Detecção de Intrusões em Backbones de Redes de Computadores Através da Análise de Comportamento com SNMP

Guilherme Eliseu Rhoden
rhoden@inf.ufsc.br

Edison Tadeu Lopes Melo
melo@npd.ufsc.br

Carlos Becker Westphall
westphal@lrg.ufsc.br

Laboratório de Redes e Gerência
Curso de Pós-Graduação em Ciência da Computação
Universidade Federal de Santa Catarina

Resumo: *A detecção de intrusões em backbones é um fator importante quando pretende-se fazer o melhor uso de recursos possível, visando principalmente garantir a disponibilidade e a confiabilidade da rede. Este trabalho pretende apresentar um modelo baseado em SNMP para auxiliar na detecção de problemas relacionados a ataques de Denial of Service que envolvem a degradação de desempenho de backbones através da análise de comportamento utilizando variáveis da MIB dos roteadores.*

Palavras-chave: *Detecção de Intrusão, Gerenciamento de Redes de Computadores, SNMP, MIB.*

Abstract: *The intrusion detections in backbones is a very important factor when you intend to assure the best use of resources, the availability and reachability over the network. This report intends to present a SNMP model based to help in detection of problems related to attacks involving the performance degradation in backbones through the analysis of behavior, using routers MIB variables.*

Keywords: *Intrusion Detection, Network Management, SNMP, MIB.*

1 Introdução

Nos dias atuais a preocupação com segurança em sistemas computacionais e, principalmente, em redes de computadores está sendo considerada como um fator primordial para um melhor funcionamento de uma rede. Isto permitirá uma melhor qualidade para seus usuários, possibilitando que a confiança dos usuários perante a rede alcance os patamares de 100% e os transtornos causados por atacantes sejam minimizados com o auxílio de ferramentas de detecção de intrusões e melhorias nos protocolos atuais que interconectam as redes e serviços, garantindo uma melhor confiabilidade e privacidade para seus usuários.

João Cabrera e sua equipe de pesquisadores [1] apresentaram o estudo realizado da detecção prematura de ataques de *Distributed Denial of Service* (DDoS), utilizando sistemas de gerência de redes para analisar as variáveis de tráfego da MIB (*Management Information Base*), onde analisaram 3 scripts de DDoS e fizeram a correlação de eventos de cada ataque gerado pelos scripts e com as variáveis MIB. Com esse estudo, a equipe conseguiu gerar "assinaturas" específicas para cada um dos ataques, somente pela análise destas variáveis, o que possibilitou a sua detecção com um reduzido número de falsos alarmes.

A estrutura deste texto introduz na seção 2 uma visão geral sobre detecção de intrusões e ataques de negação de serviço (DoS e DDoS) que degradam o desempenho de um *backbone*. A seção 3 apresenta o modelo e a ferramenta de análise do comportamento de equipamentos gerenciáveis através do protocolo SNMP (*Simple Network Management Protocol*). Na seção 4 são apresentados os resultados atingidos no desenvolvimento do trabalho. Finalmente, na

seção 5 apresenta-se o encerramento do trabalho com suas conclusões, trabalhos futuros e considerações finais.

2 DETECÇÃO DE INTRUSÕES

A grande parte dos sistemas computacionais possuem algum tipo de vulnerabilidade originado por problemas de implementação, configuração ou projeto, que poderão ser futuramente explorados para os mais diversos fins, como meio de negação de serviço ou até mesmo permitir um acesso não autorizado ao sistema. Com o surgimento destes ataques, foram e continuam sendo desenvolvidos vários métodos/ferramentas a fim de detectar o mau uso a partir de análise do comportamento dos usuários/sistemas, análises de "assinaturas" de ataques dentre outras técnicas.

Os intrusos podem ser caracterizados como mascarados, mal feitores e usuários clandestinos [2] e a detecção destes intrusos pode estar baseada em *hosts*, *multi-host* e redes. As implementações de *Host* e *multi-hosts* assumem que a segurança está voltada no controle dos sistemas computacionais finais verificando os processos, enquanto a detecção de intrusos em redes busca monitorar os pacotes que estão trafegando [3].

