Evolução dos Trabalhos em Detecção de Anomalias na Rede

Lília de Sá Silva
DSS-LAC/INPE
lilia@dss.inpe.br

Antonio Montes
CENPRA/INPE
antonio.montes@cenpra.gov.br

José Demisio Simões da Silva
LAC/INPE
demisio@lac.inpe.br

Resumo

Neste artigo são apresentadas as atividades realizadas até o momento para o desenvolvimento de um sistema de detecção de intrusão baseado em rede, para o qual é utilizada a abordagem baseada em anomalias. O objetivo deste sistema é sinalizar desvios do comportamento normal de uma rede, os quais podem indicar a ocorrência de ataques. Inicialmente, é apresentada uma breve descrição do objetivo do trabalho e da situação atual em que se encontra. Na seção 2, o ambiente configurado para a monitoração do tráfego de rede é descrito. Em seguida, é apresentada a estratégia de recuperação de atributos a partir da qual será desencadeada a representação do comportamento normal da rede, na seção 3. Finaliza-se este artigo com conclusões e descrição dos próximos desafios a serem enfrentados.

Palavras-chave: *detecção de intrusão, detecção de ataques, detecção por anomalia, ids, aplicação de redes neurais.*

1. Introdução

Para proteger uma rede de computadores do ciber-terrorismo é necessária a implantação de um sistema de defesa em profundidade, considerando várias camadas de segurança [11]. Fortalecimento dos sistemas de *hosts* da rede, análise periódica da configuração de segurança do ambiente e dos registros de eventos (logs) dos sistemas, estratégia de localização dos recursos, uso de sistemas de filtragem e controle do tráfego, configuração de regras de controle de acesso em elementos ativos de rede e implantação de sistemas de detecção de intrusão, são exemplos de camadas de segurança que podem tornar uma rede mais segura.

Detecção de intrusão corresponde a um conjunto de técnicas que são usadas para identificar ataques contra computadores e infra-estrutura de rede. Os métodos mais desenvolvidos para detectar ciber-ataques à rede utilizam técnicas de detecção baseadas em assinaturas [2,14,16]. Tais métodos possuem a limitação de detectar apenas ataques previamente conhecidos representados por meio de assinaturas. Uma assinatura é manualmente inserida em um banco de dados para cada novo tipo de ataque que é descoberto. Esta limitação conduz ao interesse crescente pelo uso de técnicas de detecção de intrusão baseadas em *datamining* [1,5,8,10,12], descritas basicamente em duas categorias: detecção por abuso e detecção por anomalia.

Na detecção por abuso, cada instância de um conjunto de dados é rotulada como "normal" ou "intrusiva" e um algoritmo é treinado a partir dos dados rotulados. Neste tipo de técnica, os modelos de detecção de intrusão são automaticamente re-treinados a partir de dados de entrada diferentes que descrevem novos tipos de ataque, uma vez que tenham sido adequadamente rotulados [8]. Pesquisas em detecção por abuso são centradas principalmente na classificação de intrusões pelo uso de algoritmos de *datamining* padrão, modelos de predição de classe rara, regras de associação e modelagem de custo sensitivo [5,8]. Diferente dos sistemas de detecção de intrusão baseados em assinaturas, os modelos por abuso são criados de forma automática, e costumam ser mais sofisticados e precisos que as assinaturas criadas manualmente. Uma grande vantagem do uso de técnicas baseadas em abuso é seu alto grau de exatidão na detecção de ataques conhecidos e suas variações. A principal desvantagem é a incapacidade de detectar ataques cujas instâncias ainda não tenham sido observadas.

Detecção por anomalia, por outro lado, é uma metodologia de detecção de intrusão em que perturbações do comportamento normal sugerem a presença de ataques, falhas, defeitos e outras ameaças, induzidas intencionalmente ou não. Dado um conjunto de dados normais para treinamento e dado uma nova porção de dados de teste, o objetivo do algoritmo de detecção de intrusão por anomalia é determinar se os dados de teste pertencem a um comportamento "normal" ou "anômalo".

A proposta de uma solução híbrida para detecção de intrusos em redes de computadores, apresentada no WORCAP 2004 [15], tem como objetivo o desenvolvimento de um sistema de detecção de intrusão baseado em anomalia intitulado ANIS – *ANomaly Identification-based Intrusion detection System* , em que técnicas de *datamining*, tais como redes neurais, deverão ser utilizadas para a identificação de informações anômalas em grandes conjuntos de dados do tráfego de rede.

Os módulos da aplicação em desenvolvimento são ilustrados na figura 1, a seguir, e devem realizar as seguintes tarefas: captura de pacotes, filtragem de dados, extração de atributos, modelagem do perfil normal, classificação de eventos e identificação de ataques.

