Detecção de Anomalias em Redes de Computadores através de Transformadas Wavelet

Tiago Perlin [1]
Raul Ceretta Nunes [1]
Alice de Jesus Kozakevicius [1]

Resumo: Ataques em redes de computadores comprometem a segurança do sistema e degradam o desempenho da rede, causando prejuízos aos usuários e às organizações. Sistemas Detectores de Intrusões de Rede são usados para a detecção de ataques ou outras atividades maliciosas por meio da análise do tráfego. A detecção de anomalias é uma abordagem de análise usada na detecção de intrusões, na qual se assume que a presença de anomalias no tráfego, desvios em relação a um comportamento padrão, seja indicativo de um ataque ou defeito. Uma das principais dificuldades dos Sistemas de Detecção de Intrusão de Rede baseados em anomalias está na construção do perfil devido à complexidade do tráfego de rede. Métodos derivados da Análise de Sinais, dentre os quais a transformada wavelet, têm recentemente demonstrado aplicabilidade na detecção de anomalias de rede. Esse artigo apresenta os conceitos fundamentais de detecção de intrusão, bem como conceitos recentes relacionados à detecção por anomalias através de transformadas wavelet, uma técnica com capacidade de análise em multirresolução e baixa complexidade computacional.

Palavras-chave: Detecção de intrusões. Anomalias. Ataques. Wavelet. Segurança da informação.

Abstract: *Attacks on computer networks compromise the security of the system and degrade the performance of the network causing problems to users and organizations. Network-based Intrusion Detection Systems are used to detect attacks or malicious activity by analyzing the network traffic. The anomaly-based detection approach is used for intrusion detection. It is assumed that the presence of traffic anomalies, deviations from standard behavior, is indicative of an attack or malfunction. A major difficulty of an anomaly-based Intrusion Detection System is the construction of the profile due to the complexity of network traffic. Methods derived from Signal Analysis, among which, the Wavelet Transform, have recently demonstrated applicability in detecting anomalies in network. This paper presents the basic concepts of intrusion detection and recent concepts related to intrusion detection by wavelet transforms, a multiresolution analysis technique with low computational complexity.*

Keywords: *Intrusion Detection System. Anomaly Detection. Wavelet. Attacks. Security.*

1 Introdução

A expansão da internet aumentou a exposição das redes de computadores às ameaças, como ataques aos sistemas computacionais e à infraestrutura, o acesso indevido às informações dos usuários e abusos de privilégios. Nesse cenário de interconexão global de dispositivos computacionais, medidas preventivas e ferramentas de detecção são essenciais para garantir a segurança de todo o ambiente computacional pessoal e empresarial.

Medidas preventivas devem ser incluídas prioritariamente em qualquer plano para garantir a segurança de um sistema. Essas medidas são constituídas, principalmente, por [20]: controles de acessos físico e lógico, ferramentas de software como firewalls, dispositivos de hardware e configurações. Concomitantemente ao desenvolvimento e implementação de medidas preventivas, os atacantes têm explorado vulnerabilidades (principalmente

[1]Programa de Pós-Graduação em Informática, UFSM, Camobi - 1000 - Santa Maria (RS) - Brasil
{{perlin81,alice.kozakevicius}@gmail.com},{ceretta@inf.ufsm.br}

doi: 10.5335/rbca.2011.002

de software, mas também de hardware e protocolos) e brechas na configuração de sistemas para obter acesso e efetivar os ataques. Assim, as medidas preventivas, apesar de essenciais, possuem limitações e muitas vezes são contornáveis pelos atacantes.

Sistemas de Detecção de Intrusão (SDI) [31] são ferramentas que visam melhorar a segurança em um sistema computacional. Detecção de Intrusão são as técnicas utilizadas para detectar ataques ou perturbações a um sistema computacional ou rede de computadores [20]. O SDI usa as informações coletadas do sistema monitorado (computador, rede ou segmento de rede) para detectar intrusões. Enquanto as medidas de prevenção ativamente buscam evitar que ataques aconteçam, os sistemas de detecção procuram identificar ataques pela análise passiva do tráfego da rede ou os logs do sistema. Após a detecção de um ataque, um SDI deve gerar uma resposta, que pode ser uma intervenção automatizada no sistema ou um alerta para intervenção humana.

Especificamente para redes de computadores, têm-se os Sistemas de Detecção de Intrusão de Rede (SDIR) [31], que utilizam informações coletadas em uma rede ou segmento de rede para identificar ataques que estejam ocorrendo ou que já tenham ocorrido. Para a análise dos dados coletados da rede, os SDIR usam principalmente [20] a abordagem baseada em assinaturas [39] e a abordagem baseada em anomalias [21], ambas apresentando suas peculiaridades e limitações. A abordagem baseada em assinaturas [20] requer um conhecimento prévio a respeito da forma como cada ataque a uma rede ocorre, ou seja, sua assinatura. Por isso, os SDIR baseados em assinaturas são menos eficientes na identificação de ataques que usam técnicas ainda desconhecidas. Já a abordagem baseada na detecção de anomalias [21], que procura detectar alterações no padrão do tráfego em relação ao perfil da rede, pode gerar um excesso de falsos positivos, inviabilizando a intervenção automatizada ou acarretando a geração de muitos falsos alertas, dificultando a intervenção humana. A pesquisa na área de detecção de intrusões de rede, entre outras, busca tratar desses problemas.

A detecção de anomalias de rede é uma área de pesquisa bastante ativa, com alguns trabalhos recentes [12] [3]. Na pesquisa e desenvolvimento de um SDIR baseado em anomalia um dos pontos essenciais é a construção de um perfil da rede. A construção do perfil da rede depende do método de análise usado e implica o conhecimento das características específicas do tráfego de rede. Nesse sentido, há diversos métodos de detecção de anomalias no tráfego de rede, como métodos baseados em análise estatística [36] e estatística bayesiana [25]; métodos de mineração de dados, como algoritmos de agrupamento [23] e lógica *fuzzy* [49]; métodos de inteligência artificial, como sistemas imunológicos artificiais [16] e algoritmos genéticos [38]; e métodos baseados na análise de sinais [2] [45]. No contexto dos métodos baseados na análise de sinais, a transformada wavelet [30] mostra-se adequada para a modelagem do tráfego de rede em vários trabalhos [2] [42] [17] [14] [27] [19].

O objetivo deste artigo é apresentar uma visão geral sobre o funcionamento e as principais abordagens usadas em sistemas detectores de intrusão em redes de computadores. Faz-se uma descrição de várias técnicas de detecção usadas na abordagem baseada em anomalias. A partir desse levantamento de várias técnicas de detecção de anomalias, é feita uma discussão sobre alguns mecanismos que empregam a transformada wavelet. Busca-se oferecer neste artigo uma ideia mais abrangente sobre a detecção de intrusões em redes de computadores, juntamente com alguns exemplos mais específicos e promissores que fazem uso de wavelets.

O restante deste artigo está organizado da seguinte maneira: na seção 2 são vistas as características e a classificação dos sistemas detectores de intrusão; na seção 3 são apresentadas as principais técnicas usadas no desenvolvimento de sistemas detectores de anomalias de rede; na seção 4 é apresentado o conceito das wavelets e como são usadas por alguns detectores de anomalias; e, por fim, na seção 5 são feitas as considerações finais e discutidos os principais desafios no desenvolvimento de sistemas detectores de anomalias de rede.