A detecção de intrusão é motivada por diversos aspectos, segundo Stallings [2]:

- Se um intruso é detectado rapidamente, ele poderá ser identificado e expulso do sistema sem causar nenhum dano ou nenhum dado ser compromissado;
- Um efetivo sistema de detecção de intrusão pode servir como um impedimento, assim atuando na prevenção de intrusos; e
- Detecção de intrusão facilita a coleta de informações sobre técnicas de intrusão, que podem ser utilizadas para facilitar a prevenção de intrusão.

A detecção de intrusão é baseada na suposição de que o comportamento do intruso difere do usuário legitimo, podendo assim ser diferenciado. Não podemos esperar que o comportamento seja totalmente diferente, ou que exista distinção exata entre um ataque vindo de um intruso e o uso normal de recursos por um usuário autorizado. No entanto, devemos esperar que haja alguma sobreposição conforme apresentado na Figura 1.

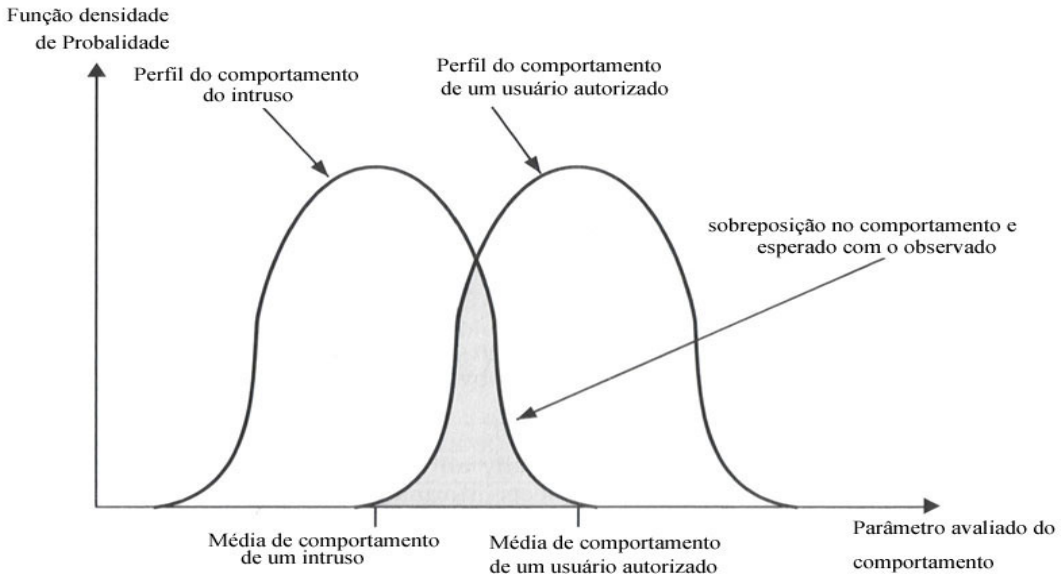

Figura 1 - Perfil do comportamento de Intrusos e Usuários Autorizados [2]

A Figura 1 sugere, em termos muito abstratos, a natureza da tarefa que confronta o sistema de detecção de intrusão. O comportamento dos usuários legítimos e dos intrusos se sobrepõe e neste ponto sua diferenciação é impraticável.

Em redes de computadores são utilizadas, principalmente, ferramentas detecção de intrusão conhecidas como NIDS (*Network Intrusion Detection System*) que analisam o conteúdo dos pacotes que estão trafegando em uma rede, geralmente pacotes IP, sendo uma forma mais segura de se conseguir detectar ataques que trafegam por ela. A detecção destes ataques é baseada em "assinaturas" contidas no cabeçalho e/ou carga útil do pacote IP. Mas para que essas ferramentas de detecção consigam detectar os mais novos tipos ataques e suas variantes, é necessário que suas "assinaturas" estejam sempre atualizadas. Como exemplo de ferramentas, podemos citar SNORT[3], SHADOWN[4], Enterasys Dragon IDS[5], NFR[6] dentre outros.