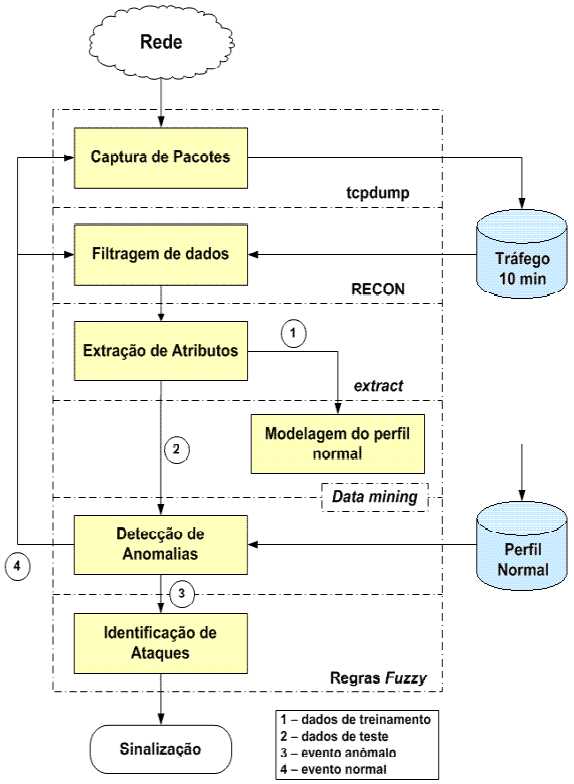

Figura 1: Arquitetura modular do sistema

O módulo "Captura de dados" será utilizado para a coleta de dados de pacotes trafegando pela rede. O módulo "Filtragem" é destinado à reconstrução de todas as sessões de interesse do tráfego. A seleção de dados relevantes para compor as instâncias que descreverão o comportamento atual da rede será realizada pelo módulo "Extração de Atributos". O módulo de "Modelagem do perfil normal" tem por finalidade o armazenamento das instâncias de treinamento em bancos de dados, quando preparando o conjunto de dados de treinamento (etapa 1) para o detector inteligente.

Quando efetuando os testes e aplicação do sistema (etapa 2) , será executado o módulo "Detecção de Anomalias" para a identificação de eventos ilegítimos na rede. Em caso de descoberta de atividade hostil, o tipo de ataque será identificado (etapa 3) e informado ao operador do sistema.

Para o desenvolvimento do sistema proposto, as seguintes ações estão sendo realizadas:

- pesquisas na área: formato dos protocolos de rede TCP-IP [17]; identificação e recuperação de conjuntos de atributos que representam o comportamento da rede observada [6,8]; mapeamento do comportamento normal da rede; estudo de perfis de ataques à rede [4,9,11]; estudo de redes neurais e lógica *fuzzy*; acompanhamento da evolução dos trabalhos publicados na área [5,6,7,8,13,18,19];
- preparação do ambiente para monitoração do tráfego e captura de dados;
- coleta e análise de dados com tcpdump e Ethereal;
- estudos e reconstrução de sessões com o sistema RECON [3];
- desenvolvimento do sistema ANIS com os módulos: módulo de filtragem de dados, módulo de extração de atributos, módulo de modelagem do perfil normal, módulo de classificação e módulo de decisão.

Neste trabalho, são apresentadas as etapas concluídas e aquelas em desenvolvimento para a construção do sistema.

Pesquisas já realizadas envolvem o significado dos campos de formatação dos protocolos de rede TCP/IP, identificação de atributos-chave dos pacotes de rede e estudos de perfis de ataques à rede. Pacotes com informações de ataques simulados continuam sendo avaliados, dados de tráfego com traços de ataque são comparados aos dados do tráfego normal de uma rede de teste controlada em uso e, à medida que a pesquisa se desenvolve, novas informações estão sendo agregadas ao trabalho.

O ambiente de monitoração do tráfego da rede interna de produção determinada para os testes de desenvolvimento do sistema encontra-se operacional e em correto funcionamento. Dados do tráfego monitorado pelos sistemas *tcpdump* e *Ethereal* têm sido estudados. Na fase atual, dados de atributos do sistema RECON estão sendo recuperados e serão armazenados em uma base de dados para facilitar as análises realizadas.

Nesta etapa, parâmetros do sistema RECON, que correspondem a atributos de diferentes sessões do tráfego (HTTP, SMTP, DNS, SSH, por exemplo), os quais são armazenados em memória (árvore de sessões), estão sendo investigados e recuperados para a criação de uma base de atributos úteis. Na fase atual de desenvolvimento do ANIS, inicia-se a construção do Módulo "Extração de Atributos" do ANIS, onde os

atributos relevantes das sessões reconstruídas pelo RECON serão coletados e armazenados em base de dados, no caso da etapa de preparação de dados de treinamento ou serão encaminhados para o módulo de detecção de anomalias, na fase de testes ou de análise dos dados de produção.