2 Sistemas Detectores de Intrusão

Detecção de Intrusão são técnicas usadas para detecção de ataques e intrusões a um computador ou rede de computadores. Uma Intrusão é qualquer tentativa ilegal e deliberada, bem sucedida ou não, de manipulação, quebra ou perturbação do funcionamento de um sistema [20]. A partir do trabalho inicial de [11], que propôs um Sistema de Detecção de Intrusão (SDI), vários outros sistemas foram criados [41] [5] [28] e diversos métodos de detecção foram desenvolvidos [2] [45] [17] [14] [27] [19]. Nos diversos métodos, o processo de detecção de ataques, realizado por um SDI, normalmente compreende três atividades fundamentais [31]: Coleta, Análise e Resposta.

A Coleta corresponde à obtenção dos dados do sistema monitorado. A Coleta de informações pode ser feita diretamente ou por meio de uma ferramenta de software ou hardware chamado Coletor. A Fonte de Informação costuma ser um computador, uma rede ou um segmento de rede. A Análise consiste no processamento dos dados coletados, procurando identificar a ocorrência de uma Intrusão. Há diferentes métodos de análise que seguem cada abordagem usada, baseada em assinaturas [39] ou baseada em anomalias [21], que são vistos nas seções 2.2.1 e 2.2.2. Dentre os métodos de análise baseados em anomalias têm-se os que fazem uso da transformada wavelet, que são vistos na seção 4.2. A Resposta é o conjunto de ações que o SDI realiza quando detecta uma intrusão. Como ação típica tem-se a geração de Alarmes e relatórios, mas o SDI também pode ser programado para fazer uma intervenção automatizada no sistema em caso de Intrusão. A seguir é apresentada a classificação dos detectores quanto à fonte de informações (Seção 2.1) e quanto à abordagem de análise (Seção 2.2).

2.1 Classificação dos Sistemas Detectores de Intrusão quanto à fonte de informações

O SDI pode ser classificado, conforme a fonte de informações, em duas categorias [31]: Sistemas Detectores de Intrusão baseados em Host (SDIH) e Sistemas Detectores de Intrusão de Rede (SDIR). Um SDIH coleta e analisa informações relativas a um host, como quantidade de recursos (memória, processamento, disco) utilizada, número de processos, variáveis de ambiente etc. É necessária, para o funcionamento de um SDIH, a instalação do coletor no host a ser analisado; o analisador pode estar na mesma máquina ou em outro computador da rede.

Já um SDIR utiliza para análise informações coletadas em uma rede de computadores, como volume de tráfego, número de conexões, fluxos, pacotes perdidos etc. É preciso ter um coletor acoplado a uma rede, capturando os pacotes que passarem por ela, ou outros equipamentos capazes de coletarem informações de tráfego de rede. A coleta de informações internas de um host é dificultada ou não desejável em alguns ambientes, por razões de segurança e privacidade individuais. Este artigo está focado nesta abordagem.

2.1.1 Sistemas Detectores de Intrusão baseados em *Host*

Sistemas Detectores de Intrusão baseados em Host (SDIH) são ferramentas usadas para detectar atividades maliciosas em um único computador [20]. Um SDIH é desenvolvido para um único computador e usa um software que monitora as atividades do sistema operacional e dos programas que rodam sobre o sistema, como acesso a arquivos, chamadas de sistema e logs do sistema. Quando há uma alteração em um arquivo ou parâmetro monitorado, o SDIH compara o evento com as assinaturas de ataques predefinidas e, caso haja uma correspondência, sinaliza o evento como ilegal. O SDIH também pode ser usado para monitorar uma rede ou segmento de rede, embora este uso apresente alguns problemas, como o fato de só ser possível analisar o tráfego de rede que passa pelo computador. Um exemplo SDIH é o Tripware [46], que pode ser usado para a detecção de alterações maliciosas nos arquivos de um sistema monitorado. A Detecção de Intrusão baseada em host possui como vantagens a [20]:

- capacidade de verificar o sucesso ou falha de um ataque rapidamente pela análise de logs do evento: um SDIH possui informações mais precisas sobre um evento e menos propensa a falsos positivos. Neste caso o SDIH pode ser usado como complemento de um SDIR para verificação do sistema;
- monitoração em baixo nível: pelo fato de monitorar um host, um SDIH é capaz de analisar atividades de baixo nível, como acesso a arquivos, mudanças nas permissões de um arquivo, execução de arquivos e tentativas de mudanças de privilégios. Muitos ataques são tão discretos que apenas um SDIH é capaz de detectar;
- detecção quase em tempo real: o SDIH tem a capacidade de detectar eventos no host rapidamente e alertar o administrador;
- capacidade de analisar tráfego criptografado; um SDIH pode acessar as informações antes e após a encriptação;
- custo reduzido: não é necessário hardware dedicado ou adicional para a instalação de um SDIH.

O grande problema com o uso de SDIH é o processamento extra necessário apenas para analisar os dados coletados no computador. Em alguns casos esta sobrecarga pode comprometer o desempenho de todo o sistema computacional e inviabilizar a detecção. Os SDIH ainda apresentam outras desvantagens [20]:

- visão limitada: um SDIH possui uma visão limitada da rede;
- sujeito a fraudes: pelo fato de estarem mais perto do usuário, os SDIH são mais sujeitos a fraudes.

2.1.2 Sistemas Detectores de Intrusão de Rede

Os Sistemas Detectores de Intrusão de Rede (SDIR) [20] são SDI usados para monitorar toda uma rede, com o objetivo de detectar anomalias, ataques ou ações ilegais. Os SDIR usam para análise informações coletadas de uma rede, como volume de tráfego, número de conexões, fluxos e pacotes perdidos. É preciso ter um coletor acoplado a uma rede, capturando os pacotes que passarem por ela, ou outros equipamentos capazes de coletar informações de tráfego de rede. Um SDIR é constituído, normalmente, por alguns subsistemas [20]: Coletor, Analisador, Banco de Dados, Notificador, Atuador e Monitor.

O Coletor é um software que roda em uma máquina dedicada e usa um sensor ligado a uma fonte de informação, como uma rede ou um segmento de rede. O sensor pode estar em equipamento de rede ou computador ligado à rede. Normalmente, usa-se algum hardware de rede em modo "promíscuo", capturando todos os pacotes que passam, independentemente da origem ou destino. A biblioteca LIBPCAP [44], em conjunto com uma interface de rede em modo "promíscuo", tem sido amplamente usada [17] [40]. Noutros trabalhos [45] [48] [50] acessam-se diretamente as informações armazenadas em uma base MIB (Management Information Base), acessada via protocolo SNMP (Simple Network Management Protocol), em equipamentos de rede que disponibilizam este serviço. O desempenho do Coletor depende dos equipamentos de rede usados para a coleta, principalmente em redes de grande tráfego. Alguns firewalls atuam também como coletor, armazenando informações para um SDI [31].

