática. Se

ocorrer o usuário é considerado suspeito. No segundo caso, a média decresce e o desvio cresce. Nesta situação o usuário é considerado suspeito, pois este tipo de comportamento reflete situações em que o usuário está tendo acesso mais intenso a um único serviço do perfil. No entanto, se contabilizarmos o número total de acessos do perfil local, ele ainda poderá ser menor que o total de número total de acessos do perfil do usuário.

Tabela 4 - Combinação de estados de média e desvio padrão

Média	Desvio Padrão	Comentários
Cresce	Cresce	Usuário pode ser suspeito
Cresce	Decresce	Normalmente não ocorre
Decresce	Cresce	Usuário pode ser suspeito
Decresce	Decresce	Usuário pode não ser suspeito

No caso em que média e desvio decrescem, o usuário poderá ser considerado não suspeito se ocorrerem um número de decrementos sucessivos ou se, após o decremento, os valores de média e desvio são menores que os valores de referência. Logo, deverão ser determinados os valores para os limites de incrementos e decrementos sucessivos a serem controlados pelo sistema. Esses valores são dependentes de cada política de segurança adotada, ou seja, um grau de controle adotado forte, médio ou brando.

O diagrama de estados da figura 7 mostra os estados que um usuário assume no sistema, e as transições entre estes estados de acordo com as variações de média e desvio padrão.

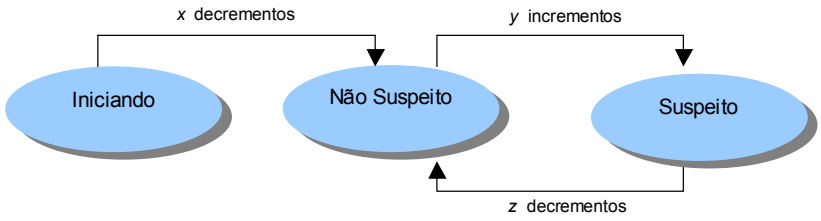


Figura 7 – Diagrama de estados: Variação da média e do desvio padrão

Neste diagrama não foram considerados os valores da média e do desvio padrão, apenas o comportamento dessas medidas conforme apresentado na tabela 4.

Pela observação do comportamento do desvio padrão e da média, verifica-se ainda que a tendência do desvio padrão é crescer quando o usuário faz acessos a destinos e serviços que têm o número de acessos menor que o valor da média. Se a tendência do usuário for de utilizar estes destinos e serviços mais do que àqueles que estão acima da média ver-se-á o crescimento do desvio padrão. Se o usuário utilizar todos os destinos ou utilizar aqueles com número de acessos acima da média, a tendência do desvio é decrescer.

3.2.4 Testes com Perfis e Validação das Medidas

Os testes foram realizados para validar a medida de grau de desconhecimento, de média e de desvio padrão, e as variáveis que constituem o perfil.

Os testes foram executados em duas fases distintas:

- 1ª. Fase: coleta de dados a respeito do comportamento do usuário;
- 2ª. Fase: cálculo e análise das medidas.

Os testes foram realizados com 20 usuários que utilizaram suas próprias credenciais, e também as credenciais de outros usuários para observação da similaridade entre os comportamentos.

A fase de coleta de dados consiste da monitoração das ações de um usuário através da coleta de informações da rede. As amostras de tráfego foram coletadas na rede utilizando o software *tcpdump* [TCP 02]. Essas amostras foram realizadas no laboratório do projeto CPSE (Centro de Pesquisa em Software Embarcado) e CPTS (Centro de Pesquisa em Teste de Software) do Convênio HP/PUC, pois nesta rede cada usuário possui uma estação de trabalho individual e com endereço IP fixo, facilitando a identificação de cada usuário. Os dados foram coletados diariamente, no período de maior atividade dos laboratórios, entre 8:00 e 17:35, por um período de duas semanas.

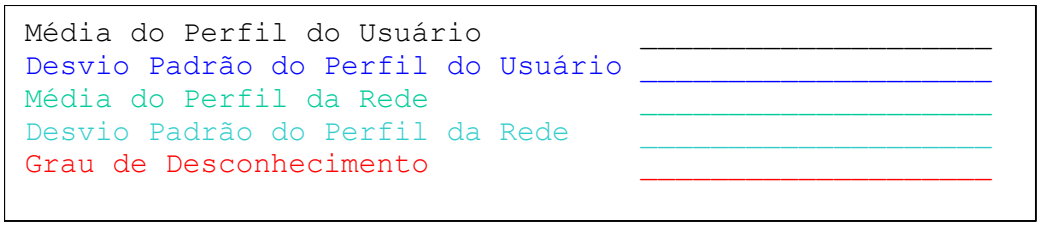
A segunda fase consistiu da análise dos dados coletados e submetidos ao sistema para cálculo das medidas de média, desvio padrão e grau de desconhecimento. O que se observou foi a comprovação, na prática, do comportamento teórico dessas medidas. As

informações de cada usuário foram analisadas de forma individual, ou seja, os dados foram processados em *off-line,* um usuário de cada vez.

O sistema cria inicialmente uma matriz de tráfego para registrar cada nova conexão entre um determinado fonte e destino, o que representa um novo acesso a um destino e serviço. Quando é registrada uma nova entrada na matriz de tráfego, os cálculos de média, desvio e grau de desconhecimento são realizados. Os dados da nova entrada são então comparados em primeira instância com os dados do perfil histórico do usuário. Se pertencerem a este perfil, ou seja, é um acesso comum ao comportamento do usuário, serão recalculados a média e o desvio padrão em relação ao perfil histórico do usuário. Se não pertencerem, os dados são comparados com o perfil histórico da rede, e em caso afirmativo, serão recalculados a média e o desvio padrão em relação ao perfil histórico da rede.

Quanto ao cálculo do grau de desconhecimento, ele é realizado em qualquer situação, mesmo que o dados pertençam ou não ao perfil histórico do usuário ou da rede, pois ele expressa o quão desconhecido é o comportamento do usuário local em relação aos outros acessos executados pelo usuário historicamente.

Os comportamentos de alguns dos usuários monitorados serão apresentados e comentados a seguir, para que se possa avaliar o comportamento das medidas discutidas até o momento. Nos gráficos apresentados a seguir, o eixo Y representa os valores da média e do desvio padrão; e o eixo X representa o número de acessos total do usuário ao longo do tempo. Para melhor compreensão dos dados, a legenda que é utilizada nos gráficos é apresentada abaixo:



3.2.4.1 Dados do Primeiro Usuário Monitorado

Inicialmente, os perfis de usuários estão vazios e o perfil da rede contém um conjunto de informações mínimo. Os resultados das monitorações diárias são utilizados para alimentar tanto o perfil de cada usuário, quanto o perfil da rede. Logo, na análise

do primeiro dia de monitoração o resultado é um alto grau de desconhecimento do usuário, podendo ainda haver alguma variação da média e do desvio padrão da rede para acessos do usuário. A figura 8 apresenta esta situação.

Antes de analisar os gráficos, é importante observar que a medida de grau de desconhecimento está em uma escala relativa, pois ela varia entre [0,1], não sendo possível visualizá-la se mantida a escala normal. O valor 1 para grau de desconhecimento representa o maior valor calculado para o eixo Y, que irá variar de acordo com os valores de média e desvio padrão. Para uma melhor compreensão, os mesmos gráficos são apresentados no Anexo A em escala logarítmica.

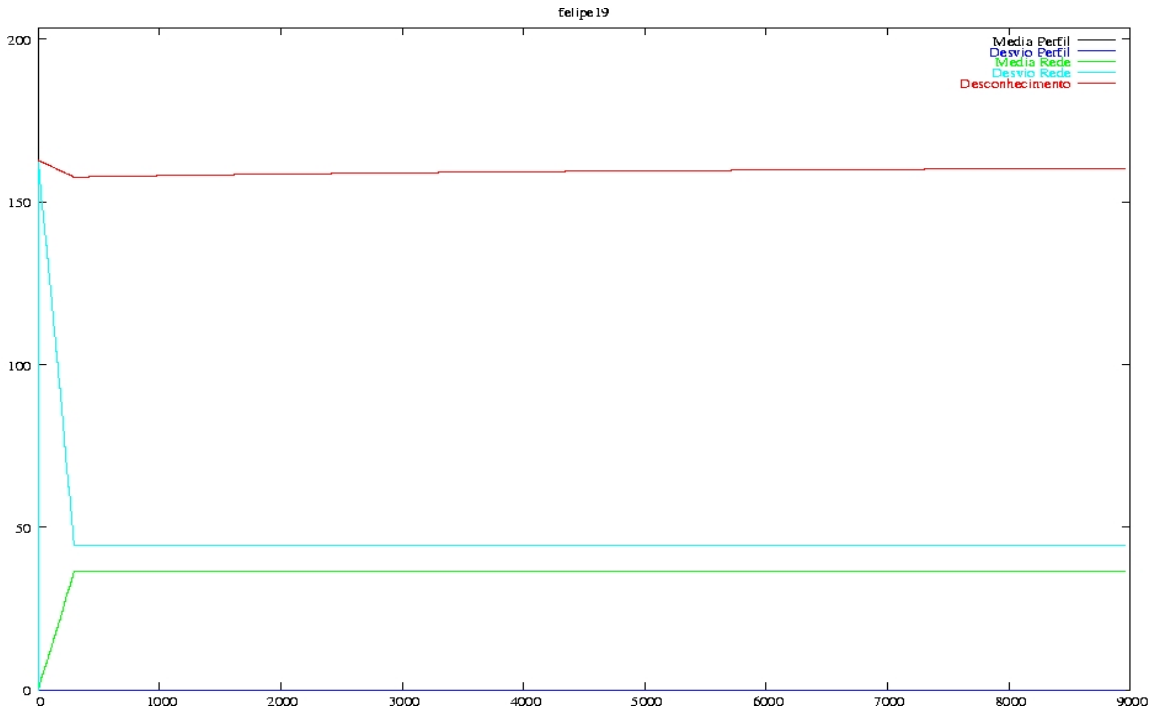


Figura 8 – Média, desvio e desconhecimento no 1º. dia de monitoração

Conforme esperado, o gráfico reflete que houve algum acesso a informações do perfil da rede apenas no início da atividade do usuário, pois, após a variação da média e do desvio do perfil da rede, as medidas mantiveram valores constantes até o final do período de monitoração. O grau de desconhecimento se manteve bem próximo ao valor máximo durante todo o período.

Após a análise da primeira monitoração, ou seja, a monitoração de um dia, já é possível conhecer um pouco em relação ao comportamento do usuário. Na figura 9, apresenta-se a monitoração de um usuário, no segundo dia, que tem o comportamento bastante similar ao dia anterior.

Como pode-se observar pelo gráfico da figura 9, a média e o desvio padrão do usuário decrescem ao longo do tempo, enquanto o grau de desconhecimento se mantém baixo, mas presente. Isto significa que o usuário executa muitos acessos comuns ao seu perfil, mas também faz alguns acessos a novos destinos e serviços. No final do período da monitoração, observa-se que as medidas de média e desvio padrão alcançam ou aproximam-se muito do valor zero e então retomam seu crescimento. Isto significa que o usuário fez tantos acessos quantos os registrados no seu perfil histórico, portanto sua média e desvio tendem a zero. Mas o usuário também executa acessos aos destinos e serviços do seu perfil em quantidade superior ao que era conhecido, pois a média e o desvio tendem a crescer no final da monitoração. Isto pode ser resultado do pouco conhecimento prévio em relação ao seu comportamento. Observa-se, também, que neste período o grau de desconhecimento não decresce, o que significa que o usuário continua alternando acessos conhecidos com novos acessos.

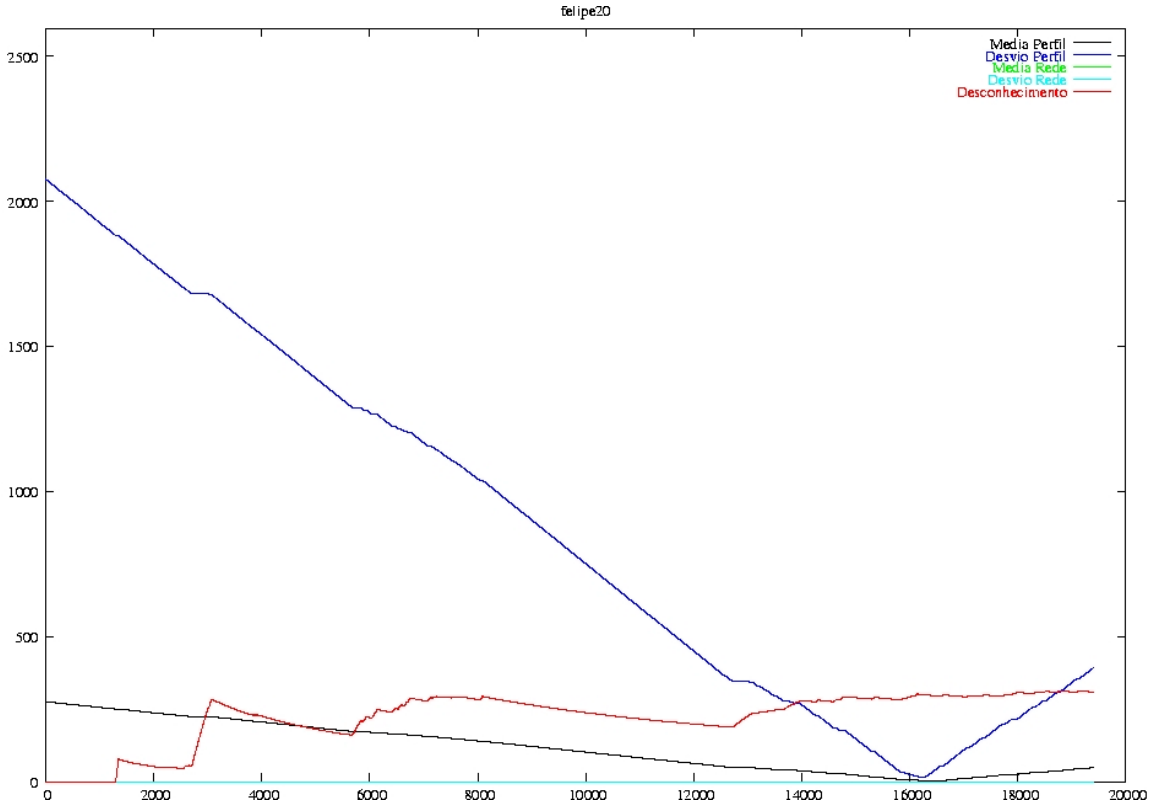


Figura 9 – Média, desvio e desconhecimento no 2º. dia de monitoração

Para exemplificar os gráficos apresentados no Anexo A, na figura 10, o mesmo gráfico da figura 9 é apresentado usando-se uma escala logarítmica. Então, observa-se o real valor do grau de desconhecimento em comparação com os valores de média e desvio padrão.

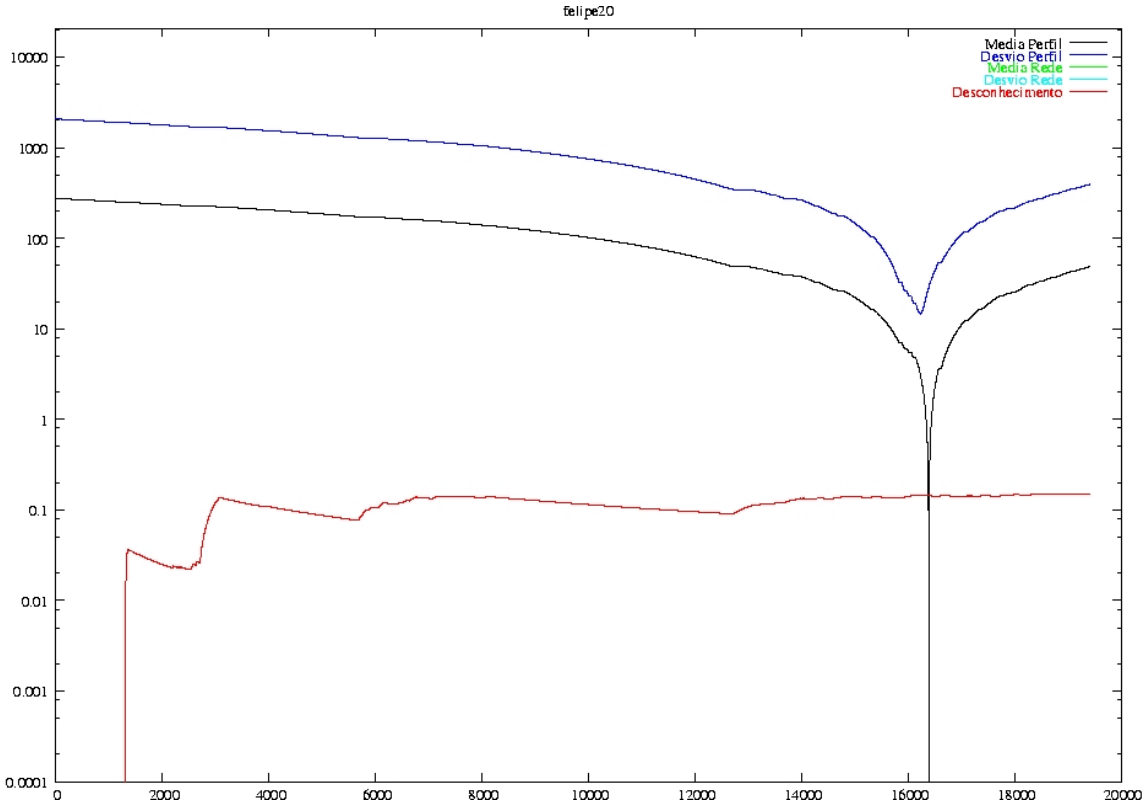


Figura 10 – Gráfico em escala logarítmica

Em relação ao grau de desconhecimento deste usuário pode-se observar que:

- Mantém-se em zero inicialmente, o que significa que o usuário não executa nenhum acesso desconhecido;
- Decresce à medida que a média e o desvio decrescem;
- Apresenta elevação nos momentos em que a média e o desvio permanecem estáveis;
- Permanece próximo a zero, o que implica que ele não afeta de forma significativa a confiança na identidade do usuário.

No terceiro dia de monitoração do usuário, apresentado na figura 11, observa-se que o conhecimento sobre o usuário aumentou, pois durante a monitoração a média e o desvio padrão apresentam apenas comportamento decrescente. Logo, pode-se observar que este usuário apresenta um comportamento bastante regular até o momento. Quanto ao grau de desconhecimento, vê-se que ele apresenta uma variação maior em relação à última monitoração, mas que também apresenta valores baixos e não interfere na legitimidade do usuário.

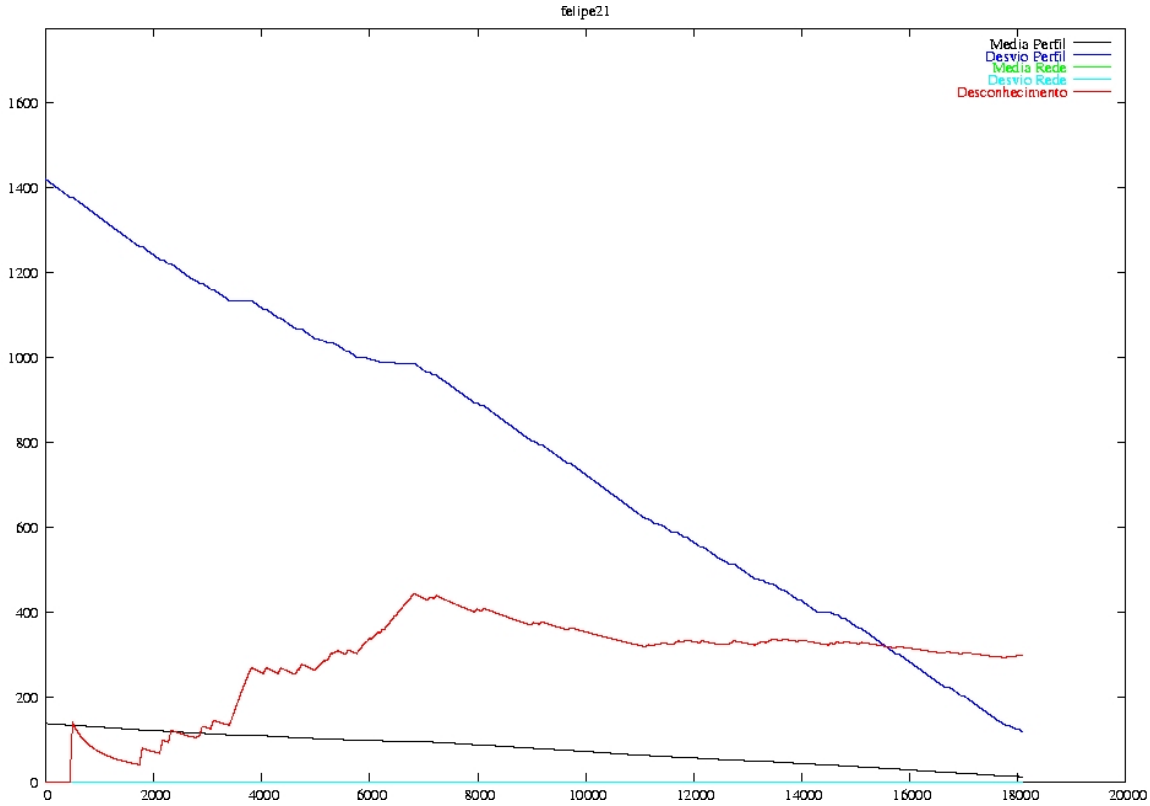


Figura 11 – Média, desvio e desconhecimento no 3º. dia de monitoração

Se comparados o comportamento das medidas, observa-se que o desconhecimento tende a ter momentos de crescimento, quando a média e o desvio apresentam momentos de estabilidade, e decrescimento, quando a média e o desvio decrescem. Este comportamento é natural, pois quanto mais acessos a destinos e serviços conhecidos, menor será o desconhecimento em relação ao comportamento do usuário. No final do período de monitoração, observa-se que o grau de desconhecimento mantém-se com pouca variação, enquanto média e desvio continuam decrescendo, o que significa que o usuário fez simultaneamente acessos conhecidos e desconhecidos.

No quarto dia de monitoração, apresentado na figura 12, observa-se a alteração do comportamento do usuário, pois:

- O usuário inicia suas atividades com acessos conhecidos, o que é demonstrado pela queda inicial da média e do desvio padrão, fazendo decrescer rapidamente o grau de desconhecimento;
- A seguir, o usuário não faz mais acessos a destinos e serviços pertencentes ao seu perfil, fazendo com que a média e o desvio padrão em relação ao perfil histórico mantenham-se estáveis;

- O grau de desconhecimento então volta a crescer, atingindo valores próximos a um, ou seja, assume valores altos;
- O usuário volta a fazer acessos conhecidos e a média e do desvio voltam a decrescer, bem como grau de desconhecimento.