2.1 Negação de Serviço (DoS)

Os ataques de negação de serviço, mais popularmente conhecidos por DoS (*Denial of Service*), são utilizados em grande escala como uma tentativa para desabilitar ou corromper redes, sistemas ou serviços fazendo com que os usuários legítimos não consigam obter o acesso a estes recursos. Os intrusos que utilizam essa forma de ataque podem ser comparados a vândalos. O principal problema está no protocolo IP, mais especificamente na sua versão 4, que é altamente vulnerável a ataques DoS, além disso muitas ferramentas de ataques estão disponíveis para o acesso público e possuem seu uso relativamente fácil. Estes tipos de ataques podem ser lançados contra *perimeter routers*, ou *bastion hosts*, ou *firewalls*, conforme o ilustrado na Figura 2.

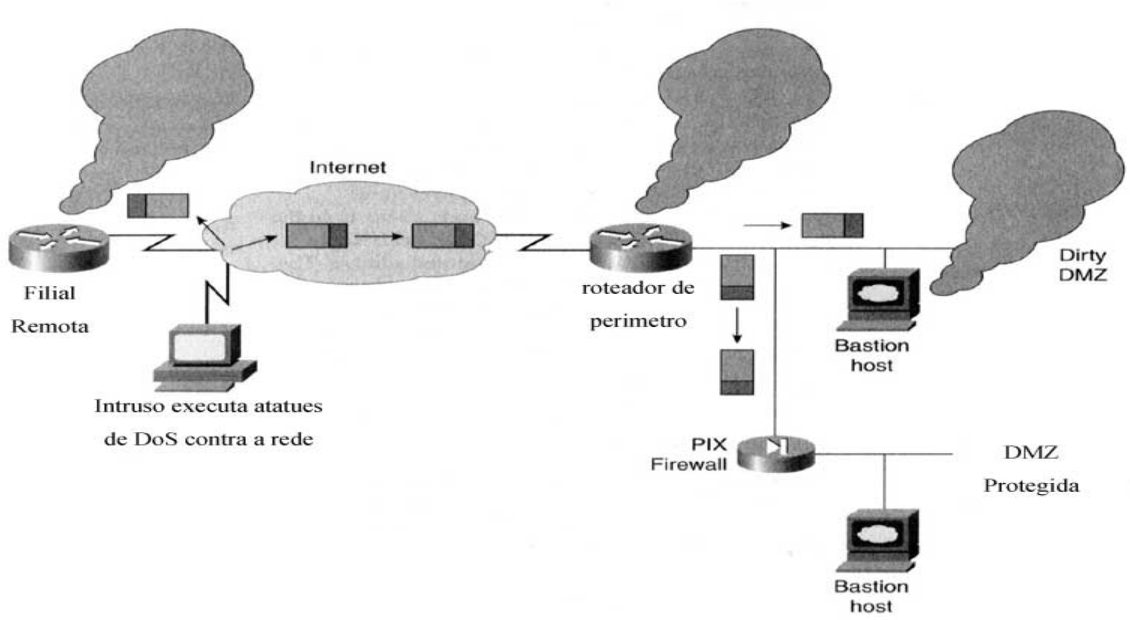

Figura 2 - Ataques de Negação de Serviço

Estes ataques acabam causando diversos problemas para uma rede ou serviços, onde o intruso tenta sobrecarregar os recursos alvos, incluindo a largura de banda de uma interface, o uso interno de memória, capacidade de processamento ou espaço em disco.

Este trabalho faz a análise das variáveis da MIB críticas dos equipamentos de roteamento, principalmente o uso da CPU, traçando o perfil (*baseline*) de comportamento de algumas

variáveis do equipamento automaticamente, para que desvios de comportamento possam ser detectados e os administradores do *backbone* serem alertados.