O Analisador verifica os dados coletados, buscando por eventos que indiquem uma intrusão ocorrida ou que esteja ocorrendo. Há diferentes abordagens para a análise dos dados, como a baseada em assinaturas e a baseada em anomalias, com vários métodos diferentes, como métodos estatísticos, aprendizagem de máquina e baseados em conhecimento [13]. O Banco de Dados é o repositório de informações do SDI, onde são guardadas informações sobre o sistema monitorado e os eventos suspeitos. As informações guardadas no Banco de Dados dependem do método de detecção usado e da necessidade de se manter um histórico do sistema.

O sistema Notificador é responsável pelo envio de alertas ao administrador do sistema. A notificação pode ser um alerta na tela de um monitor, um aviso sonoro ou uma mensagem eletrônica. Alertas frequentes, com vários falsos positivos, são prejudiciais pois banalizam a detecção e acabam desacreditando a ferramenta. O desempenho de um SDI depende da relação entre falsos positivos e falsos negativos. Assim, é importante que o sistema possa ser ajustado [20]. O Atuador possui a capacidade de executar ações automatizadas conforme a Intrusão detectada. Tipicamente, a resposta a um evento intrusivo é a reconfiguração do roteador, alteração de regras no firewall ou a desconexão de algum usuário ou serviço. O Monitor ou Terminal de comando tem o objetivo de ser a ligação entre o administrador e o SDI. O Monitor pode ser usado para configurar o sistema, verificar o funcionamento do SDI e a ocorrência de Alarmes. As principais vantagens de um SDIR são [20]:

- habilidade de detectar ataques, que o SDIH não consegue porque monitora no nível de transporte da arquitetura de rede; neste nível, o SDIR pode analisar pacotes não apenas por endereços, mas também por números de porta. O SDIH, que monitora pacotes em baixo nível, pode não ser capaz de detectar alguns tipos de ataque;
- dificuldade de remover evidências: geralmente um SDIR está em uma máquina dedicada e protegida, o que dificulta a remoção de evidências por um atacante;
- detecção e resposta em tempo real: como o SDIR está em pontos estratégicos da rede, ele pode detectar intrusões e, tão rápido quanto possível, notificar o administrador;
- habilidade de detectar mesmo ataques malsucedidos: muitos ataques são parados por firewalls ou outros motivos; mesmo assim, informações referentes a esses ataques são importantes ao administrador.

O principal desafio no desenvolvimento de um SDIR é escolher um método eficiente, que identifique uma intrusão de maneira correta sem gerar um número excessivo de falsas detecções. Os SDIR apresentam algumas desvantagens [20]:

- pontos cegos: normalmente os sensores de um SDIR são colocados nas bordas da rede; com isso, algumas vezes alguns segmentos da rede não são vistos pelo SDIR;
- informações criptografadas: o SDIR não consegue analisar tráfego de rede criptografado, porém algumas vezes é possível analisar as informações dos cabeçalhos dos pacotes.

Como exemplos de SDIR mais conhecidos têm-se o Bro [5] e o Snort [41], ambos disponibilizados como software livre. Tanto o Bro quanto o Snort são baseados em assinaturas que por meio de ferramentas são compatíveis entre si. Há ainda plugins, em ambos os sistemas, para a inclusão da capacidade de detecção baseada em anomalias.

2.2 Classificação dos Sistemas Detectores de Intrusão quanto à abordagem de análise

Os SDI em geral, bem como os SDIR, também são classificados conforme a abordagem de análise dos dados: baseada em conhecimento (assinaturas) e baseada em comportamento (anomalias).

2.2.1 Detecção de Intrusões de Rede baseada em assinaturas

Os SDIR baseados em assinaturas [20], como o Bro [5] e o Snort [41], comparam os dados coletados da rede com uma base de dados de assinaturas de ataques conhecidos ou regras predefinidas e, quando os eventos analisados são compatíveis com alguma das assinaturas da base de dados, um alarme é disparado. Novas formas de ataques ou variações de ataques conhecidos surgem constantemente; por isso, para o bom funcionamento de um SDIR baseado em assinaturas é necessário manter a base de assinaturas de ataques atualizada. Porém, mesmo com uma base de assinaturas atualizada, tais SDIR têm dificuldade em detectar ataques desconhecidos, ataques mutantes ou camuflados. Os SDIR baseados em assinaturas são, portanto, bastante precisos em suas detecções, apresentando baixo número de falsos positivos; porém, devido a sua dificuldade de detectar ataques novos, podem apresentar um grande número de falsos negativos, o que pode representar uma brecha de segurança.

Resumidamente, as desvantagens da abordagem de Detecção de Intrusões baseada em assinaturas [20]:

- o sistema não é capaz de detectar ataques desconhecidos, ou seja, que não possuam uma assinatura arquivada;
- o sistema não é capaz de prever e detectar novos ataques.

2.2.2 Detecção de Intrusões de Rede baseada em anomalias

A Detecção de Intrusão usando a abordagem baseada em Anomalias apoia-se na ideia de que um ataque gera um desvio do comportamento padrão do sistema [11] [21]. Assume-se que a atividade maliciosa difere do comportamento padrão do sistema e que essa diferença pode ser expressada quantitativamente [21]. Os SDIR baseados em anomalias [13] [21] [45], SDIR-A, constroem um perfil do comportamento padrão da rede com base em informações do histórico, quando o comportamento observado se desvia significativamente deste perfil, ou seja, uma anomalia é detectada, um alarme é disparado. Os SDIR-A são conhecidos também como Sistemas Detectores de Anomalias de Rede [33].

Uma Anomalia é um evento que causa um desvio (alteração) em relação ao perfil (padrão) do sistema. Assume-se que uma Anomalia é indicativo de um ataque. De um modo amplo, uma Anomalia de rede pode ocorrer devido a um Ataque, falha de equipamento, problemas de configuração, sobrecarga ou uso abusivo ou inadequado de algum serviço ou recurso da rede. Embora o foco principal de um SDIR seja a detecção de Ataques, no caso de um SDIR baseado em anomalias, a possibilidade de detecção de outras anomalias de rede é interessante. A Detecção de Anomalias é a tarefa de determinar o que é normal e esperado para um sistema e encontrar ou diferenciar as anomalias.

Pelo fato de buscar por comportamentos anômalos, um SDIR baseado em anomalias é capaz de detectar ataques sem seu conhecimento prévio, sendo uma alternativa a abordagem baseada em assinaturas. O tráfego de rede, de modo geral, apresenta como característica alta variabilidade, dificultando a construção de um perfil para a rede e a definição de intervalos confiáveis de variação. Em algumas situações, mudanças do padrão de tráfego

de uma rede podem ser erroneamente identificadas pelo SDIR, como indício de um ataque ou falha, gerando um falso alarme. Os SDIR baseado em anomalias são capazes de detectar ataques desconhecidos; no entanto, uma das limitações ainda é a ocorrência de um grande número de falsos positivos.