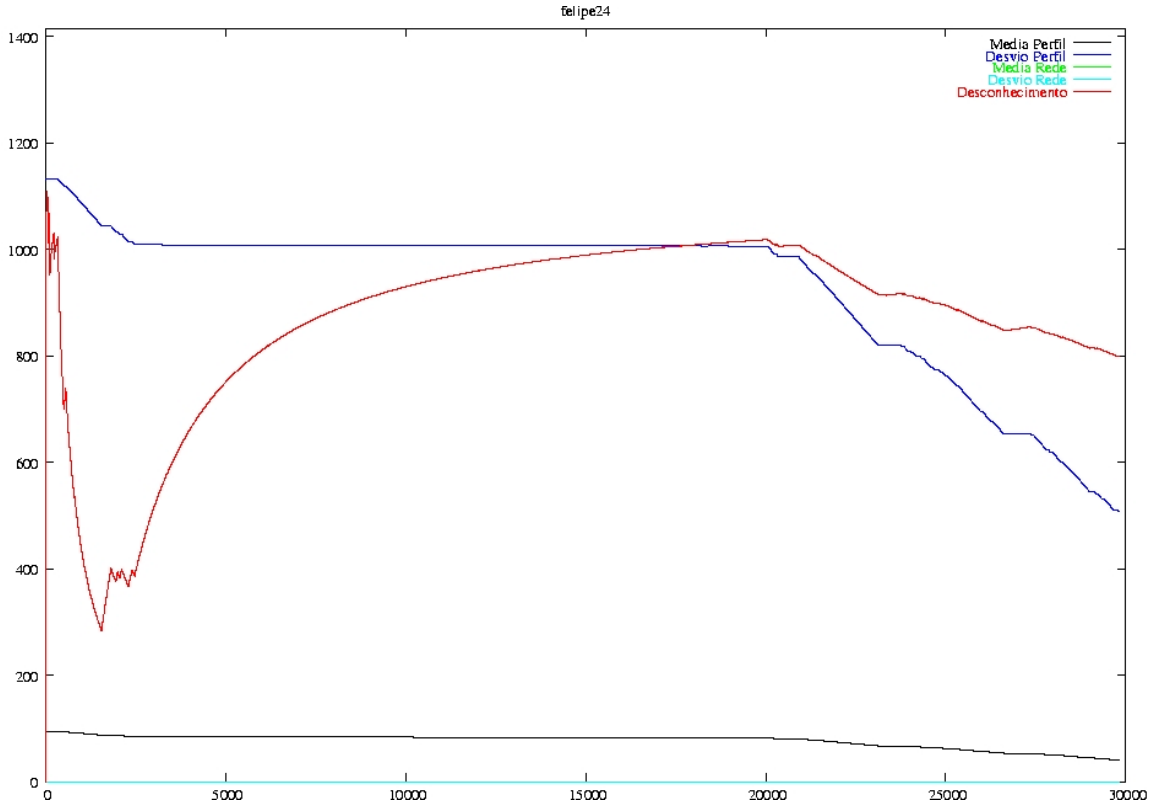


Figura 12 – Média, desvio e desconhecimento no 4º. dia de monitoração

Os dados de cada monitoração analisada passam a incorporar o perfil histórico do usuário e da rede. Isto aumenta o conhecimento sobre o usuário e permite acompanhar as alterações que podem ocorrer, ou seja, permite incorporar no perfil informações sobre os novos destinos e serviços que o usuário está utilizando. A tendência é que com o decorrer do tempo, mais informações a respeito da conduta do usuário sejam conhecidas. Este fato pode ser observado no resultado do quinto dia de monitoração do usuário, cujas informações estatísticas resultantes são apresentadas na figura 13.

Conforme se pode observar, o usuário reproduz seu comportamento regularmente, pois a média e o desvio padrão em relação ao seu histórico decrescem continuamente, tendendo a zero. Também se observa que o usuário continua a executar

alguns acessos novos, pois o grau de desconhecimento está presente, mas assume valores baixos.

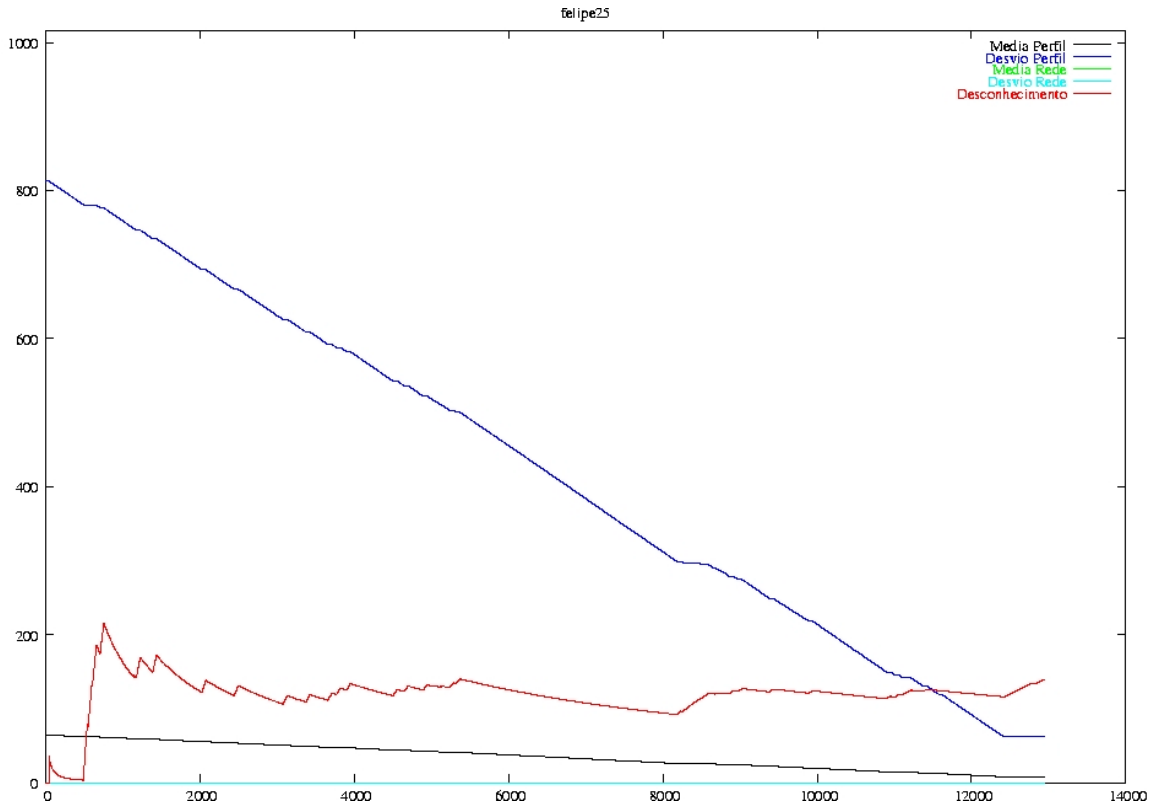


Figura 13 – Média, desvio e desconhecimento no 5º. dia de monitoração

A análise dos demais dias de monitoração apresenta comportamento similar ao dos primeiros cinco dias, podendo-se observar o aumento de conhecimento sobre o comportamento do usuário.

Sobre o usuário monitorado pode-se concluir que ele apresenta um comportamento regular, o que facilmente permite reconhecê-lo como um usuário legítimo no sistema. Nos momentos em que houve variação significativa no seu comportamento, o sistema deverá executar uma medida preventiva a fim de confirmar sua identidade. Uma vez confirmada, as ações do usuário são incorporadas ao seu perfil e o usuário passa a ser reconhecido como legítimo pelo sistema nos demais períodos de monitoração.

Nos gráficos apresentados observa-se que os dados referentes à média e ao desvio padrão do perfil da rede são a maioria das vezes zero. Isto deve-se ao perfil da rede inicial ser muito pequeno, sendo os acessos do usuário pertencentes ao perfil do próprio usuário ou considerado desconhecido.

3.2.4.2 Dados do Segundo Usuário Monitorado

A análise de um segundo usuário, nos permite observar um comportamento similar ao do primeiro, mas com variações de medidas mais acentuadas. Por exemplo, a análise dos dados do segundo dia de monitoração do segundo usuário, figura 14, mostra que o desvio padrão volta a crescer antes da média.

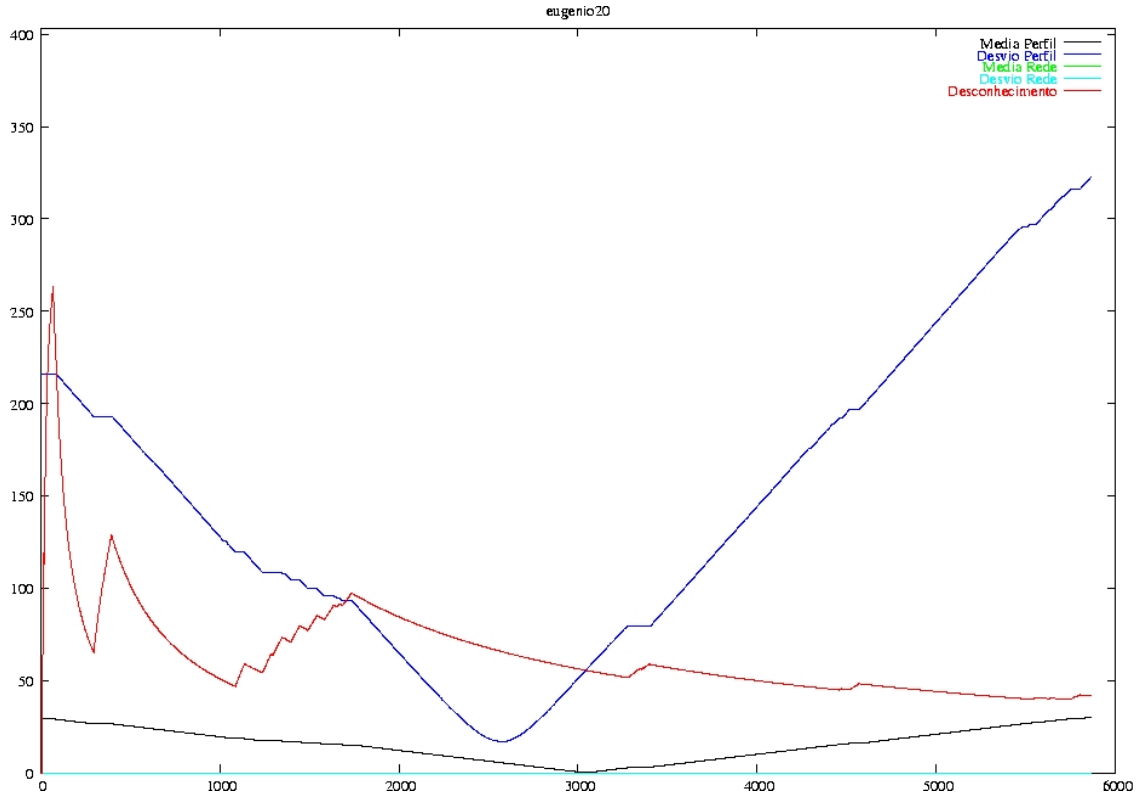


Figura 14 – Análise do 2º. usuário no 2º. dia de monitoração.

Isto significa que o usuário está excedendo o número de acessos a um ou mais destinos e serviços em relação ao seu perfil. Assim, a amplitude total é maior que zero, fazendo com que média continue a decrescer e o desvio cresça. Este fato poderá fazer com que, em um determinado momento, o sistema execute uma ação preventiva, pois pode estar ocorrendo utilização indevida das credenciais do usuário. Se for um usuário malicioso e o evento é uma atitude escusa, então é necessário mais do que a verificação de sua identidade. Ainda se o usuário for legítimo, neste caso, seria necessário comparar os acessos do usuário com um perfil de atitudes indesejáveis, para que fosse identificada a intrusão, ou então, fosse utilizado outro sistema de detecção de intrusão que identifique outros tipos de intrusão e um módulo de correlação de dados e execução de contramedidas combinadas.

As figuras 15, 16 e 17 apresentam os gráfico com as medidas de média, desvio padrão e grau de desconhecimento para o segundo usuário monitorado. E conforme dito antes, quanto mais aumenta o conhecimento sobre suas atividades, e o usuário as reproduz, a tendência da média e do desvio padrão é de decrescimento.

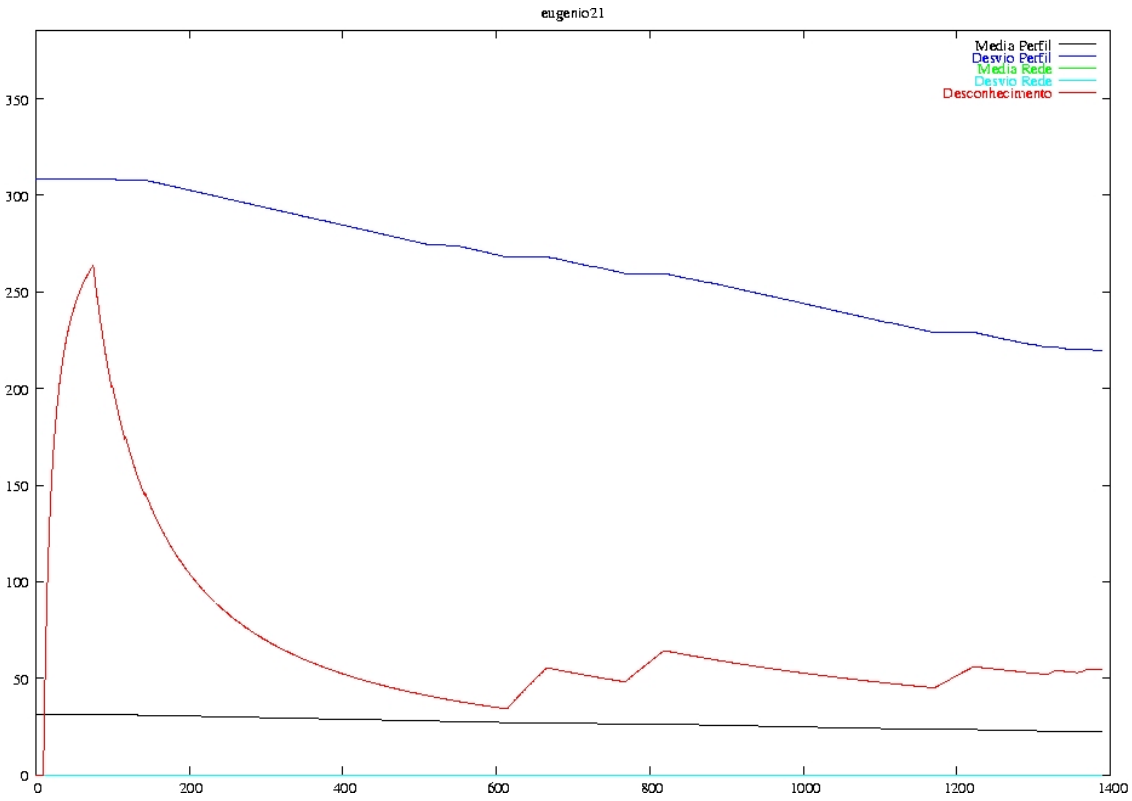


Figura 15 – Análise do 2º. usuário no 3º. dia de monitoração.

O gráfico da figura 15 permite observar que:

- O usuário inicialmente executa poucas ações conhecidas, ou seja, registradas no seu perfil de usuário, pois a média e o desvio padrão tem um ligeiro decréscimo;
- O usuário a seguir executa acessos desconhecidos em número relativamente alto aos acessos conhecidos, pois o grau de desconhecimento cresce rapidamente e atingindo valores relativamente altos;
- O usuário volta ao seu comportamento normal, pois a média e o desvio padrão decrescem ao longo do período de monitoração continuamente;
- O grau de desconhecimento também decresce à medida que aumentam o número de acessos conhecidos. Ele irá apresentar alguns pequenos picos de

crescimento em momentos que se observa a ligeira estabilização da média e do desvio padrão.

A atividade do usuário no terceiro dia mostra que ele é legítimo, apesar de um momento de instabilidade quanto o desconhecimento no início da monitoração. Caso o grau de desconhecimento tenha avançado além do limiar normal para este sistema, uma ação de verificação do usuário deverá ser executada.

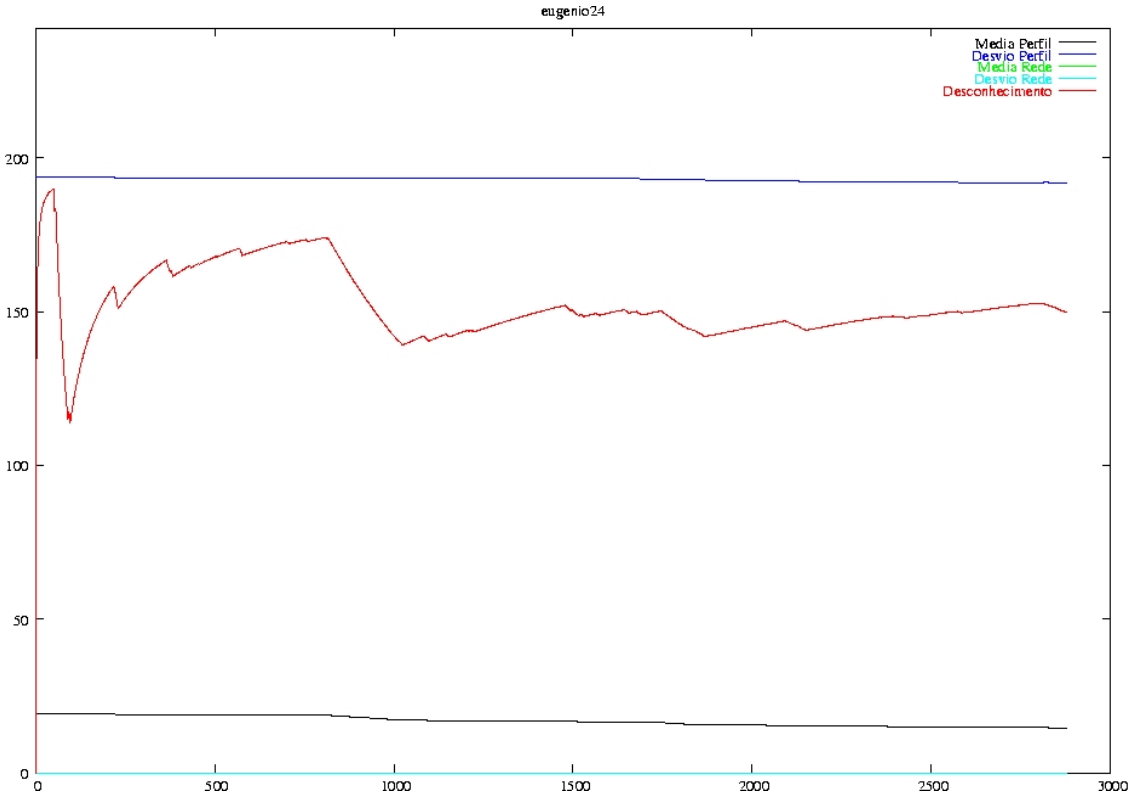


Figura 16 – Análise do 2º. usuário no 4º. dia de monitoração.

O gráfico da figura 16 permite observar que no quarto dia de monitoração do usuário seu comportamento não permite identificá-lo como legítimo. A observação dos valore e do comportamento da média e do desvio padrão permite observar que:

- O usuário fez poucos acessos a destinos e serviços presentes no seu perfil, pois e o desvio e a média decrescem muito lentamente e mantêm-se constantes a maior parte do período de monitoração;
- O grau de desconhecimento mantém-se sempre alto.

Neste caso, o sistema iria com certeza executar ações que permitissem validar o usuário e manter o seu acesso aos serviços.

Na figura 17, vê-se que o usuário reproduz um comportamento normal, sendo identificado como um usuário legítimo. Neste gráfico verifica-se que o grau de desconhecimento mantém-se baixo e a média e o desvio padrão são decrescentes.

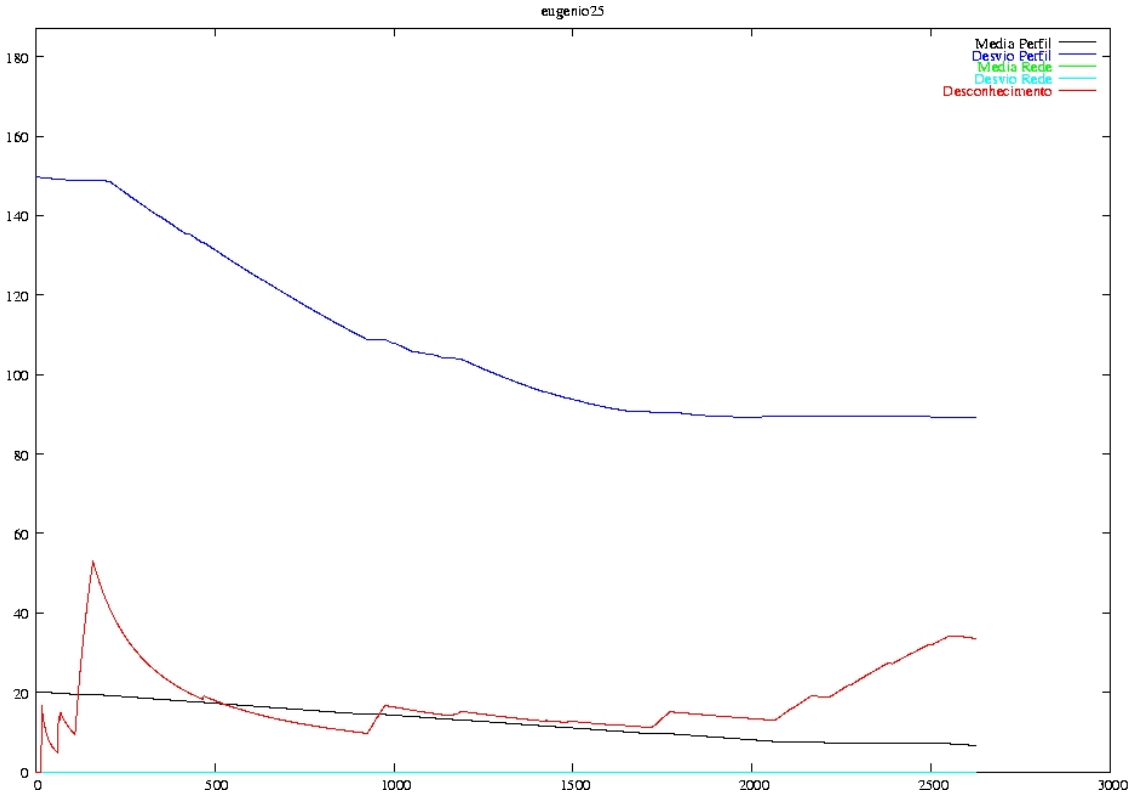


Figura 17 – Análise do 2º. usuário no 5º. dia de monitoração.

3.2.4.3 Dados do Terceiro Usuário Monitorado

A monitoração dos usuários permite verificar que a maioria apresenta um comportamento regular, ou seja, reproduz constantemente os acessos conhecidos. Mas também foi possível verificar que alguns usuários apresentam um comportamento bastante irregular, o que não permite ao sistema ter um alto grau de confiança a respeito de sua identidade. Os gráficos de média, desvio padrão e grau de desconhecimento apresentados nas figuras 18, 19, 20 e 21, demonstram um caso de comportamento irregular. Na análise feita durante duas semanas, dos quais os cinco primeiros dias foram apresentados, observa-se que o usuário faz poucos acessos a destinos e serviços presentes no seu perfil de usuário e no perfil da rede, tendo sempre um alto valor para o grau de desconhecimento. Neste caso, o sistema sempre irá considerar o usuário suspeito.