3 Ferramenta de Análise de Comportamento Através da Análise das Variáveis da MIB.

O presente trabalho tem por objetivo principal apresentar um método alternativo que sirva para diagnosticar o estado de um equipamento de interconexão de rede gerenciável via SNMP, auxiliando a gerência de segurança e a detecção de intrusões em redes de computadores.

Com o uso deste método, foi desenvolvida uma ferramenta que analisa o comportamento de diversos equipamentos gerenciáveis através de sua MIB, tendo como base à observação da alteração do comportamento característico de cada equipamento.

Espera-se que a rede e o equipamento estejam operando em suas condições normais, para garantir que o comportamento que será adquirido inicialmente seja o mais próximo possível da realidade.

A justificativa para a criação desta ferramenta é devido ao fato de que os ataques às redes de computadores e seus equipamentos de interconexão tais como *switches*, roteadores, servidores e outros, estão crescendo constantemente e existem poucas medidas de contra-resposta automática perante a este problema. Suas principais dificuldades são detectar alguma anomalia na rede antes que o usuário final reclame, detectar quando está sendo atacado ou servindo de ponte para um ataque a uma outra rede, principalmente em uma rede de grande porte, como nos *backbones* de grandes instituições.

A ferramenta possui o gerador/analisador de eventos que foi escrito com a linguagem JAVA, onde sua função é coletar as variáveis dos equipamentos gerenciáveis, analisar se elas estão de acordo com o comportamento adequado para o respectivo equipamento e caso fuja dos padrões adquiridos, eventos são gerados como envio de e-mail para os responsáveis pelo equipamento, inclusão do evento na base de dados e envio de SNMP TRAPs para uma estação de gerência externa ao sistema. A gerência do sistema como um todo é apresentada através de uma interface web amigável com auxílio de PHP e MySQL e dispondo de recursos gráficos gerados em tempo de carregamento da página web.

3.1 Modelo Lógico da Ferramenta Desenvolvida

O modelo aqui proposto pela ferramenta visa monitorar um determinado número de roteadores, onde informações como percentual de uso da CPU, *buffers* de filas, vazão de pacotes em uma determinada interface, através do protocolo de gerência SNMP. Estas variáveis são coletadas pelo agente e guardadas em uma base de dados para futuras análises, que serão realizadas pela ferramenta e/ou pelo administrador, para que se possa modelar o comportamento de cada roteador, observe a Figura 3.