Uma das dificuldades de SDIR baseados em anomalias está em construir um perfil da rede devido a algumas características específicas do tráfego de rede. As características do tráfego de rede, de modo geral, foram estudadas em alguns trabalhos [34] [43] [37], que apontam que algumas variáveis descritivas, como número de pacotes ou tamanho dos arquivos transmitidos, apresentam distribuição de probabilidade com cauda pesada, ou seja, com decaimento mais lento que a distribuição normal. Distribuição de probabilidade de cauda longa nas variáveis do tráfego de rede normalmente é devida principalmente à dependência de longa duração (LRD). A LRD, em uma variável, significa que a função de autocorrelação decai lentamente. A autossimilaridade ou característica fractal está relacionada à dependência de longa duração e refere-se à característica de uma variável de possuir a mesma distribuição de probabilidade em qualquer nível de agregação ou resolução. O tráfego de rede é muito variável, sendo constituído basicamente por picos, e devido as características de dependências de longa duração, autossimilaridade e distribuição de probabilidade com cauda pesada, é estatisticamente difícil identificar valores extremos e definir intervalos de confiança. Resumidamente, as desvantagens da abordagem de Detecção de Intrusões baseada em anomalias [20]:

- falsos positivos: muitas atividades anômalas, porém não intrusivas, são equivocadamente sinalizadas como intrusões;
- falsos negativos: intrusões podem não ser detectadas, caso não produzam alguma anomalia perceptível;
- são computacionalmente complexos, pela necessidade de criação e atualização de um perfil.

Abordagens de detecção por assinaturas podem ser adequadas para casos distintos de formas de ataques, enquanto que a abordagem baseada por anomalias é mais indicada para a detecção de ataques desconhecidos. Levando-se em conta a grande variedade de ataques existentes e o rápido surgimento de novos ataques, é possível o uso de um SDI híbrido, que incorpore os dois métodos, unindo as vantagens de ambos. Alguns projetos de SDIR baseados em anomalias conhecidos são: o EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances), o Prelude IDS, o POLVO-IIDS (Sistema de Detecção de Intrusão Inteligente Baseado em Anomalias) [28]. A maioria usa algum método de aprendizagem de máquina [13].

3 Principais técnicas usadas para a detecção de anomalias de rede

A detecção de anomalias em redes de computadores é uma área de estudo bastante ativa e várias técnicas são usadas. A classificação das técnicas de detecção de anomalias de rede, presentes na literatura, é uma tarefa difícil devido à diversidade e ao desenvolvimento constante de novas técnicas. Em [13], o autor classificou os métodos de detecção de anomalias de rede em métodos baseados: Conhecimento, Aprendizagem de Máquina e Análise Estatística. Neste texto usa-se a classificação conforme segue:

- Conhecimento: [45] Máquina de estados finitos; Sistemas especialistas ou baseado em regras; Busca por padrões (Pattern Matching);
- Aprendizagem de Máquina: Redes bayesianas [25]; Cadeias de Markov [13]; Redes Neurais [28]; Lógica difusa (*Fuzzy*) [49]; Algorítimos genéticos [38]; Algorítimos de agrupamento (Clustering) [24]; Sistemas imunológicos artificiais [16];
- Análise de Sinais: Análise estatística [36] filtros de Kalman [42]; CUSUM (CUmulative SUM) [45]; Séries Temporais [48]; Wavelets [17];

Em relação à classificação adotada em [13], neste texto acrescentaram-se na classificação dos métodos de detecção as técnicas derivadas da análise de sinais, separando-se algumas das técnicas de análise estatística. Na análise de sinais são usadas técnicas mais elaboradas para a modelagem dos dados e criação de um perfil que as baseadas na análise estatística básica.

Os métodos baseados em conhecimento, ou baseados em regras, fazem uso de um conjunto de regras e parâmetros elaborados e classificados por um especialista, usando algum formalismo, como máquina de estados finitos por exemplo. Tais métodos são muito robustos, apresentando poucos falsos positivos, e flexíveis. A principal desvantagem, no entanto, está na dificuldade e demora em se obter o conhecimento de qualidade necessário [13].

A abordagem de aprendizagem de máquina baseia-se no estabelecimento de um modelo implícito ou explícito que permite que padrões sejam analisados e classificados. São usadas diversas técnicas, como redes neurais e algorítimos de agrupamento, com diferentes propriedades. Contudo, a principal característica da abordagem está na necessidade de uma fase de treinamento com dados rotulados para a diferenciação do comportamento aceitável do não aceitável pelo sistema. As principais vantagens destes métodos estão na flexibilidade, adaptabilidade e capacidade de capturar interdependências desconhecidas nos dados. Porém, esta abordagem depende da determinação (rotulagem) do comportamento aceitável pelo sistema e os métodos empregados demandam muito de recursos computacionais [13].

Métodos derivados da análise de sinais têm sido propostos para a detecção de anomalias de rede [2]. Nos métodos baseados na análise de sinais, um perfil é criado representando o comportamento passado da rede. O perfil usa métricas de tráfego, como número de pacotes por protocolo, número de conexões e outras. Um alerta de anomalia é disparado quando o comportamento atual da rede difere significativamente do encontrado no perfil, ultrapassando algum limite (threshold) estabelecido. A principal vantagem desses métodos está em não precisar de algum conhecimento predefinido do comportamento padrão da rede, pois são capazes de se adaptar ao comportamento da rede. A principal dificuldade, no entanto, está na definição dos parâmetros, o que influencia na taxa de detecções e de falsos positivos.

Tendo como vantagem não necessitar de conhecimento predefinido ou de uma etapa de treinamento, as abordagens baseadas na análise de sinais tornam-se interessantes para uso na detecção de anomalias devido à variabilidade do tráfego de rede. Nesse sentido, a transformada wavelet, método de análise de sinais, demonstrou aplicabilidade para a análise do tráfego e detecção de anomalias de rede ([2], [45], [17], [14], [27], [19] e [9]) por permitir a análise em diferentes escalas de tempo [30]. A maioria dos métodos baseados na análise de sinais para detecção de anomalias de rede presentes na literatura ([17], [14], [27] e [19]) apresenta ao menos três etapas diferentes: Seleção de Variáveis, Transformação dos dados e Geração de Alarmes.

A detecção de anomalias é uma atividade complexa. A seleção do conjunto de variáveis usadas pelo processo de análise de dados influencia na capacidade de detecção do SDI e o número de variáveis usadas impacta no desempenho computacional da ferramenta. No entanto, a seleção de variáveis normalmente é guiada por critérios empíricos [1]. As variáveis selecionadas dependem também do tipo de SDI usado e dos tipos de ataques ou anomalias de interesse. Por exemplo, para um SDIR normalmente se está interessado nos endereços de origem e destino, portas e protocolos dos pacotes de rede. Quanto aos dados coletados em uma rede, um SDIR pode utilizar os dados do payload do pacote, como em [21], ou apenas as informações do header, como em [26] e [19].

A seleção de variáveis consiste na escolha das características (ou descritores) de rede a serem utilizadas para a análise. Normalmente, faz-se a distinção entre as características referentes a uma única conexão TCP daquelas referentes a múltiplas conexões. Conforme [32] as características do tráfego de rede, são classificadas como básicas e derivadas:

- características básicas: são características que representam a uma única conexão TCP/IP. Estas características são extraídas diretamente dos pacotes de tráfego de rede. Diferentes nomes também são usados para nomear estas características, como Características Básicas; Atributos Essenciais; Características Básicas de uma conexão TCP; Características TCP Básicas. Ainda podem incluir as Características de Fluxo, que englobam também os protocolos não orientados a conexão (exemplo: UDP, ICMP).
- características derivadas: representam múltiplas conexões TCP/IP ao mesmo tempo. Também são conhecidas como Características de Tráfego.