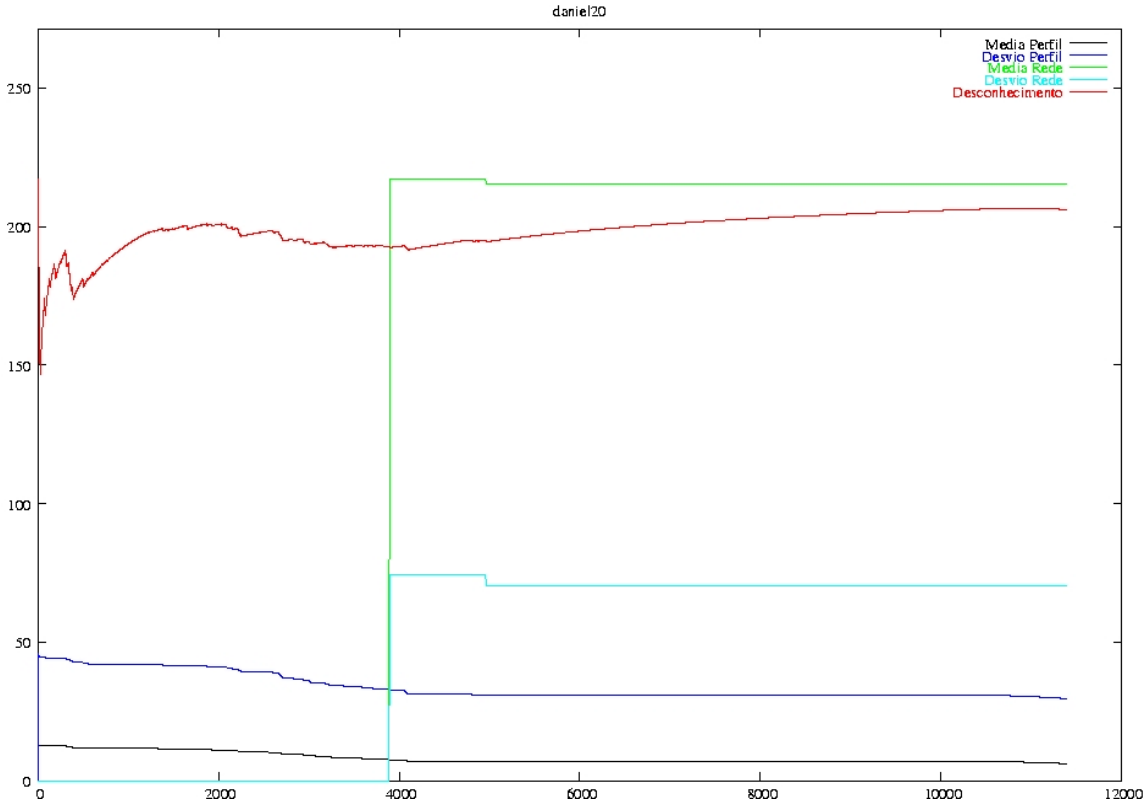


Figura 18 – Análise do 3º. usuário no 2º. dia de monitoração

A análise do segundo dia de monitoração do usuário, apresentada na figura 18, mostra que o usuário executa acessos que fazem parte de seu perfil, mas como o conhecimento a seu respeito é baixo é normal que o grau de desconhecimento seja alto. Pode-se observar que o usuário faz acessos a destinos e serviços comuns tanto ao seu perfil de usuário, quanto ao perfil da rede. Este evento pode ser observado, pois existem no gráfico as informações a respeito da média e do desvio padrão tanto do perfil do usuário, quanto da rede. Observa-se também que os acessos estão de acordo com os acessos que o usuário habitualmente executa, pois a média e o desvio padrão tendem apenas a decrescer.

O gráfico da figura 18 mostra que quando o usuário faz acessos conhecidos o grau de desconhecimento tende a decrescer e quando a média e o desvio tendem a estabilizar, ou seja, mantêm-se praticamente constantes o grau de desconhecimento eleva-se.

Neste dia, o usuário seria considerado suspeito várias vezes durante a monitoração. Para que ele não fosse importunado constantemente, uma vez que ele é

legítimo, o sistema deverá prever formas para minimizar o assédio ao usuário e até mesmo evitar que o acesso do usuário aos serviços seja bloqueado.

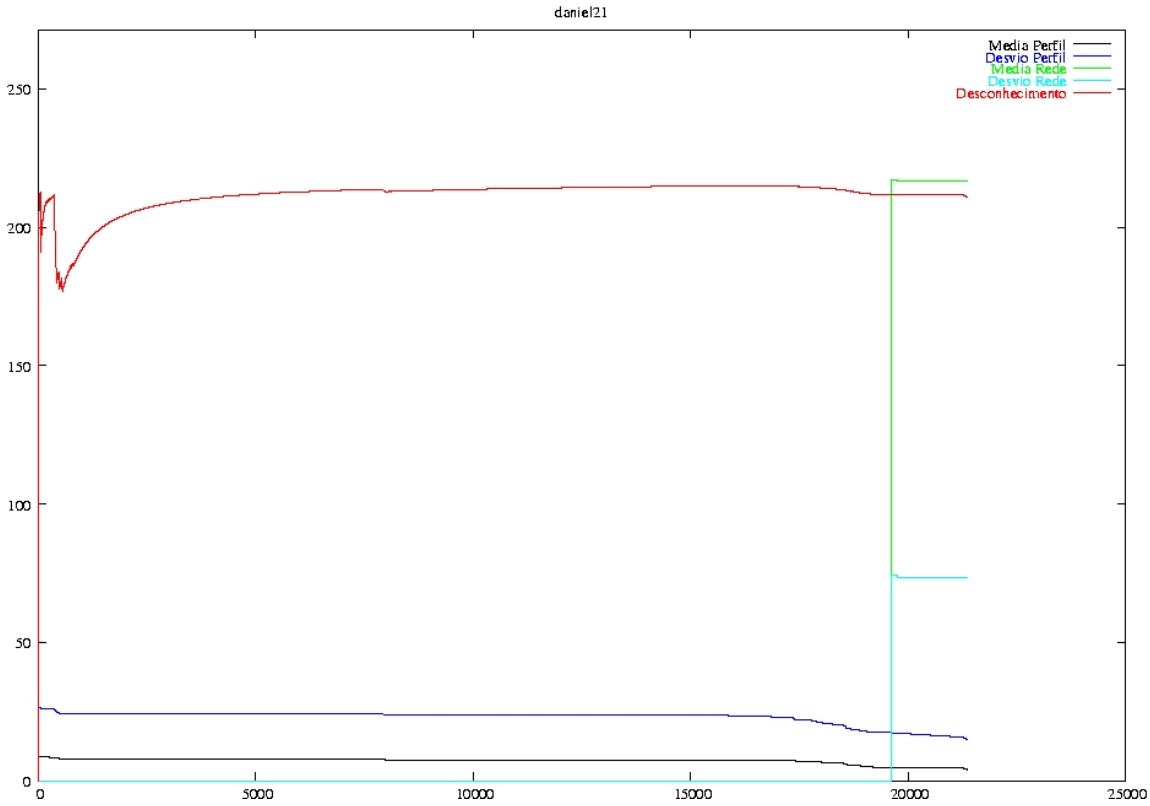


Figura 19 – Análise do 3º. usuário no 3º. dia de monitoração.

No terceiro dia de monitoração, o grau de desconhecimento que mantém-se elevado e com pouca variação. Observa-se que este usuário geralmente, no seu início de atividade, executa acessos conhecidos, fazendo com que a média e o desvio padrão decresçam e também o grau de desconhecimento. Após este evento, o usuário não executa mais acessos conhecidos, pois a média e o desvio padrão mantêm-se estáveis, enquanto que o grau de desconhecimento volta a crescer rapidamente e permanece alto até o final do período da monitoração.

O usuário analisado voltou a realizar acessos registrados tanto no seu perfil quanto no perfil da rede, pois o gráfico mostra que no final do período de monitoração a média e o desvio em relação ao perfil do usuário voltam a decrescer. Este fato observa-se até então nos dois dias de monitoração.

No quarto dia de monitoração do usuário, figura 20, observa-se que o usuário faz acessos conhecidos, mas o volume de acessos a destinos e serviços diferentes dos anteriores ainda é alto. Observa-se que a média e o desvio padrão em relação ao perfil

do usuário oscila, sempre com tendência decrescente. O grau de desconhecimento irá oscilar conforme o número de acessos aos destinos e serviços conhecidos ocorrem, mas percebe-se que ele se mantém alto, indicando que a maioria das ações do usuário são novas para o sistema. No gráfico o grau de desconhecimento apresenta uma variação de comportamento mais visível que a média e o desvio padrão devido à escala utilizada.

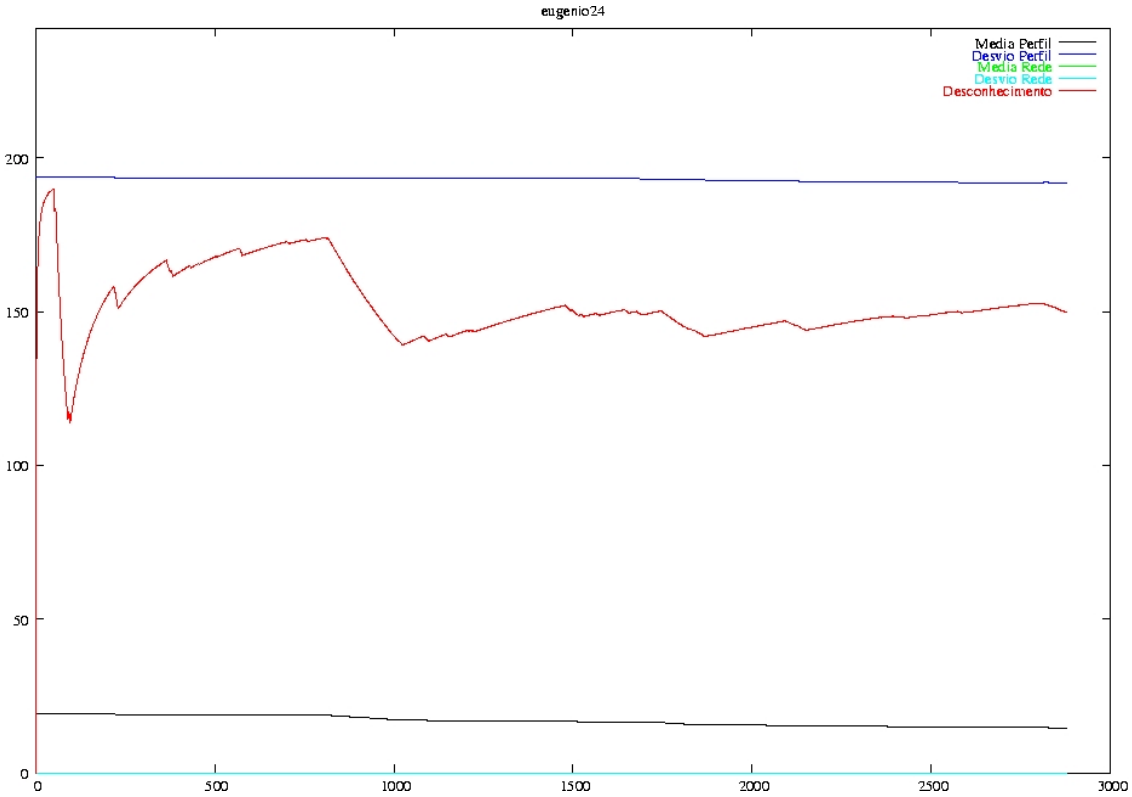


Figura 20 – Análise do 3º. usuário no 4º. dia de monitoração

Se for observado o gráfico da figura 40, no Anexo A, pode-se verificar que o grau de desconhecimento varia pouco e permanece próximo ao valor 1.

Neste dia, o sistema teria o mesmo comportamento em relação ao usuário que no dia anterior, pois ele tem um comportamento suspeito com alto índice de desconhecimento.

No quinto dia da monitoração apresentado na figura 21, o comportamento do usuário é idêntico aos demais dias observados, sendo que este usuário seria constantemente considerado suspeito pelo sistema.

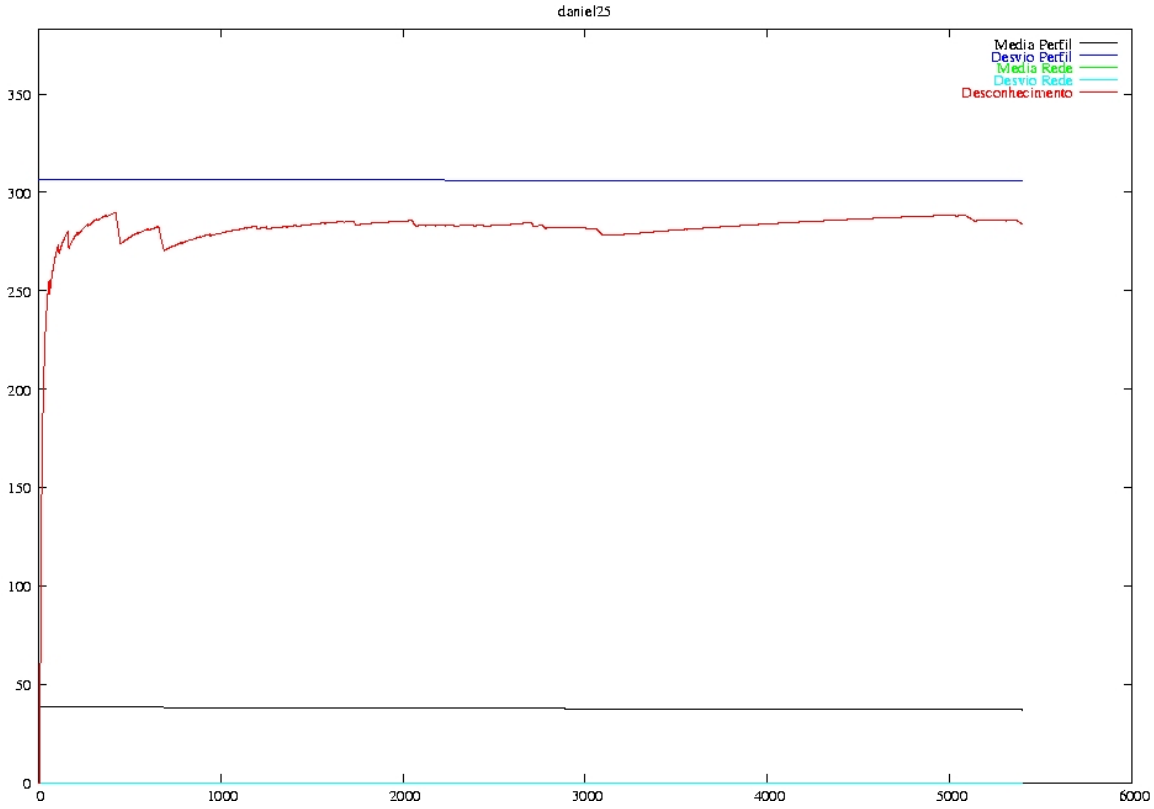


Figura 21 – Análise do 3o. usuário no 5o. dia de monitoração.

3.2.4.4 Falsificação de Dados

No caso de falsificação das credenciais, para avaliação dos resultados, fez-se a troca de perfis entre os usuários, isto é, foram submetidos ao sistema os quatro primeiros dias de monitoração do segundo usuário, que foi analisado anteriormente. Então foram utilizados os acessos do primeiro usuário como se fossem do segundo usuário, no quinto dia de monitoração. O que se observa é que o grau de desconhecimento do usuário cresce substancialmente, figura 22, o que faria com que o sistema executasse uma medida para validação da identidade do usuário ou até mesmo o bloqueio dos serviços, de acordo com a política de segurança local.

O teste foi feito com usuário de um mesmo laboratório e com número de acessos a destinos e serviços semelhantes. Isto é necessário, pois caso os acessos de um ou outro fossem em maior número, o pior caso, ou seja, a falsificação poderia não ocorrer ou ser forçada pela diferença de acessos. Assim, utilizou-se usuário de comportamentos semelhantes para verificar se as variações de comportamento seriam detectadas pelo sistema. Como se pode observar, o segundo usuário apresenta nos 5 primeiros dias de monitoração um comportamento mais legítimo do que suspeito. Enquanto que, sendo

fornecidos os dados do quinto dia de monitoração do primeiro usuário para a compilação e análise do segundo usuário, verifica-se que o usuário passou a ser desconhecido para o sistema. O resultado é um alto índice de ações desconhecidas e poucos acessos conhecidos, implicando em um grau de desconhecimento alto e uma média e o desvio padrão que praticamente não se alteram.

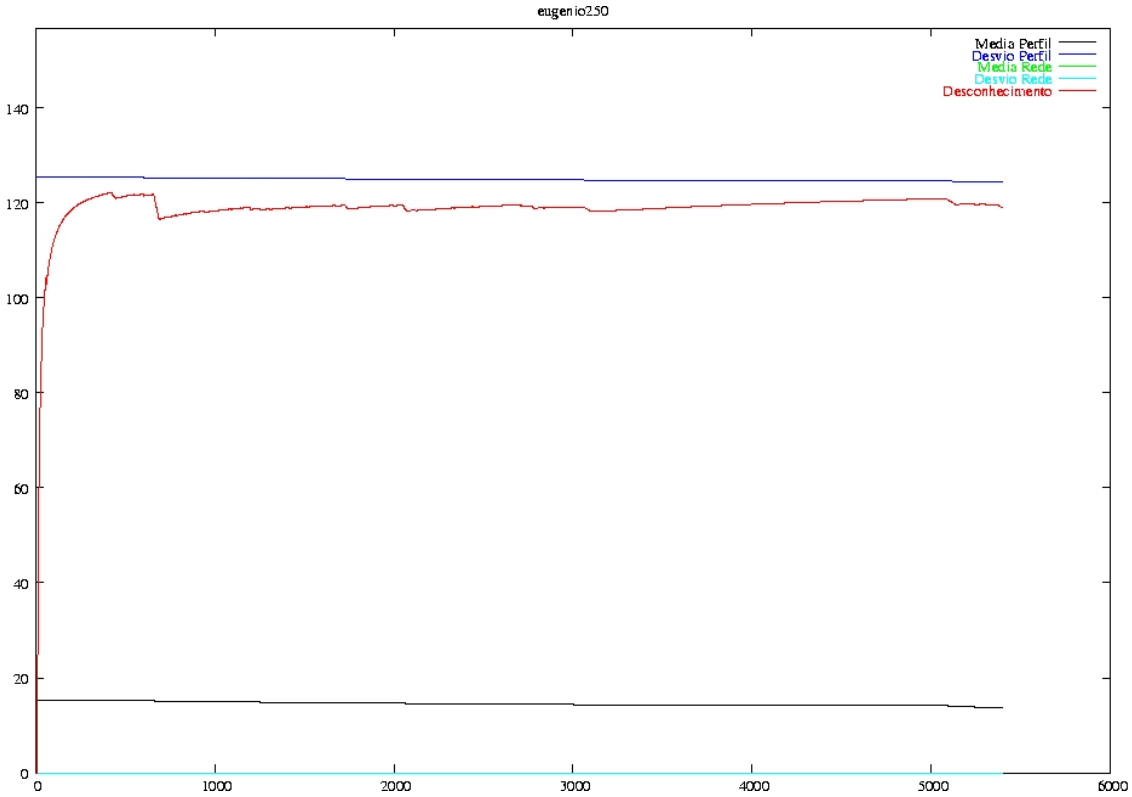


Figura 22 – Falsificação de credenciais

Através da observação do comportamento dos usuários, pode-se observar que é válido monitorar o comportamento através do que os usuários fazem, observando os destinos e serviços que eles têm acesso e quantos acessos normalmente o usuário faz.

3.2.4.5 Análise Geral dos Usuários Monitorados

Em geral, os usuários analisados, em torno de 90%, apresentaram um comportamento coerente, isto é, após o período inicial de monitoração (um dia), o comportamento do usuário passa a ser conhecido pelo sistema. Os acessos desconhecidos não tiveram peso suficiente para considerar os usuários suspeitos a maior parte do tempo. Como os acessos desconhecidos passam a incorporar o perfil do

usuário, aumenta-se o grau de conhecimento sobre o mesmo e permite-se que as alterações de comportamento sejam acompanhadas pelo sistema.

Em 10% dos casos analisados, os usuários apresentaram diariamente um comportamento bastante variável e com alto grau de desconhecimento, sendo este fator um determinante para que o sistema excute alguma contramedida para garantir a legitimidade do usuário.

3.2.5 Grau de Desconhecimento, Média e Desvio Padrão

O sistema deve observar o resultado das medidas do grau de desconhecimento, os valores e o comportamento da média e do desvio padrão como forma de detecção de situações anormais de comportamento para um usuário. Alguns autores propõem em suas abordagens métodos matemáticos que combinam todas as medidas em um índice que indica a ocorrência de uma intrusão. Outros autores utilizam métodos baseados em lógica *fuzzy*, ou redes neurais, para a avaliação das medidas e determinação da intrusão. Neste trabalho optou-se por não utilizar ou criar qualquer método matemático para agregação de valores, pois considera-se que há perda de informação nesta abordagem, sendo mais interessante a utilização de métodos que possam avaliar as medidas individualmente.

A primeira abordagem avaliada neste trabalho foi a utilização de um sistema de regras para teste das medidas resultantes do sistema associadas à utilização de políticas, através das quais são determinadas as ações ou contramedidas executadas pelo sistema. Outra abordagem estudada emprega a utilização de lógica *fuzzy* para a implementação do sistema de regras.

3.2.6 Escalabilidade do Sistema Proposto

A escalabilidade do sistema está vinculada ao número de usuários monitorados, ao volume de tráfego da rede e a quantidade de informação armazenada nos perfis. O número de usuários e o volume de tráfego da rede afetam diretamente a capacidade de processamento do sistema, enquanto que o volume de dados dos perfis afeta diretamente a capacidade de memória do sistema.

O tempo de processamento das informações de endereços, serviços e protocolos não é uma operação cara em termos de processamento se avaliada individualmente, pois constitui basicamente a comparação de valores inteiros e incremento de contadores. O maior custo está associado ao tempo de busca das informações do perfil nas estruturas de dados. Mas isto pode ser minimizado com a implementação de algoritmos otimizados de busca.

O número de usuários a serem monitorados e o volume de dados a ser analisado pelo sistema é um fator de sobrecarga para o processamento. O sistema de detecção deve ser projetado para conter o maior nível de paralelismo possível para tratamento das informações.

A utilização de memória pode ser o fator mais severo para a escalabilidade do sistema, pois se cada perfil for implementado como:

- um vetor de 2^{56} e o dado armazenado ocupa 32 bits, o total de memória necessária será de 288.230.376.151.711.744 bytes. Esta solução é considerada obviamente inviável;
- um vetor com *n* entradas por usuário no qual são armazenados a tupla <IP, porta, protocolo, número de acessos>, utilizando um total de 88 bits, será necessário *n x 88 bits* para cada perfil. Então, se for utilizado um perfil com 1000 entradas, será necessário para o perfil do usuário aproximadamente 11 Kbytes de memória.