2. Preparação do ambiente para monitoração do tráfego

O comportamento de duas redes – Rede de Teste e Rede de Produção – tem sido estudado. A coleta de dados destas redes é realizada através de um sensor localizado no ambiente de monitoração do tráfego preparado para esta finalidade.

A Rede de Teste corresponde à rede utilizada para os testes de aplicação de ataques simulados e monitoração do tráfego. Esta rede reside no ambiente do Laboratório de Redes da Divisão de Desenvolvimento de Sistemas de Solo "LabRedes-DSS". Até o momento, são utilizados três computadores nos quais são instaladas aplicações cliente e servidoras em ambiente Windows e Linux, além de ferramentas de análise e exploração de vulnerabilidades de sistemas, conforme necessário. Os serviços instalados até o momento na Rede de Testes são: HTTP (IIS e Apache), DNS, FTP e SSH.

À medida que diferentes ataques a serviços precisam ser aplicados, a Rede de Teste tem a sua configuração modificada. O tráfego desta rede é observado por intermédio de ferramentas, tais como tcpdump, Ethereal e scripts de monitoração de rede.

Na Rede de Teste foram identificadas, através da ferramenta Languard e outras ferramentas similares, algumas brechas de segurança em máquinas Windows, enquanto aplicações como Nessus e scripts de varreduras foram utilizadas para identificar vulnerabilidades em maquina Linux. Alguns sistemas do ambiente desenvolvido foram fortalecidos segundo os procedimentos encontrados em livros [4], pesquisas pela Internet e conforme recomendações aprendidas nos cursos de Segurança em Redes do INPE, enquanto algumas vulnerabilidades de serviços de rede de alguns hosts foram estrategicamente mantidas para a realização dos testes.

O ambiente de rede principal (Rede de Produção) monitorado neste trabalho é a RedeBeta, rede interna do INPE utilizada para compartilhamento e integração de conhecimento entre um grupo de usuários da ETE (Área de Engenharia e Tecnologia Espacial). Para a monitoração deste ambiente foi implementado o sensor de rede descrito na próxima seção.

2.1. Características do sensor de rede

O sensor de rede é um dispositivo utilizado para a captura de dados que são introduzidos e processados em sistemas de monitoramento de rede ou de detecção de intrusão.

Neste trabalho, o sensor utilizado para a monitoração da Rede de Produção é um microcomputador denominado "Maquina de Captura", com as seguintes características: Pentium 4 com 1.5 GHz de velocidade de processamento; disco rígido com capacidade para armazenamento de até 120 GB de dados; memória RAM de 520 MB e sistema operacional Linux *Slackware*.

Para fortalecimento da Máquina de Captura foram instalados apenas os serviços de rede e pacotes do sistema operacional necessários para as operações desejadas, além da configuração segura de parâmetros dos arquivos de pacotes e serviços instalados.

Como a Máquina de Captura possui uma comunicação com a rede externa para backup de dados, foi configurado o serviço de filtragem de pacotes, para bloquear o tráfego indesejado. Além disto, o relógio do computador foi sincronizado com serviço de tempo de referência para armazenar informações de data-hora corretas nos históricos de eventos registrados.

2.2. Posicionamento do sensor

Existem várias possibilidades de posicionamento do sensor na rede e que influenciam diretamente na eficiência dos resultados gerados pelo monitor de rede ou pelo detector de intrusões após análise dos dados coletados [3]. No ambiente configurado para este trabalho, o sensor é colocado fora dos limites de proteção do *firewall*, de modo que todo o tráfego destinado à ou proveniente da Rede de Produção é coletado. Esta configuração permite a observação de ataques direcionados ao *firewall* e a recursos protegidos por este. Deste modo, a quantidade de dados a serem tratados é consideravelmente grande.

Conforme ilustrado na figura 2, o sensor de rede está conectado a uma porta do *switch* para a qual é espelhado o tráfego de entrada e saída do *firewall*, o que viabiliza a observação de todo o tráfego passando pelo ponto de monitoramento em questão. O sentido unidirecional da seta representa o tráfego fluindo para o sensor, indicando que o sensor é passivo, ou seja, não interage com outros dispositivos, apenas transfere dados coletados para *backup* em outra máquina.