Ainda segundo [32], as características derivadas destinam-se a encontrar similaridades entre diferentes conexões de rede. Para a coleta dessas características podem ser usados dois tipos de janelas de observação. O primeiro tipo é baseado em uma janela com intervalo de tempo (por exemplo, 5 segundos), enquanto que no segundo tipo é usada uma janela com intervalo de conexões (por exemplo, as últimas 100 conexões). O uso desses

dois tipos diferentes de janelas separa as características derivadas em: características baseadas no tempo e características baseadas em conexões:

- baseadas no tempo: são computadas com respeito a um determinado intervalo de tempo passado. Esse tipo de características é boa para a detecção de ataques que geram anomalias de volume de tráfego, como ataques do tipo DDoS.
- baseadas em conexão: são computadas considerando-se o número de conexões passadas. Essas características são usadas apenas com protocolos de rede orientados à conexão, como TCP, e são boas na detecção de ataques que aconteçam em um grande intervalo de tempo.

Devido à diversidade de protocolos e serviços de rede existentes, a quantidade de características possíveis é imensa. Embora seja possível no desenvolvimento de um SDI considerar um número grande de características de rede para a detecção de anomalias, têm-se restrições de desempenho computacional. Portanto, as características de rede são escolhidas conforme a necessidade do SDI. Uma variável (contador) armazena uma amostragem de determinada característica de rede. O conjunto de amostragens, ordenadas no tempo, de uma variável forma uma série temporal, que é usada pela maioria dos métodos baseados na análise de sinais. Neste caso, fala-se especificamente das características de rede baseadas no tempo. Neste texto ainda se faz uma diferenciação entre variáveis primárias e variáveis derivadas. As variáveis primárias relacionam-se a características extraídas diretamente dos pacotes TCP/IP computadas conforme o intervalo de tempo predeterminado, como, por exemplo, número de pacotes trafegados; tamanho médio dos pacotes; quantidade em bytes de dados trafegados; número de pacotes referentes a determinado protocolo, como TCP, UDP ou ICMP; número de pacotes por porta ou serviço. Já as variáveis derivadas são composições ou relações de duas ou mais variáveis primárias, como, por exemplo, a diferença entre pacotes SYN e FIN; ou a relação entre diferente portas ou serviços. Na Figura 1 é representado o funcionamento de um método genérico de detecção de anomalias de rede. Inicialmente, os dados do tráfego de rede são coletados na forma de contadores, para que posteriormente sejam transformados (análise) e possibilitem a geração de alarmes.

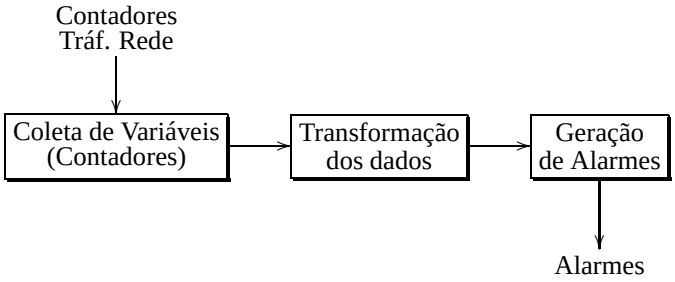

Figura 1. Fluxograma de um método genérico de detecção de anomalias de rede

Alguns trabalhos recentes [35] [15] [6] demonstram preocupação com a escolha das características de rede por um SDI e buscam por formas automatizadas de seleção. Em [35], o autor usou uma técnica de aprendizagem de máquina conhecida como Support Vector Machines (SVM) para a classificação e seleção das características de rede. Em [15] propôs um algoritmo baseado em Rede Neural para a seleção de variáveis. Já em [6], o autor propôs um algorítimo baseado em métodos de agrupamento (clustering), mais especificamente k-nearest neighbor (k-NN) e lógica difusa (fuzzy). Todos os trabalhos citados fizeram uso da base de dados do DARPA KDD 99 [18] e demonstraram uma redução do número de características consideradas importantes para detecção de ataques em um SDI.

A transformação dos dados (Figura 1) consiste na representação matemática das séries de dados de rede, de modo a remover tendências e tornar evidentes as singularidades. Na transformada wavelet, as séries de dados, no domínio do tempo, são representados no domínio do tempo e escala [30]. Algumas abordagens utilizam apenas a transformada wavelet, outras a utilizam em conjunto com outros modelos matemáticos [27]. A transformação dos dados de entrada possibilita, conforme a técnica usada, identificar as anomalias presentes no sinal e, consequentemente, permite a geração de alarmes.

Após a transformação dos dados, para que a detecção de anomalias ocorra é necessária a geração de alarmes (Figura 1), ou qualquer outra forma de aviso ou intervenção automatizada. Toda vez que as medidas estatísticas

dos dados mais recentes afastam-se consideravelmente de um modelo de tráfego padrão, construído com base no histórico da rede, deve ser gerado um alarme pelo sistema. Normalmente, esta análise é realizada sobre os dados transformados ou resíduos [27] e várias métricas estatísticas podem ser utilizadas, como média ou variância [14]. Para acomodar variações insignificantes, devido a algum componente estocástico do modelo, são definidos valores de threshold, que podem ser fixos [14] ou dinâmicos [19].

4 Transformadas wavelets e a detecção de anomalias de rede

As Transformadas Wavelet (TW) são ferramentas matemáticas usadas para analisar um sinal em diferentes níveis de resolução. Há diversas famílias de funções wavelet. Neste texto consideram-se as funções wavelets ortonormais da família discretas de Daubechies [10] por possuírem transformadas com algoritmos rápidos, sendo eficientes computacionalmente [29].

4.1 Transformada Wavelet

A Transformada Wavelet (tanto discreta quanto contínua) decompõe um sinal em vários níveis de representação. O nível mais grosseiro é responsável pela representação de comportamentos médios do sinal analisado. Cada novo nível da transformada contém informação complementar, variações complementares em relação ao comportamento médio, necessárias para reconstruir os dados originais no nível mais fino inicial.

A expressão (1) para a representação de uma série wavelet de um sinal $y[t] = (y_0, \ldots, y_{N-1})$, inicialmente dado como um vetor discreto, possui exatamente esta estrutura de multirresolução, sendo a combinação linear (somatório $c_{J,k}\phi_{J,k}$) a representação grosseira do sinal (segundo nomenclatura da área), tomada no nível mais grosseiro J. A partir desse conjunto, os demais dados acrescentados representam os complementos de informação até que o nível mais fino seja recuperado.

$$y[t] = \sum_{k=0}^{N_J} c_{J,k}\phi_{J,k}(t) + \sum_{j=J}^{1}\sum_{l=0}^{N_j} d_{j,k}\psi_{j,k}(t)\ t \in [0, N_0] \tag{1}$$

Em (1), $N_j = N/2^j - 1$ representa o número de pontos de cada novo vetor obtido pela transformação, $\phi_{j,k}(t)$ e $\psi_{j,k}(t)$ são as funções escala e *wavelet*, responsáveis pela transformação. Aqui, o parâmetro j indica escala (dilatação) e k, a posição (translação).