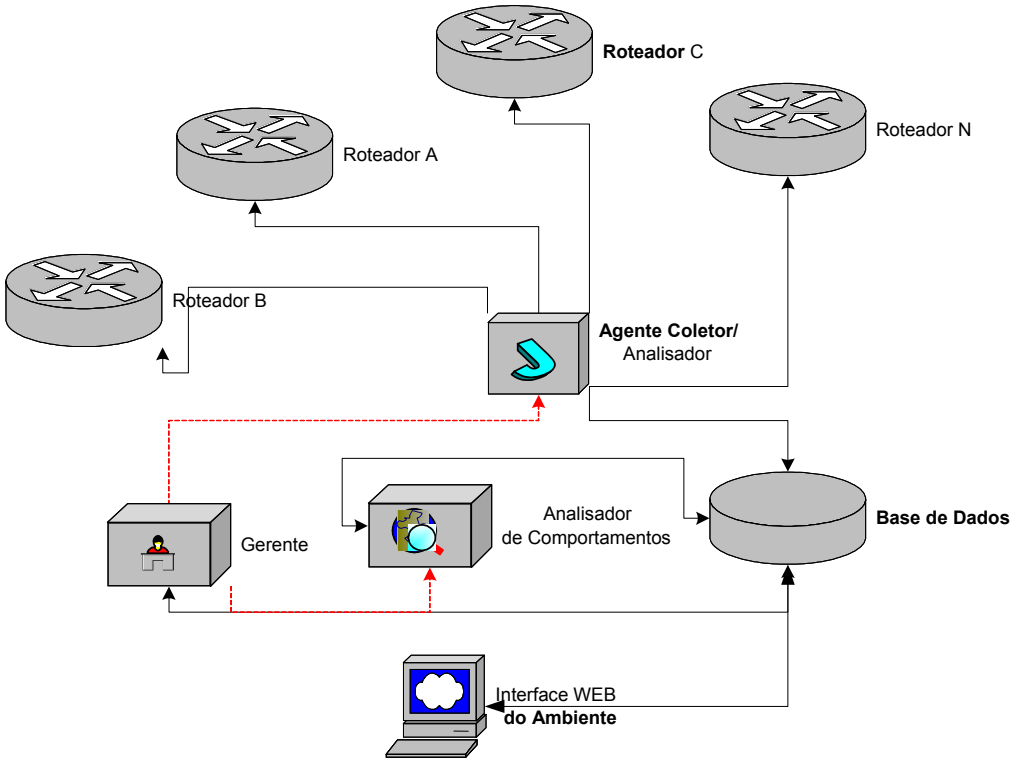

Figura 3 - Modelo Lógico da Ferramenta

O analisador de comportamentos tem o papel de consultar a base de dados gerada pelo(s) agente(s) e a partir destas informações conseguir modelar o comportamento de um roteador específico para aquele período de tempo e comparando-o com os eventos anteriores de mesma ordem, isto é, nos dias anteriores no mesmo intervalo de tempo. Na grande maioria dos casos o uso da CPU comporta-se de maneira semelhante aos períodos de mesma ordem anteriores, onde será estipulado um percentual de tolerância para a geração de eventos quando o comportamento sair dos padrões analisados. Essa faixa de tolerância é tida pelo desvio padrão que é calculada automaticamente pela ferramenta e por um percentual de erro regulável pelo administrador do sistema.

O papel do gerente como seu próprio nome indica é ser o elemento principal que comandará as ações a serem executadas pelos outros elementos que compõe o modelo em menor ordem, isto é, configurar os agentes coletores e o analista, alertar o administrador se algum componente do modelo está com mau funcionamento dentre outras funcionalidades.

3.2 Geração e Visualização de Eventos

Realizando a análise estatística do comportamento é possível prever como uma pequena margem de erro qual é o padrão de comportamento esperado. Esta margem de erro varia dependentemente de quais elementos da MIB estão sendo analisados e partindo do princípio que o equipamento encontra-se operando em condições normais, ou seja, não esteja sofrendo nenhum ataque de DDoS ou algo semelhante. Observe o comportamento analisado de um equipamento e os valores seus valores atuais gerados pela ferramenta na Figura 4.