No segundo caso, em um sistema com 100 usuários monitorados e cada um com um perfil de 1000 entradas, será necessário aproximadamente 1 Mbyte para armazenar os perfis históricos simultaneamente. Além disto, será necessário considerar o espaço para os perfis locais de cada usuário e para o perfil da rede. Se for utilizado o mesmo espaço para dos perfis de usuário para os perfis locais, e 50 vezes o tamanho de um perfil de usuário para o perfil da rede, serão necessários 2,5 Mbytes de memória no total.

4 Sistema de Regras para Avaliação das Informações Estatísticas

Regras são utilizadas em sistemas de detecção de intrusão e tem como vantagem, em relação à métodos numéricos como redes neurais, a facilidade de atualização do sistema e a flexibilidade para inserção, remoção e alteração de regras para ajuste do comportamento do sistema sem necessidade de recompilação ou treinamento para aprendizado de casos.

Conforme [OLI 02], uma regra para detecção de intrusões baseada em anomalias pode usar, como dados comparativos, a freqüência de *loggin* de um determinado usuário, o tempo que o mesmo permanece conectado, os programas que este costuma executar, dentre várias outras informações que podem ser coletadas a partir da utilização do sistema. A utilização de regras também pode facilitar o processo de estabelecimento de políticas. Juntamente com a caracterização do ataque, determina-se o procedimento a ser realizado quando esse é identificado.

Além da aplicação de regras estáticas e manualmente alteradas, muitas pesquisas têm sido realizadas na área de sistemas especialistas, de forma a estudar e desenvolver sistemas de geração automática de regras. Esses sistemas geram regras automaticamente de acordo com os eventos monitorados e, portanto, aprendem automaticamente sobre novas situações. Exemplos desses sistemas são apresentados em [COH 95] [HEL 00], onde os autores propõem métodos de aprendizado automático.

Neste trabalho adotou-se a utilização de métodos estatísticos para o processamento das informações do sistema e geração de índices que permitam a identificação de situações de intrusão. O sistema estatístico então é responsável pelas medidas, e a identificação da evidência de uma intrusão é implementada por um sistema de regras.

Com a utilização de regras, o sistema viabiliza também a utilização de políticas, as quais determinam as ações que devem ser executadas, de acordo com cada evento detectado. A utilização de políticas torna o sistema flexível para adaptar-se às políticas locais de cada domínio, e permite a fácil alteração de comportamento do sistema, quando há alterações nas políticas locais.

O sistema de regras empregado neste sistema pode ser implementado como um sistema de regras de produção simples, ou como um sistema *fuzzy*. Em um sistema baseado em regras simples, as medidas são avaliadas individualmente, e de acordo com os valores que assumem ou de sua tendência de comportamento, elas determinam diretamente a ação a ser executada. Isto é, a avaliação de uma medida como grau de desconhecimento pode determinar a execução de uma política sem a necessidade de observação das demais medidas.

Em um sistema de regras *fuzzy*, as medidas são analisadas por um conjunto de regras fuzzy de acordo com pesos atribuídos a seus valores. A combinação dos pesos resultantes leva a uma política determinada, que deve estar em acordo com a informação de maior importância.

Ambos os sistemas de regras são válidos para o sistema de detecção de intrusão proposto. As diferenças entre eles estão no conjunto de informações que são avaliadas e na forma como são avaliadas. A seguir os sistemas de regras são discutidos individualmente.

4.2 Sistema baseado em Sistema de Regras Simples

O objetivo do sistema de regras é a identificação de situações suspeitas a partir dos dados estatísticos e a determinação de um procedimento a ser executado para garantir a integridade do sistema.

O sistema de regras elaborado neste trabalho associa as regras à políticas que determinam o procedimento a ser executado para controle dos direitos de acesso do usuário aos serviços da rede. As regras são descritas da seguinte forma

If <*antecedente*> *Then* <*conseqüente*>

Onde,

- A parte <*antecedente*> pode ser descrita por um conjunto $A=(a_1, a_2, ..., a_n)$, sendo A, composta por uma ou mais sentenças conectadas por operadores lógicos AND ou OR. Cada a_i, para $1 \leq i \leq n$, expressa uma condição de teste das medidas obtidas. Isto é, cada a_i tem o formato

  <*var*> *OP* <*valor*>

Onde,

- <*var*> é o conjunto de variáveis utilizadas no sistema para armazenar medidas estatísticas, bem como variáveis condicionais, contadores e outras que são utilizadas para controle de eventos do sistema.
- *OP* é o conjunto de operadores que podem ser utilizados para cada a_i, sendo OP = {=, !=, >, <, ≤, ≥}.
- E <*valor*> são os valores para a comparação das variáveis, ou seja, os limiares de comparação.

- A parte <*conseqüente*> pode ser descrita pelo conjunto $P=\{p_1, p_2, ..., p_n\}$, sendo P é o conjunto de políticas que podem ser associadas a uma regra de acordo com as sentenças avaliadas.

Então, por exemplo, uma regra para um teste do grau de desconhecimento possível seria:

If (grau_desconhecimento > y) Then Política _1

Neste exemplo, a política descreve uma ação conveniente, de acordo com a gravidade do evento. Essa política poderia ser a solicitação de uma senha de segundo nível para o usuário, o bloqueio de acesso a um determinado serviço, a geração de um alarme para o administrador da rede, entre outros. A especificação da política é dependente da política geral de segurança da rede.

O diagrama da figura 23 apresenta as condições a serem verificadas no sistema, a partir das quais são geradas as regras. A opção pela representação através desse diagrama é baseada na facilidade de visualização das condições que devem ser contempladas pelo sistema de regras e como eles se encadeiam.

Os valores para as variáveis, que representam limiares para comparação das medidas, que são utilizadas no diagrama, são dependentes da política geral de segurança do ambiente. Estas variáveis devem ser configuradas pelo administrador local. A configuração pode ser feita através do gerenciamento baseado em políticas.

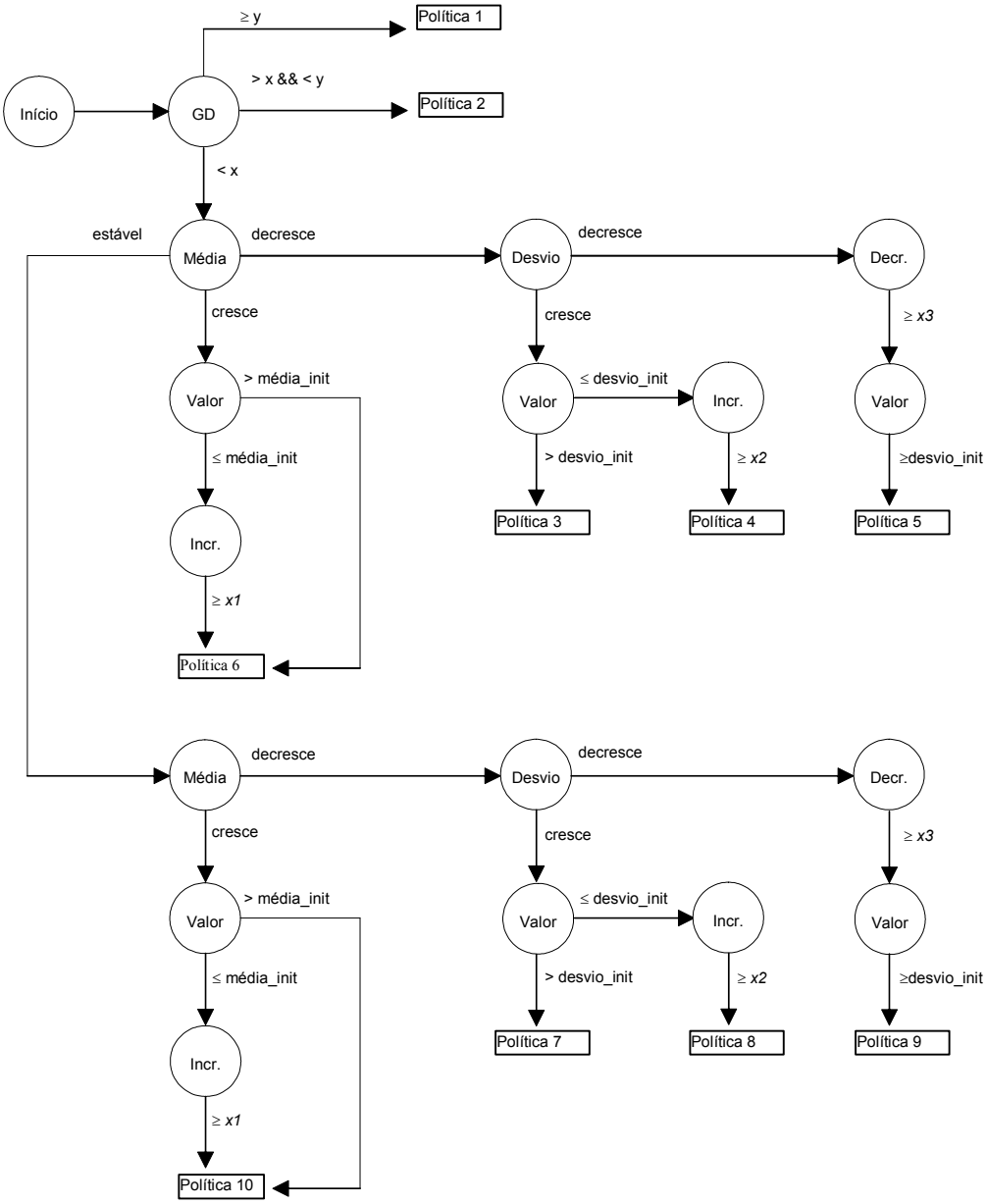


Figura 23 – Diagrama de estados do sistema de regras simples

Observando-se esse diagrama, pode-se identificar que se a primeira condição verificada resulta em verdadeiro, dispara a execução de uma política. Nesse caso, as demais condições não serão verificadas. Essa abordagem tem como vantagem a rapidez na identificação de situações de intrusão, pois dada a satisfação de uma condição, é executada uma contramedida sem a necessidade de verificar as demais condições. Uma desvantagem deste método é que ele não considera um possível histórico do sistema. Isto é, caso o usuário tenha tido um comportamento aceitável e em um determinado instante ele desvia-se desse comportamento o sistema não tem como considerar seu passado recente. Assim, a política a ser executada para este usuário poderá ser forte

demais, pois não há condições de avaliar o seu comportamento prévio e ele será considerado um intruso em potencial. Uma conseqüência disso é a geração de um alto número de falsos positivos que o sistema poderá gerar.

4.3 Sistema baseado em Regras Fuzzy

O sistema *fuzzy* [NGU 99] apresenta um conceito mais difuso em relação aos modelos matemáticos. Isto é, em um modelo matemático as mediadas são tratadas de forma absoluta, enquanto em um modelo *fuzzy* utilizam-se variáveis *fuzzy* do tipo alto, médio e baixo, cujos valores associados não são exatos. Nesse modelo, utilizam-se conceitos matemáticos, especialmente de teoria de conjuntos, para tratamento e interpretação dos dados.

A lógica *fuzzy* apresenta um sistema de regras do tipo *If X Then Y Else Z*, como solução para sistemas de controle, ao invés da utilização de um modelo matemático. Um exemplo clássico da utilização de sistemas *fuzzy* são os sistemas de controle de temperatura, que conforme as variações de quente, frio, muito quente, muito frio, executam ações de ajuste para as condições de temperatura desejadas. As ações podem ser tomadas em função de uma interpretação semântica dos dados e não em função dos seus valores pura e simplesmente, o que significa mais flexibilidade na avaliação dos dados.

A representação das regras *fuzzy* pode ser feita utilizando-se uma matriz de regras que combina os valores possíveis para um conjunto de entradas e obtém uma resposta como saída, para cada combinação. A partir da matriz de regras, ou seja, do conjunto de entradas, do conjunto de saídas e das ações associadas a cada conjunto, extrai-se as regras *fuzzy*.

As regras lingüísticas são expressas na forma *If...Then* e são compostas por duas partes, que são o bloco antecedente e o bloco conseqüente, da seguinte forma

If <*antecedente*> *Then* <*conseqüente*>

Onde,

- A parte <*antecedente*> é um conjunto sentenças $A=(a_1, a_2, ..., a_n)$, composta por uma ou mais sentenças conectadas por operadores lógicos *fuzzy* AND ou OR.
- A parte <*conseqüente*> é representada pó um conjunto $P=\{p_1, p_2 ,..., p_n\}$, que é conjunto de políticas que podem ser associadas uma regra de acordo com as sentenças avaliadas.

Neste trabalho, o conceito de regras *fuzzy* é aplicado para avaliar a combinação das medidas observadas pelo sistema e então determinar a política adequada. A situação a ser avaliada é a ocorrência de um desvio de comportamento, e para isso são observadas diversas medidas estatísticas. Essas medidas são o grau de desconhecimento, a média e o desvio padrão, referentes ao perfil histórico do usuário, e a médio e o desvio padrão, referentes ao perfil histórico da rede.

O grau de desconhecimento é, por natureza, uma medida *fuzzy*. Ela assume naturalmente valores entre [0,1] e deve ser interpretado no sistema como conjuntos *fuzzy* alto, médio ou baixo. Um valor qualquer do grau de desconhecimento pode ser, então, um valor tanto alto como médio, ou baixo, dependendo do conjunto a que ele pertencer, o que o caracteriza como uma medida *fuzzy*.

Estes conjuntos *fuzzy* podem ter intersecções que permitem que um determinado valor de grau de desconhecimento possa pertencer a dois conjuntos ao mesmo tempo. Por exemplo, o grau de desconhecimento igual a 0.75 pode ser considerado alto e médio ao mesmo tempo em um determinado sistema de segurança. Isto insere um grau a mais de incerteza no sistema. Esta incerteza força que mais regras sejam avaliadas, e mais variáveis sejam consideradas para a tomada de decisão, gerando uma decisão com maior grau de confiabilidade. Ou seja, se questionarmos o especialista em segurança do sistema do exemplo, ele vai afirmar que o valor 0.75 pode ser tanto alto quanto médio, que ele considera mais alto do que médio e que em combinação com a média de acessos do usuário ele pode tomar uma decisão precisa.

Para modelar este tipo de flexibilidade, três funções são utilizadas para a relação de pertinência do grau de desconhecimento de forma a classificá-lo como baixo, médio ou alto. A função de pertinência para classificação do valor como baixo é

$$\mu(xb) = \begin{cases} 1 & xb \le 0 \\ \dfrac{0{,}5 - xb}{0{,}5} & 0 < xb \le 0{,}5 \\ 0 & xb > 0{,}5 \end{cases}$$

A função de pertinência para a classificação do valor como médio é

$$\mu(xm) = \begin{cases} 0 & xm \le 0 \\ \dfrac{xm}{0{,}5} & 0 < xm \le 0{,}5 \\ \dfrac{1 - xm}{0{,}5} & 0{,}5 < xm \le 1 \end{cases}$$

A função de pertinência para a classificação do valor como alto é

$$\mu(xa) = \begin{cases} 0 & xa \le 0{,}5 \\ \dfrac{xa - 0{,}5}{0{,}5} & 0{,}5 < xa \le 1 \end{cases}$$

A representação gráfica das três funções é apresentada na figura 24, abaixo.

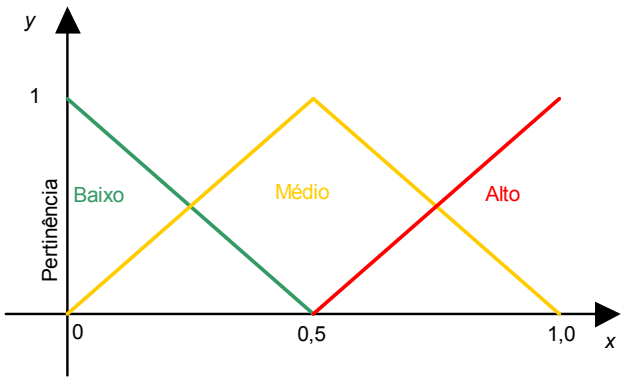


Figura 24 – Representação das funções de pertinência para baixo, médio e alto

É importante observar que, existem três possíveis resultados para o grau de desconhecimento que indicam o quão baixo, médio ou alto ele está. Estes três resultados podem ser tratados como três variáveis *fuzzy* diferentes, como desconhecimento baixo, desconhecimento médio e desconhecimento alto. Em um sistema *fuzzy,* estes três resultados irão ativar um conjunto de regras, dentre as quais uma apenas deverá ser adota, de acordo com o grau de confiança calculado em função das outras variáveis também envolvidas nas regras [BEC 98]. Uma forma de minimizar a ativação de mais

de uma regra, neste caso, seria a adoção de uma operação lógica *fuzzy* OR entre os valores resultantes do grau de desconhecimento. Esta operação resulta no valor máximo entre os operandos, portanto resultaria na informação com maior peso atribuído pela função de pertinência. Um dos problemas encontrados nesta abordagem é a perda da informação semântica a respeito da variável *fuzzy*, que passa a ser tratada como um valor único. O problema é que, dependendo do valor ser baixo, médio ou alto, uma regra específica deverá ser acionada, logo o grau de desconhecimento não pode ser representado por um valor condensado.

A média e o desvio padrão não se comportam como o grau de desconhecimento. Esses valores não são normalizados e são extremamente dependentes do volume de dados do perfil de cada usuário. Mesmo utilizando-se formas de normalização, ainda não é possível tratá-los da mesma forma, pois as médias e desvios não são usados para comparação de perfis entre usuários. Logo, não é possível dizer que uma média é baixa, média ou alta, pois a média de um usuário X, pode ser menor que a de um usuário Y em valores absolutos, e mesmo assim as duas médias serem consideradas normais individualmente para cada usuário.

No entanto, se considerarmos o comportamento destas variáveis, ou seja, se elas crescem ou decrescem, essa sim é uma medida que pode ser tratada de forma *fuzzy*, a exemplo dos sistemas de controle de temperatura. Ainda assim, no tratamento de média e desvio padrão existe um complicador a mais além do comportamento. Deseja-se também observar os valores que elas assumem, pois também devem determinar a ocorrência de situações de suspeição. Pois um indivíduo, mesmo que apresente um comportamento que leva ao decremento desses valores, enquanto estiver acima de um valor de referência da média, continuará a ser suspeito.

Assim optou-se pela utilização de uma função linear para a relação de pertinência dos valores de média e desvio padrão. Cada usuário tem uma média e desvio de referência, que são a média e o desvio somente de seus perfis históricos e nenhum acesso local. A relação de pertinência para média, tanto do perfil histórico do usuário, quanto do perfil histórico da rede, é dada por

$$\mu(x) = \begin{cases} 0 & x \leq 0 \\ \dfrac{x}{2\overline{X}} & 0 < x < 2\overline{X} \\ 1 & x \geq 2\overline{X} \end{cases}$$

A função linear é dada pela reta apresentada na figura 25, abaixo.

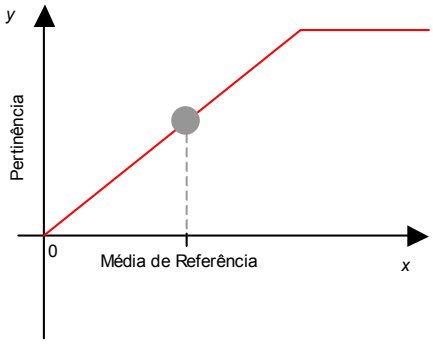


Figura 25 – Representação de função de pertinência μ(x)

A função acima irá resultar em um peso baixo para a média, quando esta estiver abaixo da média de referência. Isto significa que o usuário não é suspeito e está executando acessos conhecidos. Isto é, enquanto o usuário executa ações conhecidas, a média tende a zero, não é considerado suspeito. Se o usuário fica por um longo período ativo e executando acessos pertinentes ao seu perfil, a tendência é que a média volte a crescer. O sistema deve então determinar qual o crescimento limite aceitável e a partir para passar a considerar o usuário suspeito. Considera-se aceitável o crescimento de uma vez a média, que o leva até o valor da média de referência. Os casos em que o usuário ultrapassa essa média são considerados suspeitos, independente do período de atividade na rede. Então variações acima da média do usuário irão disparar as regras, pois o peso associado é maior que o peso associado à média de referência e irá ser mais significativo na regra *fuzzy*.

Há casos, conforme apresentado, em que a média irá decrescer, mesmo que o usuário esteja executando um número de acessos, a um determinado destino, maior que o normal para o seu perfil e não esteja fazendo acessos ou esteja fazendo muito poucos acessos a outros destinos, também pertencentes ao seu perfil. Esses casos devem ser alertados como suspeitos e serão identificados pela variação do desvio e não da média. Nestes casos, o desvio será maior que o desvio de referência, e, portanto, aplicando-se a mesma função linear para a relação de pertinência. Aplicada a média, um peso

significativo será atribuído ao desvio e irá ativar a regra adequada para o tratamento da situação.

Conforme citado anteriormente, a mesma função linear é utilizada para a relação de pertinência do desvio padrão, substituindo-se a média pelo desvio, da seguinte forma

$$\mu(x) = \begin{cases} 0 & x \leq 0 \\ \dfrac{x}{2\sigma} & 0 < x < 2\sigma \\ 1 & x \geq 2\sigma \end{cases}$$

Os valores resultantes das funções de pertinência são analisados através da utilização de regras *fuzzy*, combinando então as medidas de grau de desconhecimento, média em relação ao perfil histórico do usuário, desvio em relação ao perfil histórico do usuário, média em relação ao perfil histórico da rede e desvio padrão em relação ao perfil histórico da rede.

A combinação das variáveis irá resultar na ativação de mais de uma regra. Essa combinação é feita utilizando-se um AND *fuzzy* que resulta no valor mínimo entre os valores avaliados. Quando duas ou mais regras são ativadas utiliza-se um OR *fuzzy*, que seleciona o maior valor entre os valores avaliados, portanto será selecionada a regra que tem o maior grau de confiança [BEC 98]. A regra selecionada irá disparar a política adequada à situação.

As variáveis podem ser combinadas manualmente, por um ou vários especialistas, construindo-se grafos de conhecimento [LEA 90]. Outra abordagem seria a utilização de mecanismos automáticos de aprendizado, por exemplo, utilizando-se sistemas de aprendizado indutivo ou dedutivo da área de inteligência artificial simbólica [COH 95], ou mesmo o aprendizado por redes neurais artificiais [MAC 90] [BEC 02].

A utilização de mecanismos *fuzzy* neste trabalho é interessante, pois na sua essência apresenta um sistema que não aceita somente os valores falso ou verdadeiro como resposta. No trabalho apresentado por este volume, a utilização de um sistema flexível e sensível às variações das medidas do sistema é desejável para que se possa executar ações condizentes e de níveis de segurança diferenciados de acordo com as alterações de comportamento como um todo para obter-se uma melhor sintonia do sistema.

Uma das desvantagens em relação à aplicação da abordagem *fuzzy* é a quantidade de combinações possíveis caso o número de variáveis observadas crescer.