A Transformada Wavelet Discreta (TWD) direta de um sinal para a geração do conjunto de coeficientes é computada por sucessivas passagens pelo filtro G (passa baixa) e pelo filtro H (passa alta). Os filtros G e H são vetores de constantes já calculados e relacionados às funções escala e wavelet, respectivamente. Esse processo é conhecido como Algoritmo Piramidal de Mallat [29] e está representado na Figura 2.

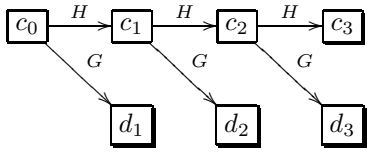

Figura 2. Representação do Algoritmo Piramidal de Mallat, Transformada *Wavelet* Discreta direta.

Na Figura 2, c_0 corresponde ao sinal original discreto $c_0 = y$, H denota o filtro passa-alta, G denota o filtro passa-baixa, d_1, d_2 e d_3 são os coeficientes wavelets ou detalhes, em cada nível, e c_3 são os coeficientes escala ou aproximação no último nível da transformada. Os coeficientes são encontrados pela convolução das constantes dos filtros:

$$c_{j+1,k} = \sum_{l=0}^{D-1} h_l c_{j,2k+l} \quad e \quad d_{j+1,k} = \sum_{l=0}^{D-1} g_l c_{j,2k+l}\ , \tag{2}$$

com $k = 0, \ldots, N/2^J - 1$ e D o número de constantes do filtro. Os coeficientes escala $c_{J,k}$ podem ser interpretados como a média local ponderada e os coeficientes wavelet $d_{j,k}$ representam a informação complementar ou os

detalhes que escapam da média ponderada. Os coeficientes da transformada ordenados por escala (j) e posição (k) são representados como

$$w = \left((c_{J,k})_{k=0}^{N_J} , \left((d_{j,k})_{k=0}^{N_J} \right)_{j=J}^{1} \right) , \tag{3}$$

ou seja, w é a representação finita (vetor) em termos apenas dos coeficientes da decomposição do sinal na Equação (1). A Figura 3 exemplifica graficamente o processo de decomposição do sinal em coeficientes wavelet pela transformada. A cada nível da transformada (Figura 3) o tamanho dos vetores resultantes é reduzido pela metade $k = 0 \ldots N/2^j$. São mantidas as informações sobre os detalhes (coeficientes wavelet) em diferentes escalas.

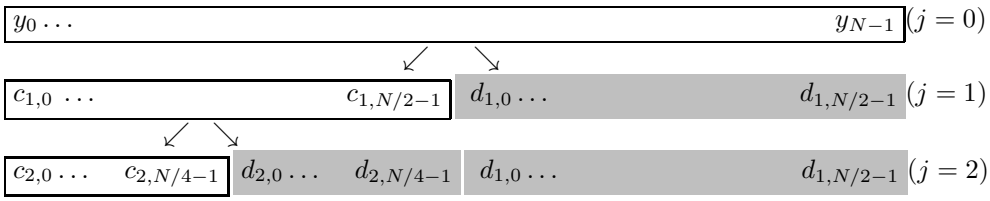

Figura 3. Representação da Transformada Wavelet Discreta do sinal y com dois níveis de transformação. Os coeficientes wavelet sombreados são obtidos a cada nível e permanecem inalterados nos níveis subsequentes.

A Transformada Wavelet Packet (TWP) [7] é uma generalização do algoritmo piramidal da TW tradicional. Na TWP, contudo, ambos os coeficientes da aproximação e detalhes são decompostos. A TWP gera 2^N grupos diferentes de coeficientes, em comparação com a TW tradicional, que gera $N + 1$. No entanto, devido à redução da escala em cada passo, o número total de coeficientes é igual ao sinal original, da mesma forma que a TWD tradicional, e dessa forma não há redundância.

Além da TWD há a Transformada Wavelet Contínua (TWC) [10]. A TWC surgiu como uma alternativa à transformada de fourier. Como computadores não processam sinais contínuos, a TWC é computada usando-se uma versão discretizada. No entanto, a versão discretizada da TWC não é equivalente à TWD. A TWC discretizada não é realmente uma transformada discreta. A TWC produz informações altamente redundantes e essa redundância requer mais recursos computacionais.

4.2 Detecção de anomalias de rede via transformada *wavelet*

Estudos demonstraram que anomalias de rede podem se manifestar em diferentes escalas de tempo [2]. Em escalas maiores são detectadas anomalias de longa duração e em escalas menores (mais finas), anomalias de curta duração ou variações abruptas [2]. É sabido que o tráfego de rede possui diversas propriedades estatísticas e exibe dependências curtas (SRD - Short-Range Dependence) e longas (LRD - Long-Range Dependence) em sua estrutura de correlação [22] [4]. A estrutura de correlação complexa dificulta a caracterização do tráfego de rede. No entanto, a transformada wavelet possui a capacidade de reduzir as complexas relações temporais do tráfego de rede em SRD nos coeficientes wavelet [47]. Como exemplos de trabalhos que usam a transformada wavelet para a detecção de anomalias de rede citam-se [8], [14], [27] e [19], sendo destacadas as suas principais características no Quadro 1.

No trabalho de Dainotti et al. [8] foi proposto um mecanismo de detecção de anomalias de volume de tráfego de rede com o objetivo de detectar ataques do tipo DoS. O sistema combina uma abordagem tradicional, baseado em Somas Cumulativas (CUSUM - CUmulative SUM) e Médias Móveis Exponencialmente Ponderadas (EWMA - Exponentially Weighted Moving Average) com uma nova abordagem baseada na Transformada Wavelet Continua (TWC) e Threshold. A arquitetura é baseada em dois estágios: o primeiro usa EWMA e Thresholds e destina-se a fazer a detecção superficial de ataques; o segundo usa a TWC e destina-se à refinação e detecção "fina" dos ataques para diminuir o número de falsos alertas.

No trabalho de Gao et al. [14] foi proposto um detector de anomalias de rede baseado na Transformada wavelet Packet (TWP). Os dados de rede são transformados utilizando-se a transformada direta wavelet packet, com bases wavelet da família Daubechies, e reconstruídos a partir dos coeficientes wavelet para cada nível da

Trabalho	wavelet usada	Outros métodos	Principais características
1. Dainotti et al. (2006) [8]	TWC, família Morlet	CUSUM, EWMA	Arquitetura de dois estágios: CUSUM-EWMA e TWC.
2. Gao et al. (2006) [14]	TWP, família Daubechies	Média e variância	Maior número de escalas para a análise (mais apurado) por causa da TWP. Reconstrução do sinal (TW inversa) em cada nível.
3. Lu et al. (2008) [27]	TWD, Daubechies, Coiflets, Symlets ou Discrete Meyer	ARX, GMM	Processo em duas fases: TWD e ARX.
4. Kim et al. (2008) [19]	TWD, família de Daubechies	Desigualdade de Chebyshev	Reconstrução do sinal em cada nível.