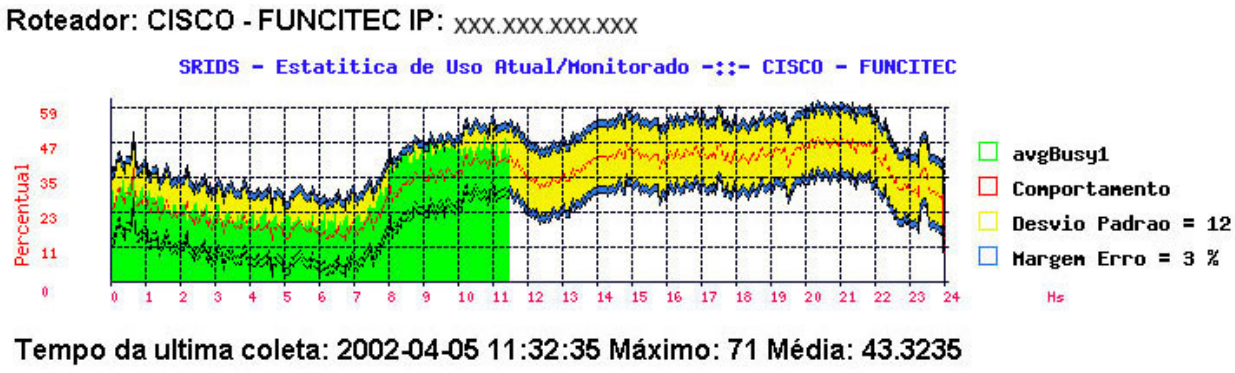

Figura 4 - Comportamento Atual, Adquirido, desvio padrão e margem de erro

Analisando o gráfico anterior retirado às 11:32hs, notamos que os valores da CPU de um roteador CISCO estão de acordo com suas condições até o presente momento. Continuando análise na linha do comportamento, que fica entre a faixa do desvio padrão e da margem de erro, espera-se que ao decorrer do dia a CPU do equipamento mantenha-se próxima da linha do comportamento. É considerado um comportamento normal quando a CPU possa chegar até os patamares do desvio padrão, podendo atingir até a margem de erro estipulada pelo administrador. Caso ocorra algum desvio superior ou inferior ao comportamento analisado, com uma margem de erro configurável, alertas serão gerados.

A visualização de eventos é apresentada de três maneiras, a primeira de forma gráfica como é mostrada na figura 3, em forma de alertas no console da ferramenta e também é possível acompanhar os alarmes na forma de tabelas para verificar o histórico de eventos que ocorreram com os equipamentos.

O uso desta ferramenta é de grande valia para controlar o estado de um equipamento, pois se simplesmente monitorarmos suas variáveis não conseguiríamos obter mais do que gráficos e o problema só seria constatado quando alguém que sempre os analisa em muitos casos poderia contatar essas alterações. Com ele alertas são enviados e o responsável verificaria se tudo está correto.

Na literatura da Cisco Systems [7], é apresentado um guia para monitoramento e correlação de eventos para seus equipamentos gerenciáveis (*switches* e routeadores), o que contribui para um melhor conhecimento dos equipamentos, permitindo assim o estudo novas variáveis com o intuito de traçar automaticamente o comportamento das mesmas.

3.3 Resultados Alcançados

Os seguintes resultados foram obtidos durante o desenvolvimento e testes do modelo:

- Monitoramento dos equipamentos de interconexão onde buscou-se estabelecer um modelo de comportamento para cada equipamento, integrando as peculiaridades de cada equipamento, através do protocolo de gerência de redes SNMP, linguagens Java e PHP, e a base de dados MySQL.
- Notificação de alterações do comportamento em forma de TRAPs SNMP, e-mail, alertas no console e na base de dados.
- Proporcionou mais uma maneira para auxiliar o trabalho dos analistas de seguranças e até mesmo dos gerentes de redes, onde através de uma interface WEB amigável podem visualizar os eventos com maior clareza e interação.
- É possível através de uma única estação gerenciar inúmeros equipamentos ao mesmo tempo, podendo estar dispostos em redes ou locais onde o uso de ferramentas de

detecção de intrusão em redes de computadores não se torna viável atualmente devido a custos extras ou em *links* com largura de banda superior a 100 Mbps [2], [8].

- Para melhorar os resultados, é interessante integrar essa ferramenta com um NIDS, para prover uma rápida solução a um ataque que tenha como objetivo o *Denial of Service*.
- O uso do RMON [9] faz um papel semelhante com o envio de TRAPs SNMP, mas é necessário especificar qual será o valor limite para que o evento ocorra. O objetivo dessa ferramenta é analisar o comportamento e medir se algo está errado com o equipamento de acordo como histórico armazenando. Quanto mais tempo for analisado, o comportamento tende a ser o mais próximo possível da realidade, levando em consideração que ele esteja inicialmente trabalhando em suas características normais.

4 CONCLUSÕES E TRABALHOS FUTUROS

A área de detecção de intrusões, especialmente em rede de computadores, possui um campo bastante amplo e onde existem inúmeras alternativas, sendo elas comerciais ou de código aberto para facilitar a identificação de ataques/ ameaças a redes de computadores.

Este trabalho visa aumentar a visão do administrador de *backbones* o qual, ainda não é possível detectar/barrar todos os ataques que passam através dele que, principalmente, degradam o desempenho da rede como um todo.