4.4 Exemplo da Utilização do Sistema de Regras Fuzzy

Para exemplificar os valores que irão assumir as variáveis *fuzzy* e as regras que possivelmente serão disparadas pelo sistema, utilizou-se os dados do primeiro usuário monitorado como exemplo. Este é apenas um exemplo e não tem a intenção de demonstrar a aplicação exaustiva das regras *fuzzy* a todos os usuários monitorados.

O comportamento do primeiro usuário, referentes às variações da média, do desvio padrão e grau de desconhecimento foi apresentado anteriormente. O primeiro gráfico apresentado na figura 8 e também na figura 28, utilizando escala logarítmica, refere-se ao primeiro dia de atividade do usuário. Nesta representação observa-se que o grau de desconhecimento do usuário é alto durante todo o tempo e ocorrem alterações nos valores de média e desvio padrão do perfil da rede. A tabela 5 apresenta os valores iniciais para as variáveis estatísticas calculadas em relação às ações iniciais do usuário.

Tabela 5 – Valores iniciais do primeiro dia de monitoração

Acesso	Média P. Usuário	Desvio P. Usuário	Grau de Desc.
1	0	0	1
2	0	0	1
3	0	0	1
4	0	0	1
5	0	0	1
...	...	...	...

Isto ocorre, no primeiro dia, pois o perfil do usuário está vazio e os seus acessos são desconhecidos. Os valores para média e desvio padrão do perfil da rede assumem seus valores de referência, pois o usuário também não faz acessos pertencentes a este perfil. A função de pertinência *fuzzy* para o grau de desconhecimento resulta nos valores apresentados na tabela 6.

Tabela 6 – Resultados da função de pertinência para o grau de desconhecimento.

Acesso	μ (xb)	μ (xm)	μ (xa)
1	0	0	1
2	0	0	1
3	0	0	1
4	0	0	1
5	0	0	1

Na tabela 7 são apresentados os resultados das funções de pertinência para média e desvio padrão em relação ao perfil do usuário e para o perfil da rede.

Tabela 7 – Resultados das funções de pertinência para média e desvio padrão.

Acesso	Média P. Usuário	Desvio P. Usuário
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0

Conclui-se a partir da observação dos resultados das funções de pertinência que, quando qualquer uma das variáveis for zero, a combinação da variável em questão com as demais, em uma regra AND *fuzzy*, resultará em zero. No exemplo apresentado nas tabelas 6 e 7, vê-se que os acessos do usuário são desconhecidos, pois a função de pertinência para grau de desconhecimento alto resulta em 1. Sendo assim, se combinadas todas as variáveis em um AND *fuzzy* os resultados serão zero. Logo, não será possível concluir nada a respeito do usuário, ou ainda, poderá se chegar à conclusão errônea.

Portanto, quando o usuário é novo no sistema, ou seja, não possui perfil histórico, o sistema deve solicitar um segundo nível de autenticação imediatamente, sem disparar o sistema de regras. Outra possibilidade é utilizar o grau de desconhecimento como um gatilho, ou seja, ele é utilizado sem combinações com outras variáveis para a ativação das regras. Assim, no caso do usuário novo para o sistema, com grau de desconhecimento alto, a regra gatilho irá testar apenas o grau de desconhecimento.

Outra variável que deve ser utilizada como gatilho é o desvio padrão, pois alterações de comportamento são rapidamente refletidas por esta medida. Por exemplo, no caso de acessos intensos a um único destino e serviço do perfil poderá ocorrer uma diminuição da média e o aumento do desvio padrão, pois a amplitude total diminui (ver

capítulo 3 figura 2). O valor baixo para a média irá refletir em um peso baixo para a média e um peso alto para o desvio, conforme a função de pertinência utilizada para eles. Na execução do AND *fuzzy*, combinando-se as três variáveis, o valor da média baixa será selecionado como saída das regras. Uma saída baixa indicará um baixo grau de suspeição com relação às atitudes do usuário. Esta não é uma situação desejável, pois o desvio alto indica que o usuário é suspeito. Então se conclui que o desvio padrão também deve ser utilizado como gatilho.

A observação do comportamento do usuário no final do período de monitoração mostra que, apesar do usuário ter feito alguns acessos pertencentes ao perfil da rede, eles não foram suficientes para reduzir o grau de desconhecimento em relação a este usuário. Os valores obtidos para os últimos acessos do usuário são apresentados na tabela 8.

Tabela 8 – Valores referentes aos últimos acessos do usuário no primeiro dia

Acesso	Média P. Usuário	Desvio P. Usuário	Média P. Rede	Desvio P. Usuário	Grau de Desc.
8998	0	0	36,428571000	44,324100000	0,984765000
8999	0	0	36,428571000	44,324100000	0,984766000
9000	0	0	36,428571000	44,324100000	0,984767000

Os valores das funções de pertinência para o grau de desconhecimento, a média e o desvio padrão para os valores da tabela 8 são apresentados na tabela 9.

Tabela 9 – Resultados das funções de pertinência

Acesso	μ (xb)	μ (xm)	μ (xa)	Média P. Usuário	Desvio P. Usuário	Média P. Rede	Desvio P. Usuário
8998	0	0,0304700	0,9695300	0	0	0,364286	0,136103
8999	0	0,0304680	0,9695320	0	0	0,364286	0,136103
9000	0	0,0304660	0,9695340	0	0	0,364286	0,136103

Observa-se que os últimos acessos do usuário foram a destinos e serviços desconhecidos, pois ocorreram alterações nos valores do grau de desconhecimento, conforme os dados da tabela 8, e também houve oscilação nas funções de pertinência μ(xa) e μ(xm), conforme os dados da tabela 9. Os resultados da tabela 9 mostram que o grau de desconhecimento pode ser alto, pois o grau de confiança para alto é maior do que para médio.

O usuário por ser novo no sistema com comportamento desconhecido, mantendo assim o grau de desconhecimento alto. A cada aplicação do sistema de regras, o resultado seria de indicação de suspeição e de execução de nova autenticação, bloqueio de serviços, etc. Mas na prática esse tipo de ação seria extremamente inconveniente para o usuário e também para o sistema, pois a cada pacote o usuário seria solicitado para executar uma autenticação, ou teria o serviço bloqueado, mesmo sendo um usuário legítimo. Então se conclui que o sistema necessita de regras adicionais que permitam verificar se o usuário já foi autenticado pelo sistema em um ou mais níveis e se a autenticação ainda é válida. Por exemplo, pode-se dizer que cada autenticação do usuário é válida por um período X de tempo e espirado o tempo ele será novamente consultado se o grau de desconhecimento se mantiver alto.

Os resultados das variáveis estatísticas referentes à monitoração do usuário no segundo dia de atividade foram apresentados na figura 9, e na figura 29 em escala logarítmica. Os resultados numéricos das variáveis para os acessos iniciais do usuário são apresentados na tabela 10. De acordo com o que foi observado no gráfico, verifica-se que o usuário executou acessos já conhecidos, pois o grau de desconhecimento permanece em zero e a média e o desvio padrão em relação do seu perfil decrescem.

Os resultados das funções de pertinência *fuzzy* são apresentados na tabela 11. A tendência da função de pertinência para o grau de desconhecimento é manter-se igual aos valores apresentados, pois o usuário não executa acessos a destinos e serviços desconhecidos. O mesmo ocorre para os valores das funções de pertinência da média e do desvio padrão em relação aos acessos do perfil da rede. Enquanto que, os valores das funções de pertinência da média e do desvio padrão em relação ao perfil do usuário devem decrescer. O que se observa é que aumenta o grau de confiança na legitimidade do usuário.

O resultado da aplicação das regras *fuzzy* seria a seleção da regra que representa a média e desvio padrão em condições normais para o usuário e grau de desconhecimento baixo com alto grau de confiança ($\mu(xb)$). As demais combinações entre $\mu(xm)$ e $\mu(xa)$ resultariam em zero, sendo selecionada a regra que contém $\mu(xb)$ na combinação com grau de confiança de aproximadamente 0,49.

Tabela 10 – Valores das variáveis estatísticas no 2º. dia de monitoração

Acesso	Média P. Usuário	Desvio P. Usuário	Grau de Desc.
1	275,35294100	2075,93350300	0
2	275,33333300	2075,78165900	0
3	275,31372500	2075,62981600	0
4	275,29411800	2075,47797300	0
5	275,27451000	2075,32612900	0
6	275,25490200	2075,17428600	0
7	275,23529400	2075,02244300	0
8	275,21568600	2074,87060000	0
9	275,19607800	2074,71875600	0
10	275,17647100	2074,56691300	0
11	275,15686300	2074,41507000	0
12	275,13725500	2074,26322600	0
13	275,11764700	2074,11138300	0
14	275,09803900	2073,95954000	0
15	275,07843100	2073,80769600	0
16	275,05882400	2073,65585300	0
17	275,03921600	2073,50401000	0
18	275,01960800	2073,35216600	0
19	275,00000000	2073,20032300	0
20	274,98039200	2073,04848000	0
21	274,96078400	2072,89663700	0
22	274,94117600	2072,74479300	0
23	274,92156900	2072,59295000	0
24	274,90196100	2072,44110700	0
25	274,88235300	2072,28926300	0
26	274,86274500	2072,13742000	0
27	274,84313700	2071,98557700	0
28	274,82352900	2071,83373400	0
29	274,80392200	2071,68189000	0
30	274,78431400	2071,53004700	0
31	274,76470600	2071,37820400	0
32	274,74509800	2071,22636000	0
33	274,72549000	2071,07451700	0
34	274,70588200	2070,92267400	0
35	274,68627500	2070,77083100	0
36	274,66666700	2070,61898700	0
37	274,64705900	2070,46714400	0
38	274,62745100	2070,31530100	0
39	274,60784300	2070,16345800	0
40	274,58823500	2070,01161400	0
...	...	...	...

Tabela 11 – Resultado das funções de pertinência no início do 2º. dia de monitoração

Acesso	μ (xb)	μ (xm)	μ (xa)	Média P. Usuário	Desvio P. Usuário
1	1	0	0	0,499964395	0,499963428
2	1	0	0	0,499928790	0,499926855
3	1	0	0	0,499893186	0,499890283
4	1	0	0	0,499857581	0,499853711
...	...	...	...	...	...

No momento em que a média e o desvio atingem os valores mais baixos, os valores numéricos exatos das variáveis são apresentados na tabela 12.

Tabela 12 – Valores mais baixos assumidos por média e desvio padrão do usuário

Acesso	Média P. Usuário	Desvio P. Usuário	Grau de Desc.
16788	6,05882400	26,37022400	0,140004000
16789	6,05882400	26,37022400	0,140058000
16790	6,05882400	26,37022400	0,140111000
16791	6,05882400	26,37022400	0,140165000
16792	6,05882400	26,37022400	0,140219000
16793	6,05882400	26,37022400	0,140273000
16794	6,05882400	26,37022400	0,140327000
16795	6,98039200	78,77282300	0,142602000
16796	7,00000000	78,92110000	0,142593000
16797	7,01960800	79,06939100	0,142585000
16798	7,03921600	79,21769500	0,142576000
16799	7,05882400	79,36601300	0,142568000
16800	7,07843100	79,51434400	0,142560000
16801	7,09803900	79,66268900	0,142551000
16802	7,11764700	79,81104600	0,142543000

Observa-se que este é o ponto exato em que a média e o desvio padrão atingem os seus valores mais baixos e a seguir voltam a crescer, pois o usuário provavelmente está executando um número maior de acessos do que os registrados no seu perfil. Os valores das funções de pertinência correspondentes são apresentados na tabela 13.

Conforme pode ser observado, o desvio padrão cresce, mas não representa crescimento exagerado podendo-se considerar como normal o comportamento do usuário, neste momento. Neste caso, o desvio não será utilizado como gatilho porque o valor da sua função de pertinência ainda é baixo. Uma questão em aberto neste caso é qual o limiar de valores para que o desvio padrão seja usado como gatilho. A necessidade de utilizar-se o desvio como gatilho leva a uma modelagem diferenciada da

sua função de pertinência. Uma função adequada, neste caso, é a função trapezoidal semelhante a que foi utilizada para o grau de desconhecimento. O desvio padrão é classificado como alto, médio ou baixo, tendo como parâmetro de valor médio o desvio padrão inicial do perfil (desvio de referência). O desvio utilizado como gatilho é o desvio considerado alto.

Tabela 13 – Resultado das funções de pertinência para os dados da tabela 12

Acesso	μ (xb)	μ (xm)	μ (xa)	Média P. Usuário	Desvio P. Usuário
16788	0,7199920	0,2800080	0	0,011001924	0,006351413
16789	0,7198840	0,2801160	0	0,011001924	0,006351413
16790	0,7197780	0,2802220	0	0,011001924	0,006351413
16791	0,7196700	0,2803300	0	0,011001924	0,006351413
16792	0,7195620	0,2804380	0	0,011001924	0,006351413
16793	0,7194540	0,2805460	0	0,011001924	0,006351413
16794	0,7193460	0,2806540	0	0,011001924	0,006351413
16795	0,7147960	0,2852040	0	0,012675354	0,018972868
16796	0,7148140	0,2851860	0	0,012710959	0,019008581
16797	0,7148300	0,2851700	0	0,012746564	0,019044298
16798	0,7148480	0,2851520	0	0,012782170	0,019080017
16799	0,7148640	0,2851360	0	0,012817775	0,019115741
16800	0,7148800	0,2851200	0	0,012853378	0,019151467
16801	0,7148980	0,2851020	0	0,012888983	0,019187197
16802	0,7149140	0,2850860	0	0,012924589	0,019222929

4.5 Comparação do Sistema de Regras

Os dois métodos, regras simples e regras *fuzzy*, podem ser utilizados, pois ambos oferecem condições para a avaliação de eventos e definição das ações a serem executadas. Além disso, ambos permitem a associação com políticas, de forma que o sistema é flexível e ajusta-se às condições de segurança locais.

A diferença entre eles é que o primeiro modelo pode ser mais sensível às alterações de comportamento que o segundo. No primeiro, eventos são avaliados individualmente. No segundo, consideram-se todos os valores para determinar a política a ser executada. Além disso, no primeiro os alertas são gerados mais rapidamente, bem como as políticas são disparadas mais rapidamente, mas em compensação pode gerar um elevado número de alarmes falsos positivos. Enquanto que, no segundo modelo, o processamento deve ser mais lento, pois todas as regras devem ser executadas e também pode gerar um maior número de falsos negativos.

4.6 Ações do Sistema de Detecção de Intrusão

As ações são referenciadas como políticas adotadas no sistema de regras, quando detectadas situações de intrusão. As ações executadas neste sistema são em sua maioria ações de verificação das credenciais do usuário e contramedidas que visam garantir que usuários ilegítimos ou maliciosos tenham acesso aos recursos do sistema. Portanto, o sistema de detecção de intrusões ao identificar uma situação de intrusão verdadeira ou de suspeição, deverá executar medidas que bloqueiem o acesso do usuário suspeito aos recursos ou, em caso de suspeição apenas, execute ações de verificação para nova validação da identidade do usuário.

Além destas ações, é necessária a execução de medidas de liberação de recursos. De acordo com as variações de comportamento do usuário, o sistema poderá bloquear alguns recursos até que o grau de legitimidade do usuário cresça, sendo necessário liberar o acesso e os serviços para aquele usuário.

Essas ações, no sistema de detecção de intrusão, serão executadas principalmente:

- Em *firewalls*, nos casos de bloqueio ou liberação de acesso aos serviços, pois eles são mecanismos que protegem os limites da rede de acessos indevidos, bem como o uso de recursos externos por usuários sem autorização;
- No *host* do usuário, nos casos de nova validação da sua identidade;
- Nas entidades de gerenciamento, nos casos de geração de alertas e relatórios.

Inicialmente, os tipos de ações identificadas como necessárias neste sistema são:

- Bloqueio/liberação total ou parcial do *firewall* para um determinado IP interno;
- Execução de processos de autenticação, com utilização de diversos níveis de autenticação e senhas diferenciadas para cada nível;
- Execução de processos de autenticação com solicitação de informações adicionais que auxiliam na identificação do usuário;
- Geração de alarmes pelo sistema de gerenciamento.

Outras contramedidas podem ser criadas pelo usuário e agregadas ao sistema. As ações podem ser implementadas na forma de fragmentos de código que serão

executados no sistema destino, ou seja, utilizando código móvel. Essa possibilidade torna o sistema mais flexível para alterações e adaptações em relação ao ambiente em que está sendo utilizado, bem como permite a fácil alteração das ações executas sem a necessidade de instalação de novas versões e/ou recompilação de código.

4.7 Gerenciamento baseado em Políticas

Segundo [GRA 01], uma política é, em essência, um conjunto de uma ou mais regras que descrevem ações que devem ser executadas quando condições especiais ocorrem na rede. Uma regra pode ser formada pela combinação de outras regras, e como conseqüência, uma política pode ser formada pela combinação de várias políticas.

A utilização de políticas para controle de sistemas torna-se interessante, pois oferecem flexibilidade ao sistema. Em sistemas de gerenciamento de redes a utilização de políticas vem sendo investigada por vários anos. O trabalho de gerenciamento baseado em políticas pioneiro foi desenvolvido na Imperial College London e atualmente os esforços acadêmicos na área são reconhecidos pelo IETF, sendo que este institui grupos de trabalho na área buscando padronizar o modelo de gerenciamento baseado em políticas. O modelo do IETF é apresentado em vários documentos que podem ser encontrados no *site* do IETF (http://www.ietf.org/html.charters/policy-charter.html) . A expectativa é que o modelo de políticas seja inicialmente utilizado no gerenciamento de QoS, mas o modelo é suficientemente genérico para ser utilizado para qualquer outra área de gerenciamento.

A arquitetura genérica para gerenciamento baseado em políticas (*PBNM – Policy Based Network Management*), definida pelo IETF é apresentada na figura 26.

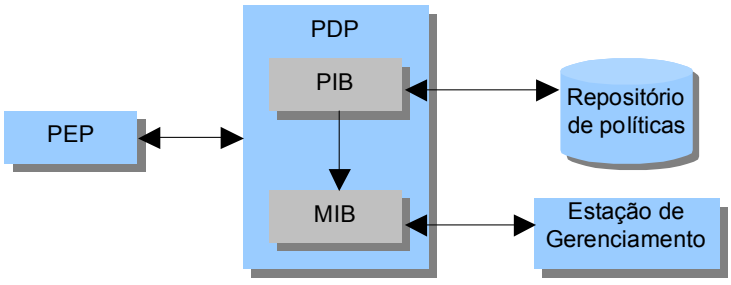


Figura 26 – Arquitetura de gerenciamento baseado em políticas

Os PEPs (*Policy Enforcement Points*) são os pontos de ação, onde são aplicadas as políticas definidas no sistema. Os PDP (*Policy Decision Point*) são os pontos que tomam as decisões, baseados nas políticas recuperadas do repositório de políticas. As políticas são armazenadas em um repositório de políticas. E em cada PDP existe uma base de políticas, denominada PIB (*Policy Information Base*), para a representação das políticas. E as políticas são armazenadas em um repositório de políticas, que segundo a definição do IETF deve ser um servidor LDAP.

Neste modelo, as estações de gerenciamento têm acesso às políticas através da PIB de cada PDP, utilizando-se o protocolo SNMP. Mas é necessário que ocorra um mapeamento da PIB para o formato de uma MIB de forma a tornar transparente o acesso das políticas pelas entidades SNMP.

Neste trabalho, o conceito de políticas está associado à ação que será executada pelo sistema quando uma determinada situação for detectada, de acordo com a literatura de sistemas de detecção de intrusão. Mas esta abordagem pode ser adaptada ao de gerenciamento baseado em políticas do IETF, que considera uma política como sendo uma regra seguida por uma ação, e não somente a ação. A adaptação dos modelos de regras ao conceito de políticas de gerenciamento não apresenta dificuldades, pois na prática são implementados de forma similar. Essa adaptação tem como vantagem a integração do sistema de detecção de intrusão proposto com um modelo de gerenciamento SNMP.

No sistema de detecção de intrusão, a entidade de decisão, ou seja, o PDP, é a entidade que realiza a análise de dados do sistema de detecção de intrusão e detecta os eventos suspeitos. Os PEPs são as entidades de ação, pois são responsáveis pela execução das ações em entidades como *firewalls*, roteadores, *proxies*, *hosts*, etc. Os PEPs podem estar localizados no próprio local onde deve ser executada a ação, ou mesmo no PDP. Tipicamente os PEPs estão localizados próximo aos limites administrativos da rede, ou seja, próximos aos equipamentos que serão configurados para controle do tráfego.

Então, por exemplo, no caso de detecção de um usuário ilegítimo, o tráfego para este usuário deve ser bloqueado, não permitindo que ele continue utilizando os serviços da rede. O PDP detecta o evento e o PEP dispara a ação a ser executa, ou seja, o bloqueio do *firewall* para o tráfego daquele usuário. O PEP envia a solicitação de

bloqueio ao *firewall* através de mecanismos específicos para comunicação com o *firewall*, ou através de operações SNMP *Set-Request*, caso ele seja gerenciável.

Uma das vantagens de integrar o sistema de detecção de intrusões à aplicação de gerenciamento SNMP, e em especial utilizar o gerenciamento baseado em políticas, é facilitar ao usuário administrador a interação com o sistema. Isto é, facilitar o acesso às informações resultantes e à configuração de informações, especialmente à configuração do conjunto de políticas do sistema. Além disso, a integração oferece a possibilidade de utilização de uma interface única para gerenciamento do ambiente, facilitando a operação do sistema para o usuário.

5 Integrando o IDS com o Gerenciamento SNMP

Existe na área de controle de segurança em redes de computadores uma clara separação das funções executadas pela aplicação de gerenciamento de redes SNMP e pelos sistemas de detecção de intrusão. Estes mecanismos são tradicionalmente implementados por ferramentas diferentes. E desta forma, não se obtém uma visão unificada dos eventos da rede, além de inibir a construção de sistemas de correlação de dados e alarmes.

Em [QIN 02], o autor apresenta um modelo para a integração de sistemas de detecção de intrusões e a aplicação de gerenciamento de redes. Ele apresenta como solução um sistema integrado com vários níveis de correlação de informações e um modelo informacional unificado, para que as informações obtidas por diversos módulos de monitoração de sistemas sejam integradas em uma visão única e mais abrangente do sistema.

Neste trabalho, propõe-se a integração parcial do sistema de detecção de intrusões com a aplicação de gerenciamento SNMP, pois não emprega correlação de dados e alarmes, conforme apresentado em [QIN 02]. Este trabalho propõe: a criação de um sistema integrado que possibilite a interação com o sistema de detecção de intrusão a partir de um gerente SNMP; a utilização, por parte dos módulos do sistema, do protocolo de gerenciamento SNMP para comunicação; e a especificação de um modelo informacional SNMP para o sistema de detecção de intrusões. Contudo o sistema apresentado considera a integração apenas parcial, pois não emprega correlação de dados e alarmes, conforme apresentado em [QIN 02].

A integração propicia, em primeira instância, a utilização de uma interface comum para acesso às informações do sistema de detecção de intrusão e da aplicação de gerenciamento de redes. Os demais benefícios advêm da integração do gerenciamento de segurança, fortemente baseado no controle de acesso, e do sistema de detecção que monitora o comportamento dos usuários e que controla dinamicamente os direitos de acesso de um usuário.