Tabela 1. Comparação de alguns trabalhos que usam a transformada wavelet para a detecção de anomalias de rede

transformada. Medidas estatísticas, como média e variância, foram usadas para caracterizar uma anomalia, como a razão da média ou da variância entre a janela de detecção e a janela histórica foram mensuradas e comparadas com valores de threshold predefinidos para identificar uma anomalia.

No trabalho de Lu et al. [27] foi usada uma abordagem para detecção de anomalias de rede baseada na transformada wavelet e séries autorregressivas. No sistema proposto foram selecionadas variáveis descritoras de tráfego usando-se o modelo de agregação por fluxos origem-destino. O sinal original é transformado usando-se wavelets (transformada wavelet discreta) e os coeficientes wavelet $d_{j,k}$ aproximados, usando-se um modelo de predição autorregressivo do tipo ARX (AutoRegressive with eXogenous input), e o resíduo da predição é usado para a detecção de anomalias utilizado o GMM (Gaussian Mixture Model). A estratégia de detecção de anomalias consiste na identificação de outliers (valor significativamente diferente dos demais), assumindo-se que a presença destes no resíduo indica a existência de anomalias no tráfego da rede.

No trabalho de Kim et al. [19] foi proposto um detector baseado na análise da correlação dos endereços IP de destino no tráfego de saída de um roteador. A principal diferença deste trabalho em relação aos demais é, justamente, a forma como os dados são agrupados. No primeiro estágio, as informações nos cabeçalhos dos pacotes TCP/IP ou vindos de uma base do NetFlow, como endereço IP e porta de destino, são selecionadas e agrupadas para reduzir o volume de informação. Em seguida, num segundo estágio, as séries são submetidas a uma transformada wavelet discreta direta e posteriormente são reconstruídos, com a transformada wavelet inversa, conforme a escala selecionada. No último estágio é verificada a regularidade das informações comparando-se o histórico dos dados, por meio de thresholds. A presença de outliers no sinal é considerada indicador de anomalias. Thresholds são estabelecidos com auxílio da desigualdade de Chebyshev e com um intervalo de confiança predefinido.

Comparações entre os trabalhos quanto ao desempenho na detecção de ataques é uma tarefa difícil devido às diferentes metodologias de obtenção e uso dos dados de entrada empregados em cada trabalho. Com respeito ao custo computacional, a TWD é mais eficiente se comparada à TWC e à TWP. Além disso, o desempenho de cada mecanismo depende do uso da TW inversa e dos outros métodos empregados em conjunto. Como o estudo dos mecanismos propostos nos trabalhos citados, constataram-se a viabilidade do uso da TW na detecção e a diversidade das configurações/estratégias empregadas nos mecanismos. Dessa forma, consideram-se importantes em estudos futuros a simplificação das estratégias empregadas e a verificação da influência de cada estratégia na detecção.

5 Considerações finais

Nas atuais redes de computadores, a coleta, análise e detecção de anomalias tem sido um desafio constante, principalmente devido à quantidade de dispositivos conectados, à variedade de protocolos e serviços, ao volume elevado de tráfego, bem como às características intrínsecas do tráfego padrão. Este artigo apresentou os principais conceitos relacionados ao desenvolvimento de Sistemas Detectores de Intrusão de rede, dando especial ênfase à abordagem de detecção de intrusão por anomalias baseada na transformada wavelet. A detecção de anomalias em redes de computadores é uma área de estudo bastante ativa e normalmente se preocupa com a eficiência dos

métodos e com o problema dos falsos positivos.

Na Detecção de Anomalias de Rede, o método de análise é de vital importância, pois impacta diretamente no desempenho e na eficiência do detector. A abordagem em tempo real ainda apresenta alguns desafios, por precisar de resposta a um determinado evento suspeito em tempo reduzido. Consequentemente, o mecanismo de detecção precisa ser eficiente para permitir tempos de resposta reduzidos. Nesse contexto, o uso da transformada wavelet mostrou-se promissor para a detecção de anomalias de rede devido a sua capacidade de análise em multirresolução e a sua baixa complexidade computacional. Um desafio da pesquisa em detecção de anomalias de rede compreende o aprimoramento dos mecanismos, em razão da diversidade das wavelets e das estratégias usadas.

Referências

[1] ABDOLLAH, M. F. et al. Revealing the Influence of Feature Selection for Fast Attack Detection. *IJCSNS International Journal of Computer Science and Network Security*, v. 8, p. 107-115, 2008.

[2] BARFORD, P. et al. A signal analysis of network traffic anomalies. In: 2nd ACM SIGCOMM Workshop on Internet Measurment, New York, NY, USA. *Proceedings...* ACM, p. 71-82, 2002.

[3] BOLZONI, D. Revisiting anomaly-based network intrusion detection systems. PHD Thesis. University of Twente, 2009.

[4] BORGNAT, P. et al. Seven Years and One Day Sketching the Evolution of Internet Traffic. *Infocom 2009*, HAL - CCSD, 2008.

[5] PAXSON, V. Bro: a system for detecting network intruders in real-time. In: 7th Conference on Security Synposium. *Proceedings...*, San Antonio, Texas: USENIX Association, 1998. p. 3.

[6] CHOU, T. S.; YEN, K. K.; LUO, J. Network Intrusion Detection Design Using Feature Selection of Soft Computing Paradigms. *International Journal of Computational Intelligence*, v. 4, n. 3, 2008.

[7] COIFMAN, R. R.; WICKERHAUSER, M. V. Entropy-Based Algorithms For Best Basis Selection. *IEEE Transactions on Information Theory*, v. 38, p. 713-718, 1992.

[8] DAINOTTI, A.; PESCAPE, A.; VENTRE, G. Wavelet-based Detection of DoS Attacks. In: Global Telecommunications Conference. *Proceedings...*, p. 1-6, 2006.

[9] DALMAZO, B. L. et al. Filtros de Alarmes de Anomalias através de Wavelets. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, (SBSeg 2009), IX, Campinas, SP, Brasil. *Anais...*, 2009.

[10] DAUBECHIES, I. Ten Lectures on Wavelets. *SIAM*, n. 61, 1992.

[11] DENNING, D. E. An intrusion-detection model. *IEEE Transaction on Software Engineering*, v. 13, n. 2, p. 222-232, 1987.

[12] FARRAPOSO, S. *Contributions on detection and classification of internet traffic anomalies.* PHD Thesis, Université Paul Sabatier - Toulouse III, 2009.

[13] GARCÍA-TEODORO, P. et al. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers and Security*, v. 28, p. 18-28, 2009.

[14] GAO, J. et al. Anomaly Detection of Network Traffic Based on Wavelet Packet. In: Asia-Pacific Conference on Communications. *Proceedings*, 2006.

[15] GHALI, N. I. Feature Selection for Effective Anomaly-Based Intrusion Detection. *IJCSNS International Journal of Computer Science and Network Security*, v. 9, n. 3, 2009.