A ferramenta proposta pode ser empregada como uma nova alternativa para o gerenciamento de redes e no auxílio na detecção de intrusão em grandes *backbones* ou redes WAN. Todos os equipamentos gerenciáveis através de SNMP possuem em sua MIB proprietária ou nas MIBs padrões, variáveis que podem ser analisadas para esse fim. Neste estudo utilizaram-se roteadores IBM das séries (2210, 8210, 8371) e CISCO das séries (2500, 7000 e 7500) que estão presentes no ambiente da rede UFSC, PoP-SC e RCT e as coletas dos valores correspondem ao uso de CPU, onde notou-se uma grande modificação do seu comportamento quando ataques de DoS eram lançados contra eles. Tal alteração também foi observada nos equipamentos serviam como rota para outras redes quando os ataques ocorreram. Outras variáveis que apresentaram e possibilitaram bons resultados na criação da *baseline* e estão padronizadas na MIB-II, são o número de pacotes *unicast* que entram e saem por uma interface (*ifInUcastPkts* e *ifOutUcastPkts*).

Através do estudo realizado notou-se que área de gerenciamento de segurança é uma área bastante promissora juntamente com a detecção de intrusão, pois mostrou-se efetiva na coleta dos dados necessários, e no envio de alertas. Por outro lado, quando o protocolo IPv6 chegar a ser utilizado em larga escala e a carga útil dos pacotes for cifrada, grande parte dos problemas de rede e segurança estarão resolvidos, principalmente o caso do *sniffing*. Essa técnica será menos utilizada, pois quando a criptografia estiver no nível de protocolo, esse problema de escuta será menos vulnerável, e quando algo for capturado somente os criptoanalistas conseguirão decifrar qual é o conteúdo dos pacotes, através de força bruta ou criptoanálise, o que não é uma tarefa trivial.

Por outro lado, a maioria dos IDSs de rede acabarão não conseguindo mais detectar muitas "assinaturas" de ataques quando a criptografia passar a ser empregada pelo novo protocolo. Com isso abrirá um novo espaço a ferramentas e métodos de análise de comportamento baseado em informações estatísticas dos equipamentos gerenciáveis que compõe a infraestrutura das redes de computadores.

Este trabalho baseou-se na utilização do protocolo SNMPv1 devido a fatores de interoperabilidade com os equipamentos que foram testados. Os problemas de segurança apresentados por essa versão do protocolo ficarão minimizados com a adoção do SNMPv3.

Este modelo de análise do comportamento, como os outros métodos de detecção de intrusão não resolvem o problema, mas contribuem para manter o *backbone* sempre monitorado e qualquer desvio de comportamento que afete o desempenho da rede possa ser detectado a tempo, sua causa encontrada e interrompida.

5 REFERÊNCIAS BIBLIOGRÁFICAS

[1] Cabrera, João. et al. *Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic Variables – A Feasibility Study.* In *Proceeding of The Seventh IFIP/IEEE International Symposium on Integrated Network Management (IM 2001),* Seattle, WA, May 2001.

[2] W. Stallings. *Cryptography and Network Security: Principles and Practice. 2º ed*, 1998.

[3] SNORT. *The Open Source Network Intrusion Detection System*, URL: http://www.snort.org (jun. 2001).

[4] SHADOW. *Shadow IDS*. URL: http://www.nswc.navy.mil/ISSEC/CID/index.html (abril de 2002)

[5] Dragon. *Enterasys Network Dragon 4*. URL: http://www.enterasys.com/ids/. (abril de 2002).

[6] NFR. *NFR Network Intrusion Detection*. URL: http://www.nfr.com/products/NID/ .(abril de 2002).

[7] CISCO, Cisco *Network Monitoring and Event Correlation Guidelines*. Cisco Systems, Inc.1999.

[8] Campello, R; Weber, R. *Sistemas de Detecção de Intrusão.Minicurso procedente do 19º Simpósio Brasileiro de Redes de Computadores* (SBRC). Florianópolis, maio de 2001.

[9] RFC2819. *Remote Network Monitoring Management Information Base. Network Working Group, Request for Comments: 2819. S. Waldbusser of Lucent Technologies*, May 2000.