O sistema prototipado implementa o mecanismo de autenticação de usuário, o mecanismo de controle de acessos aos recursos da rede e o agente para a detecção de intrusões, de acordo com o método proposto neste trabalho. Os módulos funcionam de

forma integrada para propiciar o controle de acesso e a monitoração do comportamento dos usuários em uma rede. Além disso, a implementação das entidades de acordo com o modelo de gerenciamento SNMP, permite a integração do sistema aos ambientes de gerenciamento SNMP.

A figura 27 apresenta uma visão dos módulos que compõe o sistema e sua comunicação.

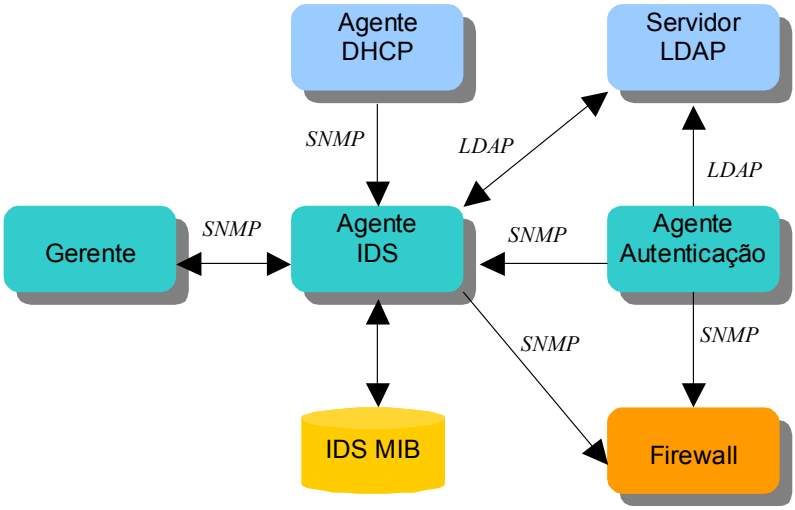


Figura 27 – Visão geral dos módulos

Os usuários devem, em primeiro lugar, ser autenticados para terem acesso aos recursos e serviços da rede. Neste caso, utiliza-se um *webservice* de autenticação e um servidor LDAP. Após a autenticação, liberam-se as portas do *firewall* correspondentes aos serviços que os usuários tem acesso. A liberação é solicitada pelo agente autenticador diretamente ao *firewall*. Esse agente informa simultaneamente ao agente IDS sobre a entrada de um novo usuário na rede, passando a ele as informações sobre o ID do usuário e o número IP do seu *host* [SIL 02]. O agente IDS passa a monitorar os passos do usuário na rede, observando os destinos e serviços que ele utiliza. Em casos de suspeição, uma das ações anteriormente descritas é acionada. No momento que o endereço do usuário é liberado, o agente DHCP sinaliza o agente IDS, que encerra a monitoração do usuário associado ao endereço IP liberado e envia o perfil do usuário para o seu domínio de origem.

A entidade agente IDS responde a um gerente SNMP através do qual o administrador do sistema pode consultar variáveis do sistema de detecção de intrusão,

configurar parâmetros, receber notificações do agente e configurar as políticas do sistema.

As entidades comunicam-se entre si utilizando protocolos variados, de acordo com a implementação de cada uma, sendo que uma entidade poderá utilizar mais de um protocolo de comunicação. A escolha do protocolo está associada à função a ser executada e à identificação da entidade com a qual se deve comunicar. A seguir as entidades são descritas separadamente.

5.1 Agente IDS

O agente IDS interage com o gerente SNMP, com o agente autenticador, com o agente DHCP e com o *firewall*. A comunicação com estas entidades utiliza o protocolo SNMPv3.

Esse agente foi implementado em linguagem C e é constituído por um módulo de captura de dados da rede, um módulo de geração e tratamento de operações SNMP, um módulo de análise estatística dos dados monitorados, e um módulo de regras que determina a ocorrência de intrusões e ativa a execução das ações do sistema.

O módulo de captura dos dados da rede implementa um *sniffer* de rede. Os dados capturados são enviados ao módulo de análise, que inicialmente constrói uma matriz de tráfego semelhante à matriz *alMatrixTable* da RMON II. É importante observar que a matriz é construída somente para os endereços IP dos usuários em observação. As informações contidas na matriz são

- Endereço IP de origem e destino;
- Protocolo encapsulado no protocolo IP;
- Porta de origem e destino.

Essas informações permitem mapear a comunicação entre pares de máquinas. As informações da tabela são utilizadas para detectar o número de acessos executados a determinados destinos e serviços. Um acesso caracteriza-se pelo número de conexões diferentes entre o mesmo IP de origem e de destino, e são diferenciadas pelo número da porta do cliente.

A cada vez que uma nova linha é adicionada à matriz de tráfego, o módulo de cálculos das medidas estatísticas é acionado. O resultado é submetido ao sistema de regras que poderá então determinar a execução de uma ação no sistema.

O módulo de análise necessita das informações do perfil do usuário para o cálculo das análises estatísticas e detecção dos desvios de comportamento. Os perfis necessários são os perfis da rede e o perfil de cada usuário monitorado. Esses perfis são obtidos da seguinte maneira:

- O perfil da rede é obtido na inicialização do sistema e atualizado periodicamente. O agente IDS é responsável por buscar os dados da rede do servidor LDAP na inicialização e periodicamente promover a sua atualização;
- O perfil do usuário é recebido do agente autenticador. Esse agente, quando realiza a autenticação do usuário com sucesso, recupera do servidor LDAP os dados do perfil que são enviados ao agente IDS.

O agente IDS, após a monitoração do usuário, é responsável por atualizar as informações do perfil de cada usuário para os usuários do domínio local, ou enviar o perfil monitorado localmente para uma entidade no domínio remoto, encarregada de executar a atualização.

O módulo SNMP está encarregado de receber as operações SNMP enviadas pelo gerente e pelos demais agentes e executar uma operação adequada para a situação, configurando variáveis no agente IDS e respondendo às solicitações de leitura das variáveis do agente. Além disso, esse módulo é responsável por gerar os alertas SNMP que são enviados ao gerente SNMP. O agente foi implementado utilizando-se o agente SNMP implementado em Java em [AND 02] e utilizado em [AND 03a] [AND 03b].

5.2 Agente de Autenticação

O servidor de autenticação foi implementado como um *webservice*, utilizando-se linguagem Java, protocolo UPnP e um agente SNMP Java, desenvolvido no trabalho de conclusão de curso apresentado em [AND 02].

O agente de autenticação foi projetado para ser um *webservice* no protótipo, pois está sendo utilizado para autenticação de usuários em uma rede *wireless*, na qual não é

exigida a prévia instalação e configuração de um cliente de autenticação nos *hosts* clientes da rede. Isso permite que usuários possam conectar-se à rede *wireless* com os seus próprios dispositivos *wireless* sem necessidade de prévia configuração.

Os clientes, ao conectarem-se à rede *wireless*, não têm acesso aos recursos locais da rede, nem da Internet. A rede está isolada da infra-estrutura da rede local cabeada por meio de um *firewall*, que encontra-se bloqueado até que o usuário seja autenticado e sejam estabelecidos seus direitos de acesso.

A implementação do agente de autenticação como um *webservice* UPnP permite que o cliente procure dinamicamente esse serviço ao ser configurado na rede. Esse agente solicita ao usuário sua identificação, senha e o domínio a que pertence, e então contata o servidor LDAP para autenticação do usuário. Em seguida, de acordo com a classe do usuário, ele terá acesso a um conjunto de serviços e recursos que terão o acesso liberado no *firewall* assim que a autenticação for efetuada com sucesso.

O agente de autenticação sinaliza ao agente IDS sobre a autenticação de novos usuários no sistema, para que eles sejam monitorados pelo sistema de detecção de intrusão. A monitoração do usuário pressupõe o conhecimento do perfil do usuário, pois implementa um sistema de detecção por anomalia. Os perfis são armazenados no servidor LDAP, devendo ser recuperados após a autenticação do usuário.

Há duas abordagens possíveis para esta implementação, uma é a execução do *download* do perfil pelo agente de autenticação e o envio posterior dos dados para o agente IDS. A segunda abordagem possível é a execução do *download* do perfil pelo próprio agente IDS. Há vantagens e desvantagens em ambas abordagens, por exemplo, na primeira deve ser feito *download* dos dados do LDAP para o agente e, após, enviados através de operações SNMP de *Set-Request* para o agente IDS. Isto causará mais tráfego na rede e obrigará o agente IDS a tratar o recebimento dos dados, que estão, possivelmente, fragmentados em vários pacotes SNMP. Entretanto o *download* sendo executado direto pelo agente IDS permite a implementação de uma classe em Java para consulta do LDAP. A utilização dessa classe em Java, por sua vez, implica na construção de uma JNI (*Java Native Interface*) para comunicação como o módulo em C do agente IDS. O agente de autenticação envia operações SNMP para o *firewall* para alterar a sua configuração, de forma a liberar as portas se serviço para o usuário autenticado.

5.3 Agente DHCP

O agente DHCP monitora a liberação de endereços IP em um servidor DHCP. Quando este agente detecta a liberação de endereços IP, ele envia uma notificação ao agente IDS para que este suspenda a monitoração de dados para o IP em questão, e inicie o processo de atualização do perfil do usuário e bloqueio do *firewall* para o IP indicado.

5.4 Gerente SNMP

O administrador tem acesso ao agente IDS e ao agente mediador através de um gerente SNMP. Esse gerente é capaz de executar operações SNMP nos agentes, bem como receber notificações SNMP geradas pelos agentes. Através do gerente o administrador da rede é capaz de configurar parâmetros, consultar informações e receber alarmes gerados pelo sistema.

Além disso, através do gerente, o administrador pode alterar as políticas adotadas no sistema. O gerente é capaz de consultar e atualizar o repositório de políticas, que são armazenadas em um servidor LDAP, de acordo com a especificação do IETF.

5.5 Resultados Obtidos

O protótipo está em utilização em uma rede interna ao laboratório de pesquisa CPSE (Centro de Pesquisa em Software Embarcado) na PUCRS, e aplicado ao controle de usuários da rede *wireless* do laboratório. Além disso, o módulo de captura de análise de dados foi utilizado para análise dos usuários em modo *off-line*. Isto é, foram capturados trechos de tráfego utilizando o *tcpdump*, e os testes foram submetidos ao agente IDS para levantamento de informações a respeito do perfil dos usuários e do comportamento das variáveis estatísticas utilizadas. Os testes foram realizados neste laboratório, pois o ambiente é controlado. Os resultados da monitoração foram discutidos no capítulo anterior.

6 Conclusões

Este trabalho apresentou uma técnica de detecção de intrusões baseada na utilização de métodos estatísticos para análise do comportamento de usuários, de forma a identificar se são usuários legítimos ou não. O sistema de detecção de intrusões apresentado é classificado como um sistema de detecção de anomalias, pois ele verifica desvios no comportamento do usuário, a partir do conhecimento sobre o comportamento considerado normal para o usuário. Este sistema também pode ser classificado com um NIDS (*Network Intrusion Detection System*), pois obtém as informações através da monitoração do tráfego da rede.

O primeiro objetivo deste trabalho era identificar e aplicar medidas estatísticas que poderiam ser utilizadas para a análise do comportamento, de forma a obter informações a respeito do desvio do comportamento do usuário em relação ao comportamento conhecido. O estudo das medidas estatísticas resultou na utilização da media e do desvio padrão para análise do comportamento do usuário. Apesar de serem medidas simples, elas demonstraram ser apropriadas para a detecção dos desvios de comportamento, quando analisado o comportamento momentâneo do usuário com o seu comportamento histórico. Outras medidas foram consideradas, mas algumas são muito sensíveis às variações no comportamento do usuário, como, por exemplo, a correlação numérica.

No contexto deste trabalho, quando um usuário faz acessos a destinos e serviços que constam do seu histórico e na mesma proporção de acessos, a média e o desvio padrão tendem a decrescer, indicando que o usuário reproduz o seu comportamento e é um usuário legitimo. Enquanto que, a média e o desvio padrão tendem a crescer para um usuário que faça acessos a destinos e serviços de forma desproporcional ao seu comportamento histórico.

Além das medidas de média e desvio padrão, foi utilizada a medida de grau de desconhecimento, proposta neste trabalho. Essa medida permite identificar quão desconhecidas são as ações do usuário em relação às atividades conhecidas. O grau de desconhecimento é a razão entre os acessos conhecidos e os acessos não conhecidos. Ele é um valor que varia entre [0,1], sendo que quanto mais próximo de um, maior é o desconhecimento em relação ao comportamento do usuário. Esta medida é necessária,

pois se o usuário não faz acesso aos destinos e serviços do seu histórico, a média e o desvio padrão não se alteram.

Outro fator importante a ser observado, na utilização destas medidas, é que elas devem ser analisadas tanto em relação ao valor, quanto em relação à tendência de comportamento, ou seja, se elas crescem ou decrescem. A observação do comportamento da medida pode acelerar o processo de detecção de um comportamento anormal, pois um usuário legítimo normalmente faz com que as medidas decresçam.

Em alguns trabalhos relacionados, os autores condensam as diversas medidas estatísticas obtidas, em um único valor, que é submetido a um conjunto de regras para avaliação. Neste trabalho, optou-se por não condensar as diversas medidas em uma única, pois considerou-se que haveria perda de informação e a utilização das medidas em separado oferece um conjunto mais rico de informações a respeito dos eventos do sistema. Esta escolha mostrou-se adequada para o sistema, pelo fato se poder ter uma visão mais abrangente dos eventos do sistema. Do ponto de vista computacional não deve haver um impacto severo, pois o número de variáveis avaliadas é pequeno.

O segundo objetivo deste trabalho era identificar as informações básicas e necessárias para identificação do comportamento do usuário. As informações a respeito do comportamento do usuário são utilizadas para formar o comportamento histórico do usuário, chamado de perfil. A utilização de um perfil é necessária nos métodos de detecção de anomalias, pois é preciso comparar o comportamento momentâneo com o comportamento conhecido e considerado normal. A observação do usuário, neste trabalho, permitiu concluir que as informações sobre os destinos e serviços a que o usuário acessa e o número de acessos que ele faz, permitem a identificação do comportamento do usuário. As informações coletadas formam o perfil do usuário.

Durante o estudo sobre o comportamento do usuário, identificou-se que era necessário criar um perfil da rede, ou seja, monitorar o comportamento de todos os usuários daquele ambiente e tratá-lo como o perfil da rede. Essa necessidade deve-se ao fato de que um usuário pode variar o seu comportamento de acordo com o ambiente em que ele está. Por exemplo, o usuário pode ser estimulado, por fatores externos e próprios do ambiente, a fazer acesso a um determinado destino e serviço. Isso passa a ser uma característica comum ao ambiente, e o usuário não é, necessariamente, ilegítimo por isso.

Uma questão relacionada ao tratamento dos perfis é a manutenção das informações para que as informações a respeito do comportamento do usuário estejam sempre atualizadas. O procedimento de manutenção das informações é extremamente importante, pois o uso de informações desatualizadas invalida o processo de detecção de alterações no comportamento do usuário. Assim, as informações do perfil de cada usuário são processadas periodicamente e passam por um processo de "envelhecimento" e de inclusão de novas informações a respeito dos destinos e serviços utilizados. O envelhecimento é necessário para que informações sobre destinos e serviços que não estão sendo mais utilizados pelo usuário não tenham um grande peso no sistema e também para que sejam retiradas do perfil, após algum tempo. A inclusão de novas informações é necessária para que sejam conhecidos os destinos e serviços que o usuário tem utilizado mais recentemente.

O terceiro objetivo deste trabalho era utilizar um sistema de regras para a avaliação das medidas, para constatação de eventos suspeitos e determinação da contramedida a ser executada. A utilização de um sistema de regras torna o sistema flexível em relação à configuração das contramedidas. O sistema de regras permite inclusive a agregação do sistema de detecção de intrusões a um sistema de gerenciamento baseado em políticas. Essa agregação dá flexibilidade ao sistema, pois permite a configuração das contramedidas através de interface de alto nível para o usuário.

Além disso, constatou-se que o sistema de regras a ser utilizado pode ser tanto um sistema de regras simples, quanto um sistema de regras *fuzzy*. A escolha de um ou outro método depende da sensibilidade esperada do sistema. A utilização de um sistema *fuzzy* permite a detecção mais refinada dos eventos, pois as medidas são analisadas de acordo com o seu grau de confiabilidade.

Enfim, a execução deste trabalho comprovou que a utilização de medidas simples como média e desvio são capazes de apontar alterações do comportamento do usuário, e que um usuário pode ser monitorado através dos destinos e serviços a que ele faz acessos.

Após a conclusão deste trabalho, verifica-se que trabalhos futuros a serem desenvolvidos podem considerar o refinamento das informações contidas no perfil, a utilização de outros métodos de avaliação das medidas, como a utilização de redes

neurais e pode-se investigar outras abordagens para a análise do comportamento do usuário, como a construção de um "mapa" mais detalhado do comportamento do usuário. Por exemplo, usando estruturas de grafos, e a implementação de um método de comparação dessa estrutura para determinar a semelhança entre comportamentos. Outros trabalhos futuros podem envolver o refinamento da integração deste sistema ao gerenciamento baseado em políticas, a integração deste sistema com outros sistemas de detecção de intrusão, e a aplicação de mecanismos de correlação de dados para maior compreensão dos eventos dos sistemas.

Referências Bibliográficas

[ALA 01] ALA-LAURILA, Juha; at all. Wireless LAN Access Network Architecture for Mobile Operator. **IEEE Communications Magazine**. V. 39, n.11, p. 82 –89, Nov. 2001.

[AND 02] ANDREOLLI, Andrey; RODRIGUES, Fábio. **Gerenciamento de Protocolo BGP em Pontos de Troca de Tráfego**. Trabalho de Conclusão. Faculdade de Informática, PUCRS, 2002.

[AND 03a] ANDREOLLI, A.; RODRIGUES, F.; BERTHOLD, L; SILVA, Ana C. Benso; TAROUCO, Liane. **Gerenciamento de Roteamento em Pontos de Troca de Tráfego**. In: 15ª. REUNIÃO DO GRUPO DE TRABALHO DE ENGENHARIA E OPERAÇÕES DE REDE. 2003. Disponível por WWW em http://eng.registro.br/gter15 (10, Abr. 2003).

[AND 03b] ANDREOLLI, A.; RODRIGUES, F.; BERTHOLD, L; SILVA, Ana C. Benso; TAROUCO, Liane. **Sub-Agente para controle BGP na RNP.** In: 4º. WORKSHOP DA RNP2. 2003. Disponível por WWW em http://www.rnp.br/wrnp2/2003 (30, Mai. 2003).

[ANT 02] ANT, Allan. **Intrusion Detection System (IDSs): Perspective**. 2002. Disponível por WWW em http://security1.gartner.com (30, Ago. 2002).

[AXE 98] AXELSSON, Stefan. **Research in Intrusion-Detection Systems: A Survey**. 1998. Technical Report. Department of Computer Engineering. Chalmers University of Technology Göteborg. Sweden. Disponível por WWW em http://www.researchindex.com (30, Ago. 2002).

[BAL 02] BALFANZ, Dirk; SMETTERS, D. K.; STEWART, Paul; WONG, H. Chi. **Talking To Strangers: Authentication in Ad-Hoc Wireless Networks**. 2002. In: Network and Distributed System Security Symposium. Disponível por WWW em http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/ (30, Ago. 2002).

[BEC 02] BECKENKAMP, Fábio. G. **A Component Architecture for Artificial Neural Network Systems**. Tese de Doutorado. University of Konstance. Alemanha, 2002.

[BEC 98] BECKENKAMP, F.G.; PREE, W. and FELDENS, M. A. Optimizations of the Combinatorial Neural Model. In: 5th BRAZILIAN SYMPOSIUM ON NEURAL NETWORKS (SBRN'98). **Proceedings…** Belo Horizonte, Dez. 1998.

[BRO 01] BRONSTEIN, A., et all. Self-Aware Services: Using Bayesian Networks for Detecting Anomalies in Internet-based Services. In: IEEE/IFIP INTEGRATED NETWORK MANAGEMENT PROCEEDINGS. **Proceedings...** IEEE, p. 623-638, 2001.

[BUS 02] BÜSCHKES, Roland; KESDOGAN, Dogan; REICHL, Peter. How to Increase Security in Mobile Networks by Anomaly Detection. In: 14th COMPUTER SECURITY APPLICATIONS CONFERENCE. **Proceedings...** IEEE. p. 3 –1, 2002.

[CAB 01] CABRERA, J., et all, The Monitoring, Detection, Interpretation and Response Paradigm for the Security of Battlespace Netowrks. In: PROCEEDINGS OF MILCOM 2001. **Proceedings…** 2001. Disponível em http://www.milcom.org.(30, Ago. 2002).

[COH 95] CHOEN, Willian W. **Fast Effective Rule Induction**. 1995. In: 12th International Machine Learning Symposium. Disponível por WWW em http://www.researchindex.com (30, Ago. 2002).

[COO 02] COOLEN, R.; LUIJF, H. A. M. **Intrusion Detection: Generics and Stat-of-the-Art**. 2002. Technical Report. North Atlantic Treaty Organization. Disponível por WWW em http://www.tno.nl/instit/fel/ts/resources/rto-tr-049-ids.pdf (30, Ago. 2002).

[DEN 87] DENNING, D. E. An Intrusion-Detection Model. **IEEE Transaction on Software Engeneering.** V. 13, n. 2, p. x-x, Feb. 1987.

[DIC 00] DICKERSON, J.E.; DICKERSON, J.A. Fuzzy network profiling for intrusion detection. In: 19TH INTERNATIONAL CONFERENCE OF THE NORTH AMERICAN FUZZY INFORMATION PROCESSING SOCIETY. **Proceedings...** IEEE, p. 302-306, 2000.

[DIC 01] DICKERSON, J.E.; JUSLIN, J.; KOUKOUSOULA, O.; DICKERSON, J.A. Fuzzy intrusion detection. In: Joint 9th IFSA World Congress and 20th NAFIPS International Conference. **Proceedings...** IEEE, V. 3, p. 1506-1510, Jul 2001

[FIO 00] FIORESE, Marcelo. **Uma Proposta de Autenticação de Usuários para Ensino a Distância**. Dissertação de Mestrado. Instituto de Informática, UFRGS, 2000.

[GRA 01] GRANVILLE, Lisandro. **Gerenciamento Integrado de QoS em Redes de Computadores.** Tese de Doutorado. Instituto de Informática, UFRGS, 2001.

[HAR 03] HARRISON, R. **LDAP: Authentication Methods and Connection Level Security Mechanisms**.2003. Internet Draft, March. Disponível em http://www.ietf.org/html.charters/ldapbis-charter.html. (30, Ago. 2002)

[HEL 00] HELMER, Guy; WONG, Johnny; HONAVAR, Vasant; MILLER, Les. **Automated Discovery of Concise Predictive Rules for Intrusion Detection**. 2000. Disponível por WWW em http://www.researchindex.com (30, Ago. 2002).