[16] GUANGMIN, L. Modeling Unknown Web Attacks in Network Anomaly Detection. In: Third International Conference on Convergence and Hybrid Information Technology. *Proceedings*, v. 2, p. 112-116, 2008.

[17] HUANG, C.; THAREJA, S.; SHIN, Y. Wavelet-based Real Time Detection of Network Traffic Anomalies. In: Securecomm and Workshops. *Proceedings*, p.1-7, 2006.

[18] HETTICH, S.; BAY, S. D. *The UCI KDD Archive.* 1999. Disponível em: <http://kdd.ics.uci.edu>. Acesso em: jan. 2010.

[19] KIM, S. S.; REDDY, A. L. N. Statistical techniques for detecting traffic anomalies through packet header data. *IEEE/ACM Transaction on Networking*, Piscataway, NJ, USA: IEEE Press, v. 16, n. 3, p. 562-575, 2008.

[20] KIZZA, J. M. *Guide to Computer Network Security*. New York, NY: Springer, 2005.

[21] KRUEGEL, C.; VIGNA, G. Anomaly detection of web-based attacks. In.: 10th ACM conference on Computer and communications security. *Proceedings*, New York, NY, USA: ACM, p. 251-261, 2003.

[22] LELAND, W. et al. On the self-similar nature of Ethernet traffic (extended version). *IEEE/ACM Transaction on Network*, Piscataway, NJ, USA: IEEE Press v. 2, n. 1, p. 1-15, 1994.

[23] LI, L.; LEE, G. DDoS attack detection and wavelets. In: 12th International Conference on Computer Communications and Networks. *Proceedings*, 2003.

[24] LI, Y.; FANG, B. A Lightweight Online Network Anomaly Detection Scheme Based on Data Mining Methods. In: IEEE International Conference on Network Protocols. *Proceedings*, p. 340-341, 2007.

[25] LIU, T. et al. Method for network anomaly detection based on Bayesian statistical model with time slicing. In: 7th World Congress on Intelligent Control and Automation. *Proceedings*, p. 3359-3362, 2008.

[26] LONGCHUPOLE, S.; MANEERAT, N.; VARAKULSIRIPUNTH, R. Anomaly detection through packet header data. In: 7th International Conference on Information, Communications and Signal Processing. *Proceedings*, p. 1-4, 2009.

[27] LU, W.; TAVALLAEE, M.; GHORBANI, A. A. Detecting Network Anomalies Using Different Wavelet Basis Functions. In: Communication Networks and Services Research Conference. *Proceedings*, p. 149-156, 2008.

[28] MAFRA, P. et al. POLVO-IIDS, Um Sistema de Detecção de Intrusão Inteligente Baseado em Anomalias. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, (SBSeg 2008), VIII. *Anais*, p. 201-214, 2008.

[29] MALLAT, S. G. *A wavelet tour of signal processing.* Academic Press, 1998.

[30] NIELSEN, O. M. *Wavelets in scientific computing.* PHD Thesis. Informatics and Mathematical Modelling, Technical University of Denmark, DTU, 1998.

[31] NORTHCUTT, S.; NOVAK, J. *Network Intrusion Detection, Third Edition*. New Riders Publishing, 2002.

[32] ONUT, L.; GHORBANI, A. A. A Feature Classification Scheme For Network Intrusion Detection. *International Journal of Network Security*, v. 5, n. 1, p. 1-15, 2007.

[33] PLONKA, D.; BARFORD, P. Network anomaly confirmation, diagnosis and remediation. In: 47th Annual Allerton Conference on Communication, Control, and Computing. *Allerton*, p. 128 -135, 2009.

[34] ROHANI, M. F. et al. LoSS Detection Approach Based on ESOSS and ASOSS Models. In: Fourth International Conference on Information Assurance and Security. *Proceedings*, p. 192-197, 2008.

[35] SAFAA, Z.; KARRAY, F. Features selection for intrusion detection systems based on support vector machines. In: 6th IEEE Conference on Consumer Communications and Networking Conference. *Proceedings*, Las Vegas, NV, USA: IEEE Pres, p. 1066-1073, 2009.

[36] SAMAAN, N.; KARMOUCH, A. Network anomaly diagnosis via statistical analysis and evidential reasoning. *Network and Service Management, IEEE Transactions on*, v. 5, n. 2, p. 65-77, 2008.

[37] SCHERRER, A. et al. Non-Gaussian and Long Memory Statistical Characterizations for Internet Traffic with Anomalies. *IEEE Transactions on Dependable and Secure Computing*, v. 4, p. 56-70, 2007.

[38] SELVAKANI, S.; RAJESH, R. S. Genetic Algorithm for framing rules for intrusion Detection. *International Journal of Computer Science and Network Security*, v. 7, n. 11, 2007.

[39] SILVA, L. S. et al. Montes, A. Detecting attack signatures in the real network traffic with ANNIDA. *Expert Systems with Applications*, Elsevier, v. 34, p. 2326-2333, 2008.

[40] SILVA, L. S. *Uma Metodologia para Detecção de Ataques de Redes baseada em redes Neurais.* PHD Thesis. Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, SP, Brasil, 2008.

[41] ROESCH, M.; STANFORD TELECOMMUNICATIONS. Snort - Lightweight Intrusion Detection for Networks. In: 13TH USENIX CONFERENCE ON SYSTEM ADMINISTRATION. *Proceedings*, Seattle, Washington: USENIX Association, p. 229-238, 1999.

[42] SOULE, A.; KAVE, S.; TAFT, N. Combining filtering and statistical methods for anomaly detection. In: 5th ACM SIGCOMM conference on Internet Measurement. *Proceedings*, Berkeley, CA, USA: USENIX Association, p. 31, 2005.

[43] STOEV, S. et al. On the wavelet spectrum diagnostic for Hurst parameter estimation in the analysis of Internet traffic. *Computer Networking*, New York, NY, USA: Elsevier North-Holland, Inc., v. 48, n. 3, p. 423-445, 2005.

[44] TCPDUMP. TCPDUMP/LIBPCAP public repository, 1998. Disponível em: <http://www.tcpdump.org>. Acesso em: jan. 2011.

[45] THOTTAN, M.; JI, C. Anomaly detection in IP networks. *IEEE Transactions on Signal Processing*, v. 51, n. 8, p. 2191-2204, 2003.

[46] Tripware, There is more than one Tripwire, 2010. Disponível em: <http://www.tripware.org>. Acesso em: fev. 2011.

[47] WANG, X.; REN, Y.; SHAN, X. WDRLS: a wavelet-based on-line predictor for network traffic. In: IEEE Global Telecommunications Conference. *Proceedings*, v. 7, p. 4034-4038, 2003.

[48] WU, Q.; SHAO, Z. Network Anomaly Detection Using Time Series Analysis. In: Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services. *Proceedings*, p. 42, 2005.

[49] YAO, L.; ZHITANG, L.; SHUYU, L. A Fuzzy Anomaly Detection Algorithm for IPv6. In: Second International Conference on Semantics, Knowledge and Grid. *Proceedings*, p. 67, 2006.

[50] ZARPELÃO, B. et al. Detecção de Anomalias em Redes de Computadores. In: SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES, XXVII. **Anais...**, 2009.