[HEL 93] HELMAN, P.; LIEPINS, G. E. Statistical Foundations of Audit Trail Analysis for the Detection of Computer Misuse. **IEEE Transactions on Software Engineering**. V. 19, p. 886-901, Sep. 1993.

[JAV 91] JAVITZ, Harold S.; VALDES, Alfonso. The SRI IDES Anomaly Detector. In: IEEE COMPUTER SOCIETY SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY. **Proceedings…** IEEE, p. 316 –326, 1991.

[KEM 02] KEMMERER, R.A.; VIGNA, G. Intrusion detection: a brief history and overview. **Computer**. V. 35, n. 4, p. 27-30, Apr 2002

[KOH 86] KOHONEN, T. **Learning Vector Quantization for Pattern Recognition**. Technical Report, TKK-F-A601. University of Technology, Helsinki, 1986. Disponível por WWW em www.cis.hut.fi/~mikkok/dt.ps.gz (30, Mar. 2003).

[LEA 90] LEÃO, B. F. and ROCHA, A. F. Proposed Methodology for Knowledge Acquisition: A Study on Congenital Heart Disease Diagnosis. **Methods of Information in Medicine**. V. 29, n.1, p. 30-40, 1990.

[LEC 02] LECKIE C; and Kotagiri, R. A Probabilistic Approach to Detecting Network Scans. In: IEEE/IFIP NETWORK OPERATION AND MANAGEMENT SYMPOSIUM. **Proceedings…**IEEE, p. 359-372, 2002.

[LEE 99] LEE, Wenke; STOLFO, Salvatore; MOK, Kui W. A Data Mining Framework for Build Intrusion Detection Models. In: IEEE SYMPOSIUM ON SECURITY AND PRIVACY. **Proceedings…** IEEE, p. 120-132, 1999.

[LUO 01] LUO, J.; BRIDGE, Susan M.; VAUGHN, R. B., Fuzzy Frequent Episodes for Real-Time Intrusion Detection. In: Proceedings of IEEE 2001. **Proceedigs…**IEEE, v. 1, p. 368-371, 2001.

[MAC 90] MACHADO, R. J. and ROCHA, A. F. The combinatorial neural network: a connectionist model for knowledge based systems. **Uncertainty in Knowledge Bases**. Springer Verlag, 1990.

[MAN 02] MANIKOPOULOS, C.; PAPAVASSILIOU, C. Network Intrusion and Fault Detection: A statistical Anomaly Approach. **IEEE Communications Magazine**. V. 40, n. 10, p. 76-82, Out. 2002.

[MAR 01] MARIN, J.; RAGSDALE, Daniel; SURDU, J. A Hybrid Approach to the Profile Creation and Intrusion Detection. In: DARPA INFORMATION SURVIVABILITY CONFERENCE AND EXPOSITION (DISCEX II' 01). **Proceedings...** IEEE, v. 1, p. 69-76, 2001.

[MIS 01] Misra, Archan; at all. Autoconfiguration, Registration, and Mobility Management for Pervasive Computing. **IEEE Personal Communications**.V. 8, n. 4, p. 24-31, Ago. 2001.

[NET 03] Net SNMP, 2003. Disponível em http://net-snmp.sourceforge.net/

[NGU 99] NGUYEN, Hung; WALKER, Elbert. A. **A First Course in Fuzzy Logic**. Second Edition. USA: Chapman & Hall/CRC, 1999. 373 p.

[OLI 02] OLIVA, Caroline; PEREIRA, D.; MATSCHULAT, D. **NetClue –**

Intrusion Detection System. Trabalho de Conclusão. Faculdade de Informática, PUCRS, 2002.

[POR 98] PORRAS, Phillip A; VALDES, Afonso. **Live Traffic Analysis of TCP/IP Gateways**. In: Internet Society´s Networks and Distributed Systems Security Symposium. 1998. Disponível por WWW em http://zen.ece.ohiou.edu/~inbounds/DOCS/reldocs/EMERALDLT.html (30.,Aug. 2002).

[PTA 98] PTACEK, Thomas H.; NEWSHAM, Timony N. **Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection**. 1998. Disponível por WWW em http://www.researchindex.com (30, Ago. 2002).

[QIN 02] QIN, Xinzhou; LEE, Wenke; LEWIS, Lundy. Integrating Intrusion Detection and Network Management. . In: IEEE/IFIP Network Operation and Management Symposium. **Proceedings…**IEEE, p.329-344, 2002.

[SHE 02] SHERIF, J.S.; DEARMOND, T.G. Intrusion detection: systems and models. In: ELEVENTH IEEE INTERNATIONAL WORKSHOPS ON ENABLING TECHNOLOGIES: INFRASTRUCTURE FOR COLLABORATIVE ENTERPRISES. **Proceedings...** IEEE, p. 115 –133, 2002.

[SHR 00] SHROBE, Howard; DOLE, Hon; SZOLOVITS, Peter. **Active Trust Management for Autonomous Adaptive Survivable Systems**. Proposal Submitted to DARPA on January, 2000. Massachusetts Institute of Technology: Artificial Intelligence Laboratory and Laboratory for Computer Science. Disponível por WWW em http://www.researchindex.com (30, Ago. 2002).

[SIL 02] SILVA, Ana Cristina Benso da; TAROUCO, Liane; NUNES, Cristina. Using Middleware Concept on Network Management Application. In: 15th INTERNATIONAL CONFERENCE ON COMPUTER COMMUNICATION. **Proceedings...** 15th International Conference on Computer Communication. 2002.

[STA 99] STALLINGS, W. **SNMPv1, SNMPv2, SNMPv3 and RMON I and II -**

Practical Network Management. Third Edition. USA: Addison Wesley, 1999. 619 p.

[STE 00] STERRIT, R.; MARSHALL, A.H.; SHAPCOTT, C. M.; McCLEAN S.I. Exploring Dynamic Bayesian Belief Networks for Intelligent Fault Managemet Systems. In: IEEE INTERNATIONAL CONFERENCE ON SYSTEMS, MAN AND CYBERNETICS. **Proceedings…** IEEE, V. 5, p. 3646-3652, 2000.

[TCP 02] Tcpdump. Disponível em http://www.tcpdump.org

[WAR 99] WARRENDER, Christina; FORREST, Stephanie; PEARLMUTTER, Barak. Detecting Intrusions Using System Calls: Alternative Data Models. In: IEEE SYMPOSIUM ON SECURITY AND PRIVACY. **Proceedings…** IEEE, p. 133 –145, 1999.

[YE 02] YE, Nong; EMRAN, S. M.; CHEN, Q.; VILBERT, S. Multivariate Statistical Analysis of Audit Trails for Host-Based Intrusion Detection. **IEEE Transactions on Computer.** V. 51, n. 07, p. 810-820, Jul. 2002.

[YUE 03] YUEBIN; B. KOBAYASHI, H. Intrusion detection systems: technology and development. In: 17th INTERNATIONAL CONFERENCE ON ADVANCED INFORMATION NETWORKING AND APPLICATIONS. **Proceedings...** IEEE, p. 710 –715, 2003.

[ZHA 00] ZHANG, Yongguang; LEE, Wenke. **Intrusion Detection in Wireless Ad-Hoc Networks**. 2002. In: 6th ANNUAL INTERNATIONAL CONFERENCE ON MOBILE COMPUTING AND NETWORKING. Disponível por WWW em http://www.researchindex.com (30, Ago. 2002).

Anexo - A

Este anexo apresenta os gráfico em escala logarítmica, equivalentes aos gráficos dos usuários utilizados na avaliação das medidas. A alteração da escala possibilita visualizar claramente os valores que o grau de desconhecimento assume realmente , ou seja, valores no intervalo [0,1], pois nos gráfico utilizados anteriormente ele é um valor relativo a escala utilizada simplesmente para que possa ser visualizado.

Gráficos do Primeiro Usuário

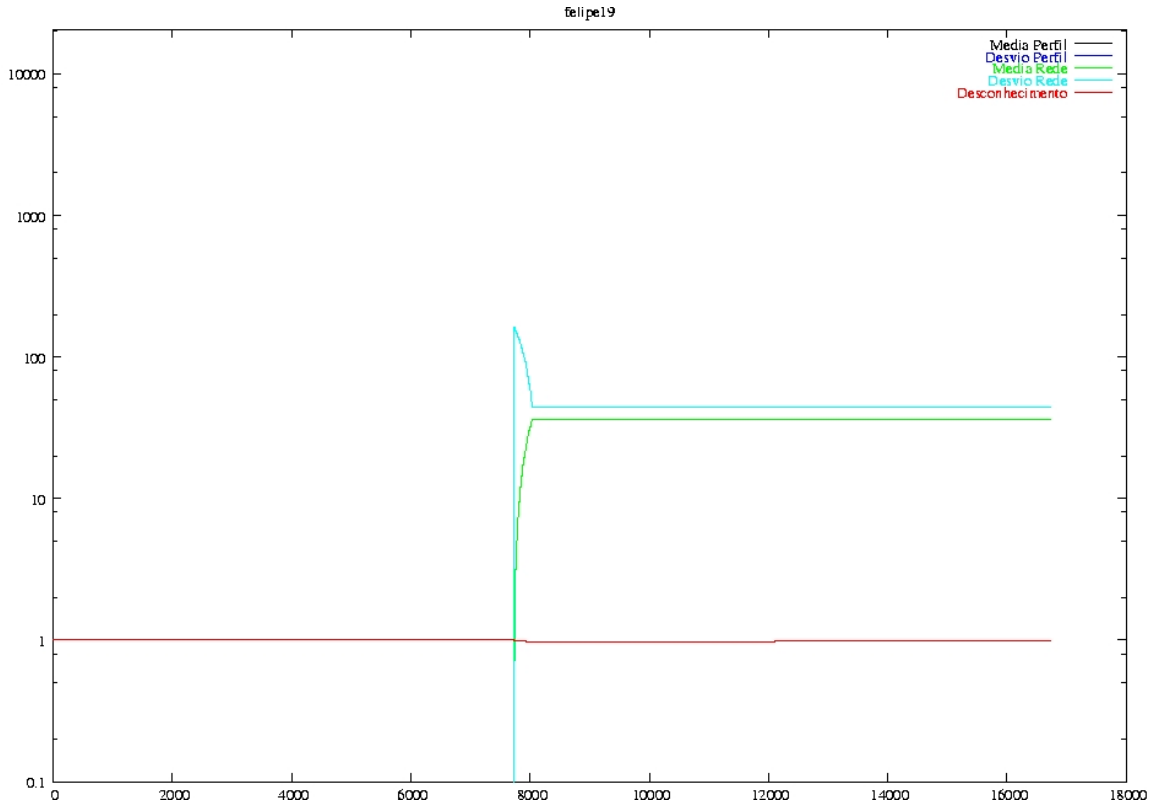


Figura 28 – Resultados da Monitoração no 1º. dia.

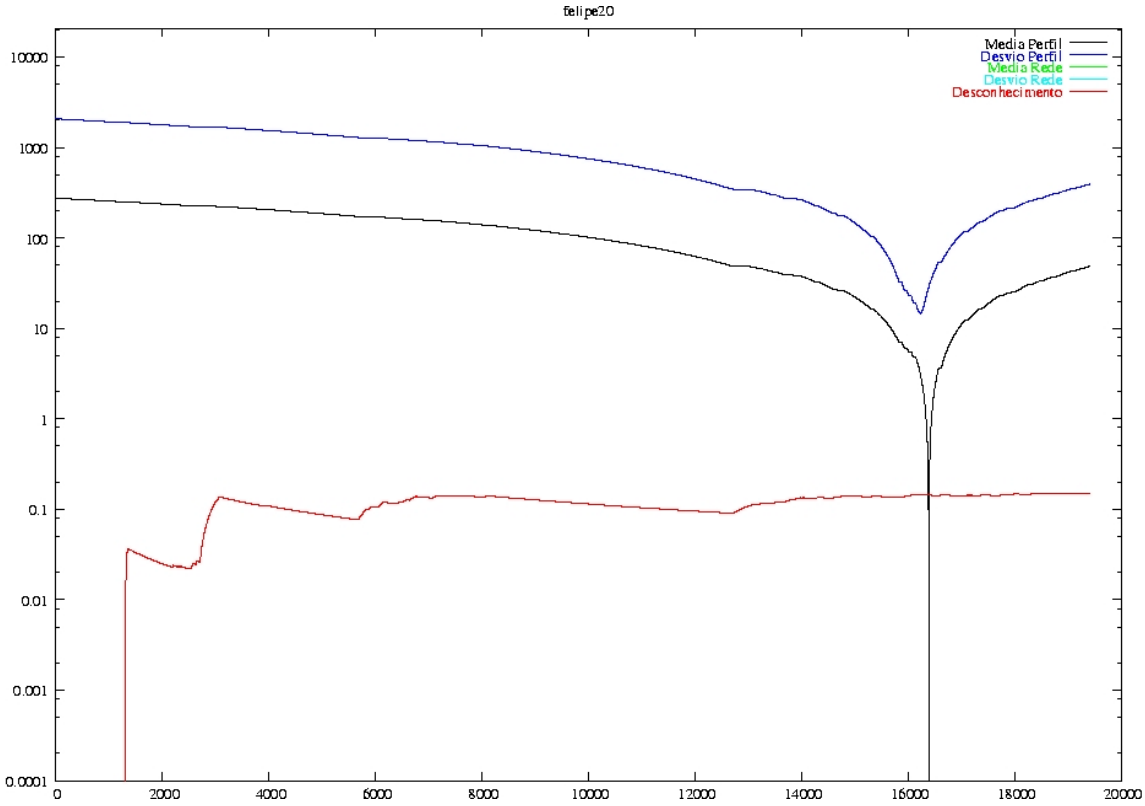


Figura 29 – Resultados da Monitoração no 2º. dia.

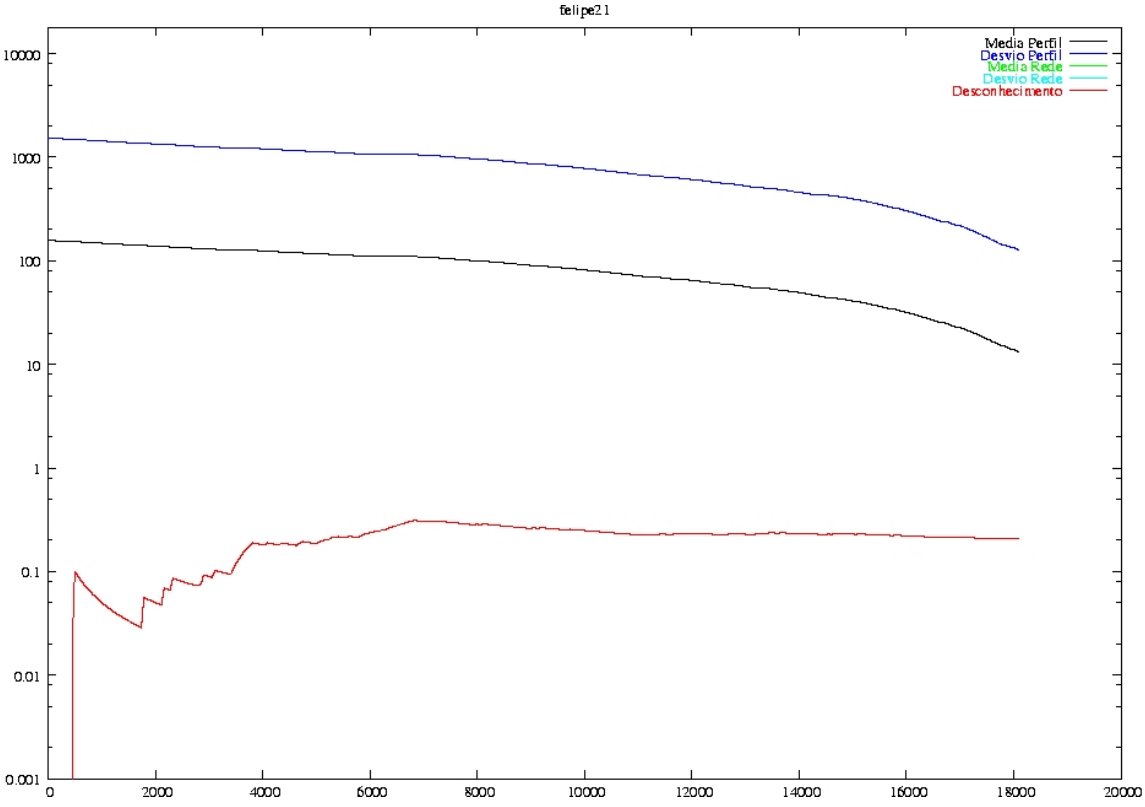


Figura 30 – Resultado da Monitoração do 3º. dia

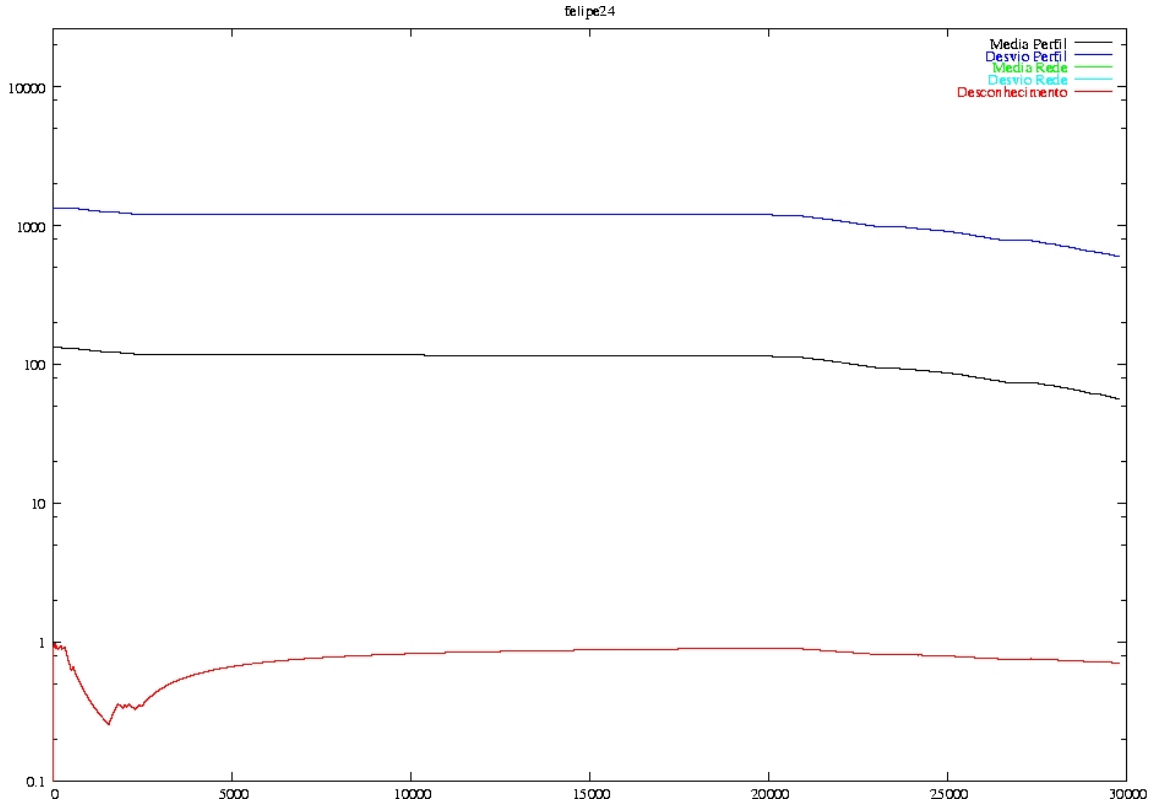


Figura 31 – Resultado da Monitoração do 4º. dia

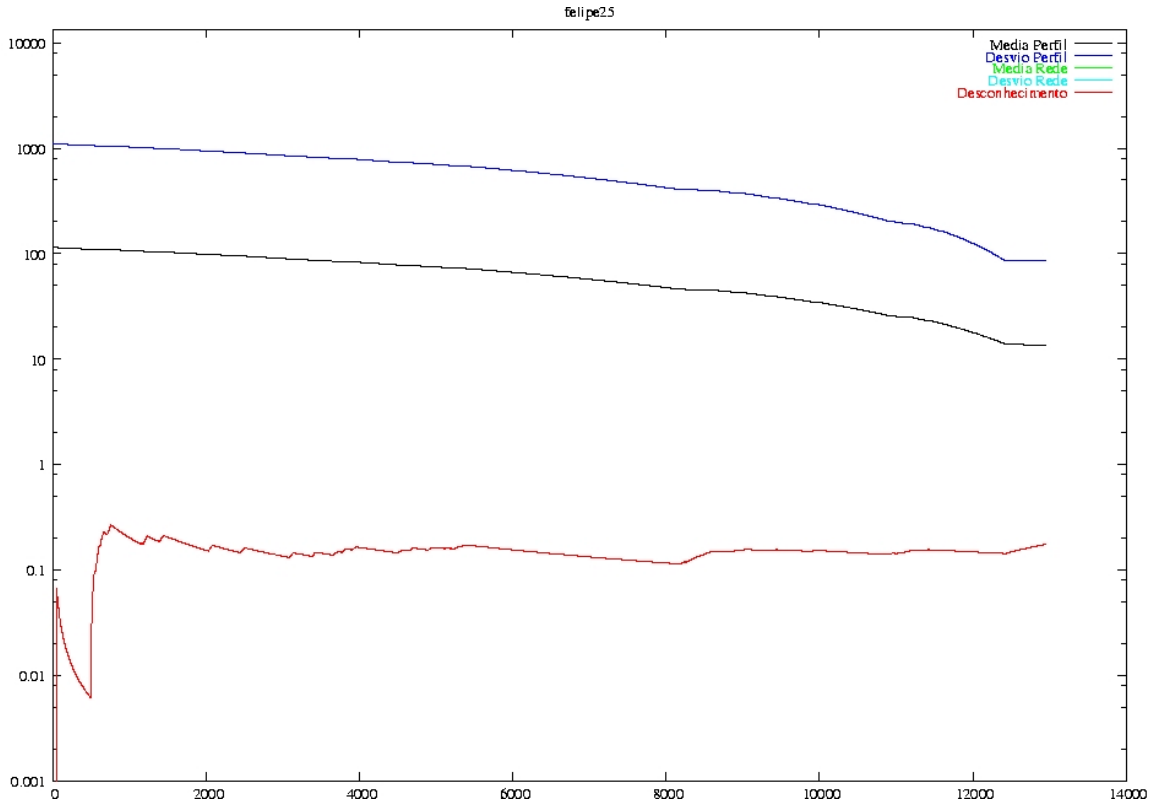


Figura 32 – Resultado da Monitoração do 5º. dia

Gráficos do Segundo Usuário

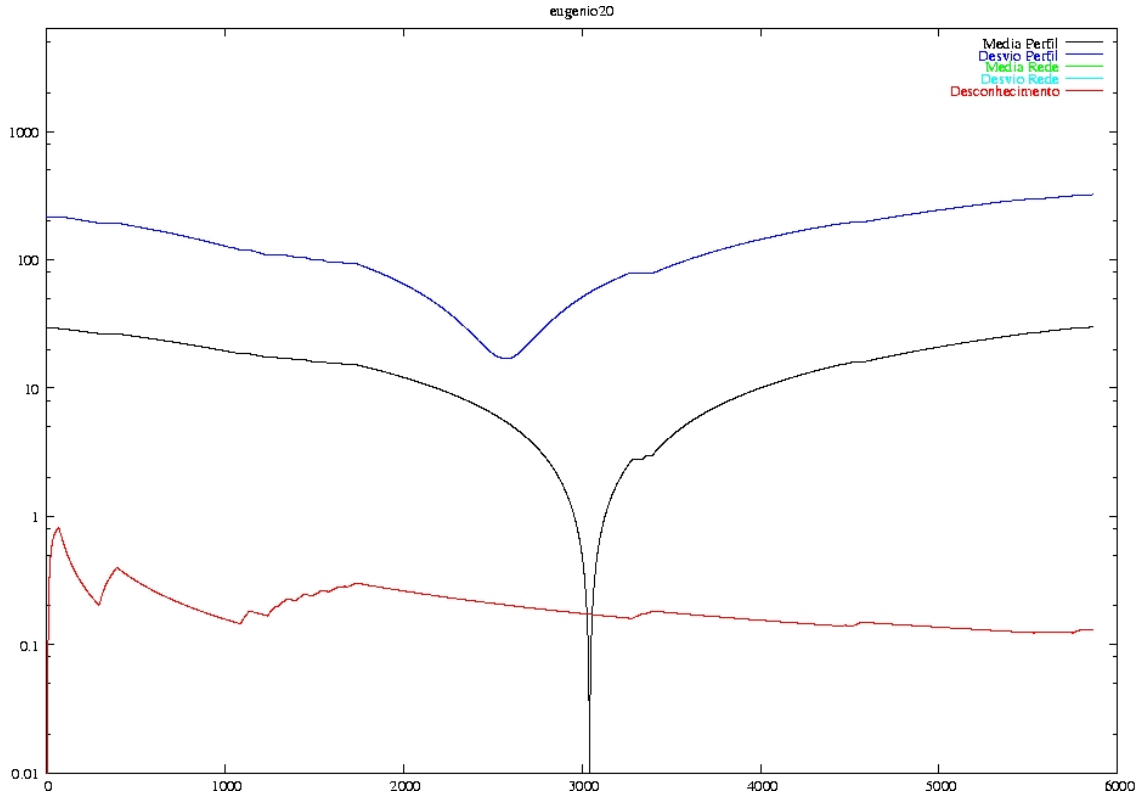


Figura 33 – Resultado da Monitoração do 2º. dia

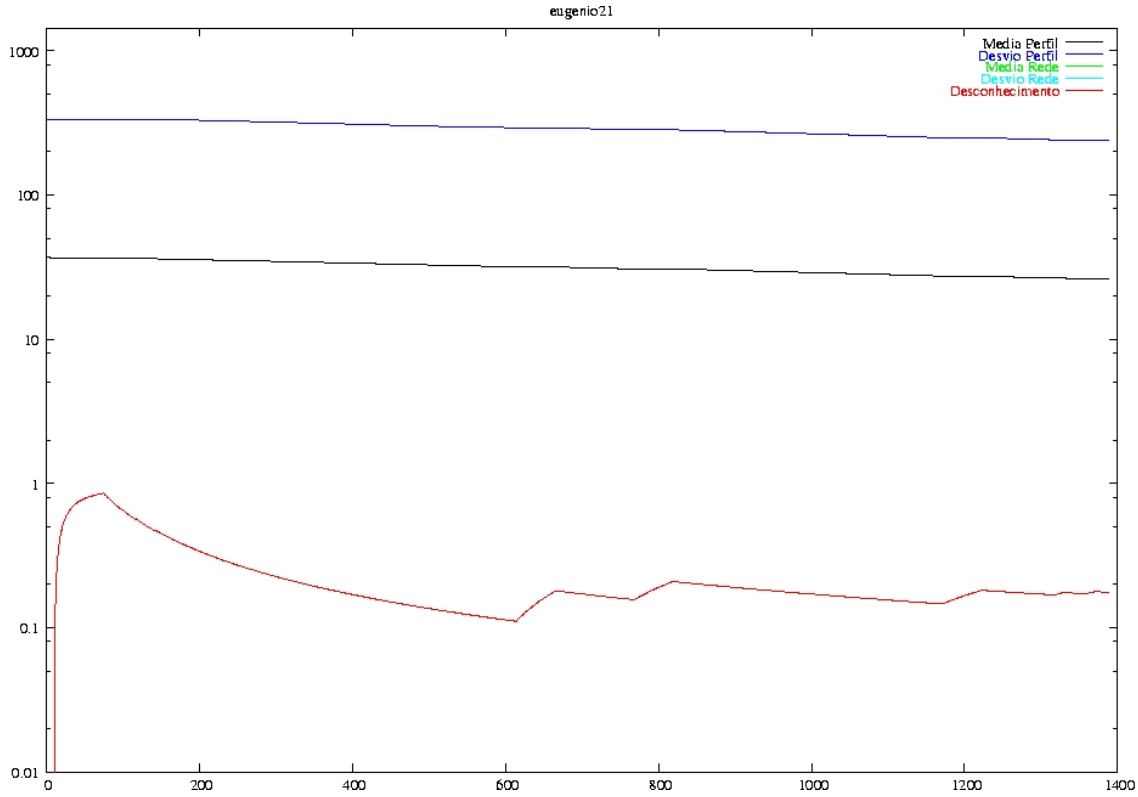


Figura 34 – Resultado da Monitoração do 3º. dia

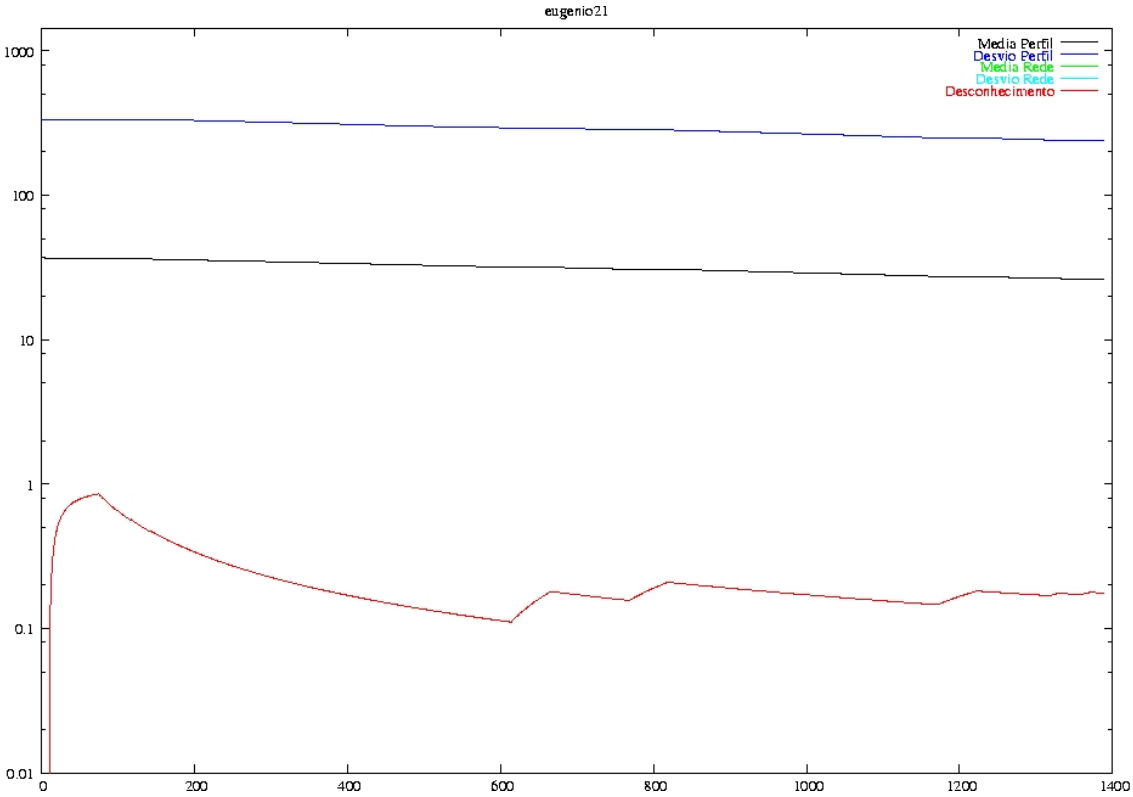


Figura 35 – Resultado da Monitoração do 4º. dia

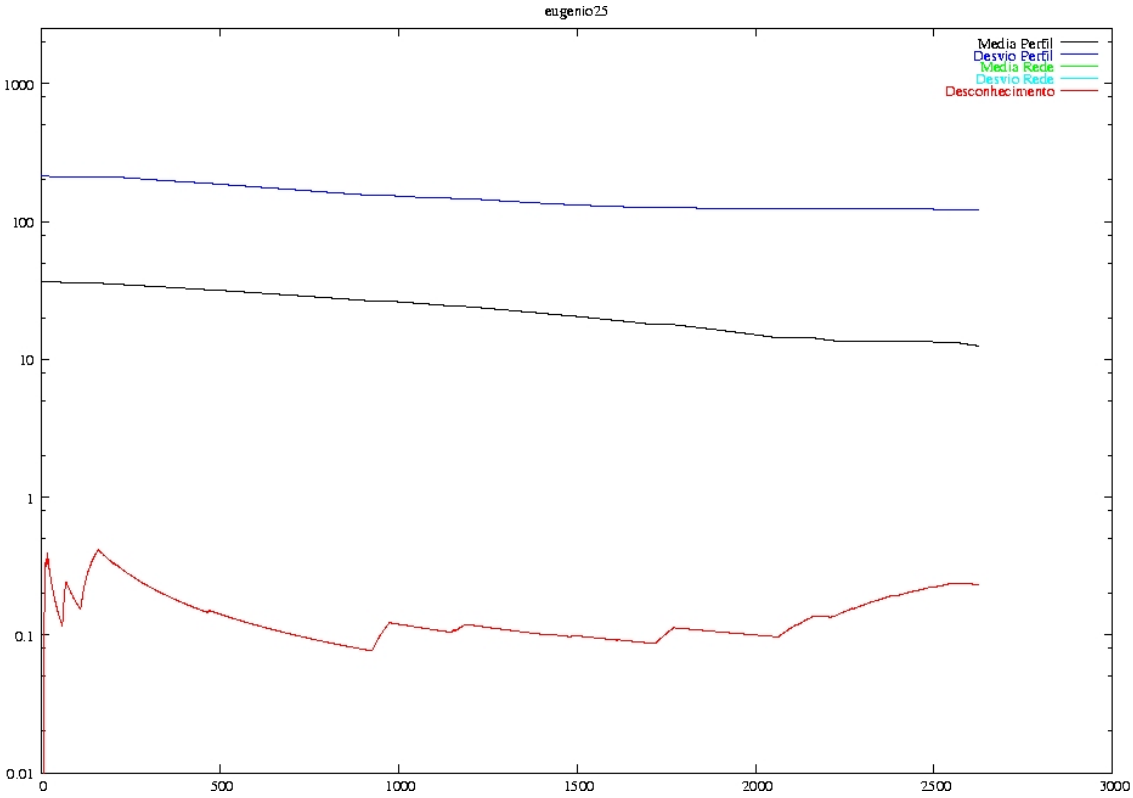


Figura 36 – Resultado da Monitoração do 5º. dia

Gráficos do Terceiro Usuário

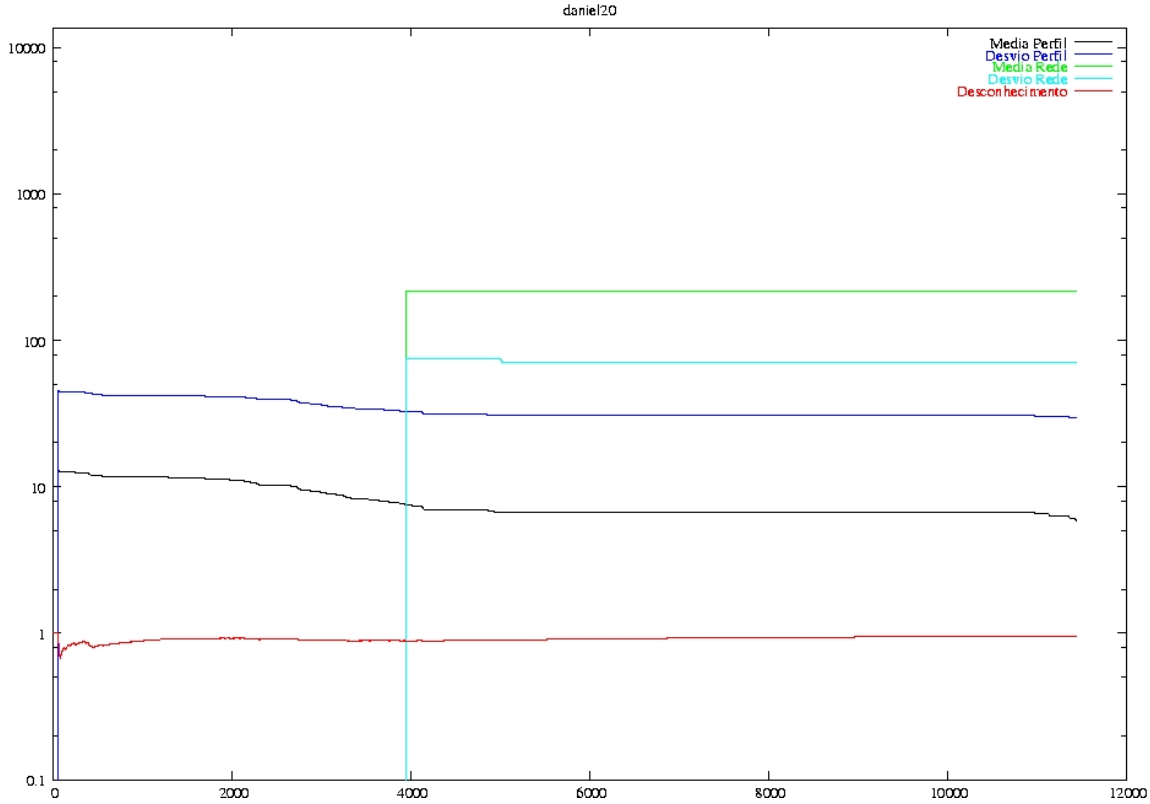


Figura 37 – Resultado da Monitoração do 2º. dia

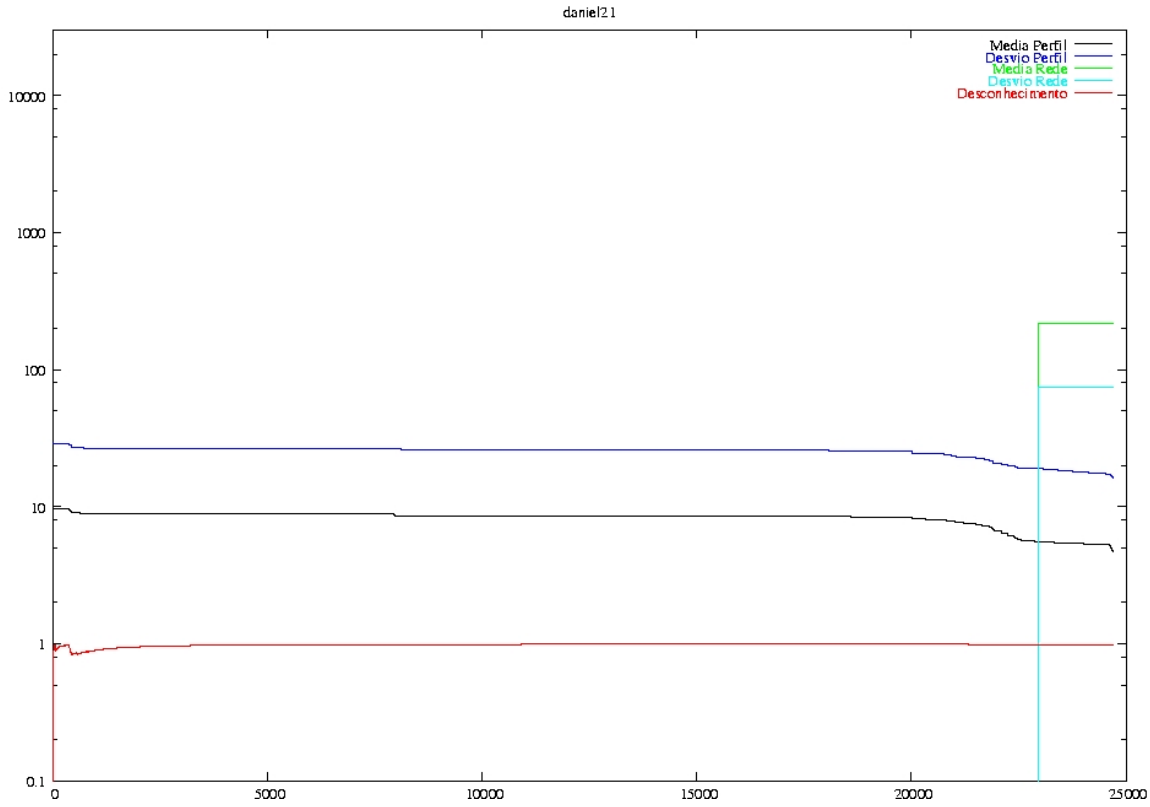


Figura 38 – Resultado da Monitoração do 3º. dia

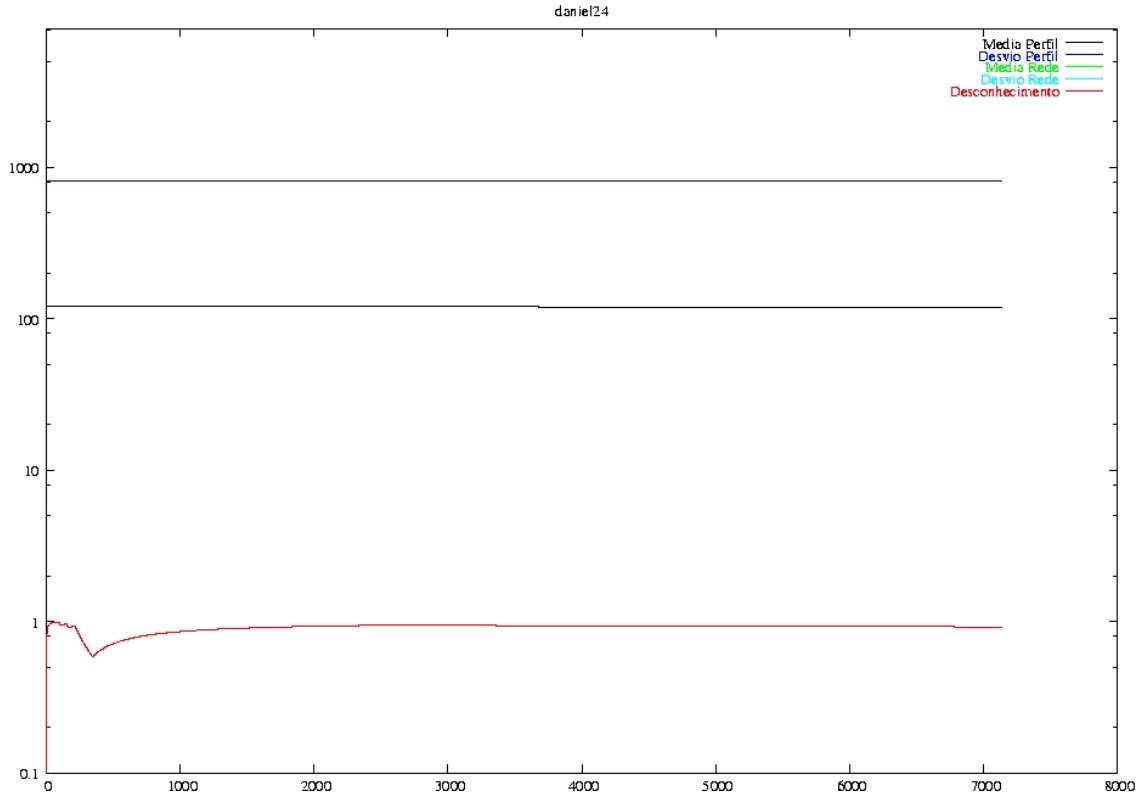


Figura 39 – Resultado da Monitoração do 4º. dia

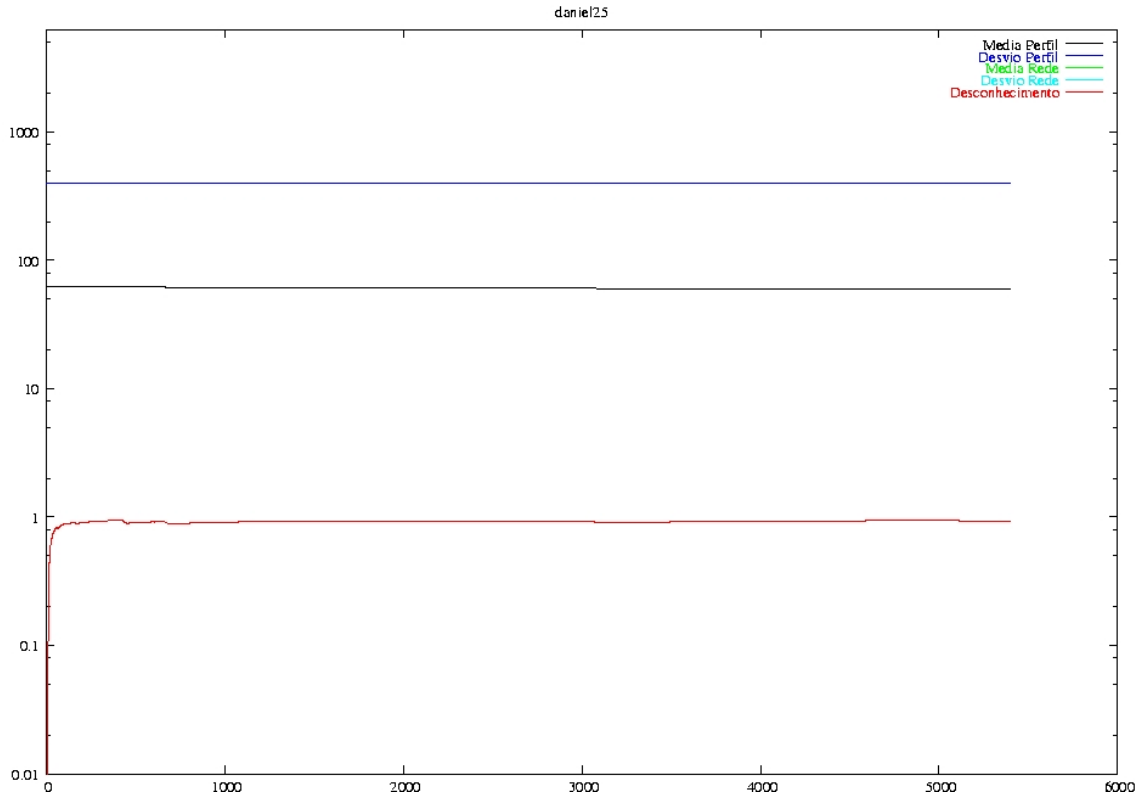


Figura 40 – Resultado da Monitoração do 5º. dia