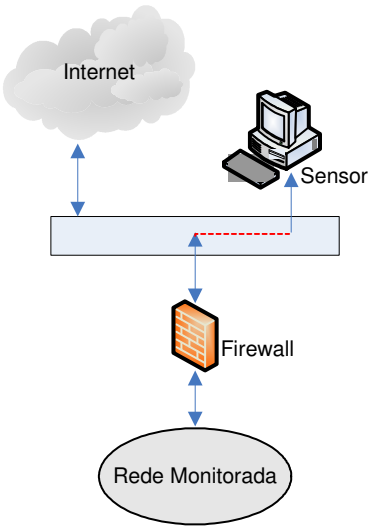

Figura 2: Posicionamento do sensor na rede

2.3. Estratégia para captura de dados

Os dados da Rede de Produção são capturados pelo sensor através de chamadas ao programa *tcpdump* implementadas nos *Shell* scripts codificados em linguagem C e compilados pelo GCC em ambiente *Linux Slackware*. A captura de dados é efetuada utilizando-se a biblioteca *libpcap* implementada no *tcpdump*. Um script de rotacionamento de logs (rotatedump.sh) é utilizado para manter o processo tcpdump em execução, coletando todo o tráfego destinado à rede monitorada através de interface em modo promíscuo, e para armazenamento dos *logs* de eventos em janelas de 10 minutos de tráfego. A cada hora os dados são armazenados em máquina remota através de um script específico para esta finalidade (senddump.sh).

3. Mapeamento do comportamento normal da rede

Com o ambiente de monitoração do tráfego preparado, um grande conjunto de dados, cerca de um mês e meio de tráfego total da RedeBeta registrado, hoje encontra-se disponível para os testes do sistema em desenvolvimento. Com o conjunto de dados armazenado, é possível realizar a extração de atributos de interesse dos pacotes de rede para mapeamento do comportamento normal da rede. Um total de 144 arquivos são armazenados por dia, tendo em média o tamanho de 2.5 MB cada um.

Participam deste grande conjunto, dados de pacotes de rede referentes às sessões TCP/IP do tráfego proveniente e em direção à Rede de Produção. Segundo [3], uma sessão TCP-IP é definida por qualquer seqüência de pacotes que caracterize a troca de informações entre dois endereços IP, e que tenha inicio, meio e fim (mesmo que toda a comunicação esteja contida em um único pacote).

Análises preliminares realizadas a partir de amostras da população do tráfego da Rede de Produção e as pesquisas conduzidas sobre o assunto [8,17] ajudaram no entendimento e identificação de atributos que são relevantes e que devem pertencer a um subconjunto de dados, ainda de grande volume, a ser explorado. Destas primeiras análises também foram revelados os serviços mais explorados na Rede de Produção em determinado dia, da semana e do mês.

Ainda como parte da pesquisa, a Rede de Testes tem sido utilizada para as análises comparativas entre o tráfego normal da rede quando acessados determinados serviços e as perturbações provocadas quando estes serviços são atacados (tráfego comprometido). Com isto, a compreensão dos atributos de rede que são influenciados ou modificados pela ocorrência de ataques ou ameaças, e que, conseqüentemente, afetam o comportamento normal da rede, é amadurecida.

O RECON está sendo utilizado para obter informações de cabeçalhos dos pacotes e, a partir destas informações, reconstruir e inferir sobre o estado das sessões TCP/IP contidas no tráfego de rede analisado. Esta aplicação utiliza a biblioteca *libpcap* para capturar dados do cabeçalho dos pacotes TCP, UDP e ICMP (em nível de Transporte), IP (em nível de Rede) e Ethernet (em nível de Enlace).

A idéia para mapeamento normal do comportamento de qualquer que seja a rede TCP/IP é definir os atributos relevantes e extraí-los (seleção de atributos) do conjunto de dados de sessões TCP e UDP filtrados e estruturados pelo RECON, os quais descrevem a utilização dos serviços e recursos da Rede de Produção. Em seguida, estes dados serão armazenados em bases de dados, por exemplo MySQL, que, embora grandes, terão menor volume que a do tráfego original carregada de atributos desnecessários para análise de anomalias. Com um conjunto reduzido de dados úteis, pode-se mapear o comportamento da rede, através de instâncias do tráfego de rede característico, em menor tempo e eficientemente.

4. Conclusões

Através dos gráficos preliminares gerados até o momento, observou-se os serviços de rede que são mais freqüentemente utilizados na Rede de Produção monitorada.

Os atributos relevantes necessários para a modelagem do perfil normal da rede podem ser classificados como atributos primitivos e atributos derivados. Dentre os atributos primitivos destacam-se: endereço IP de origem e de destino, portas de origem e de destino, tipo de protocolo, duração da sessão, total de

bytes por pacote e total de pacotes. Alguns exemplos de atributos derivados são: número de pacotes fluindo de uma determinada origem para um destino, número de pacotes e quantidade de bytes fluindo de um determinado destino para uma origem, número de conexões para IP de destino único dentro da rede nos últimos T segundos provenientes da mesma origem, número de conexões para IP de destino único dentro da rede nas últimas N conexões, partindo da mesma origem.

Com os atributos extraídos do RECON pode-se construir gráficos representativos do comportamento normal da rede, com base em análise estatística de freqüência média de acessos a serviços e recursos (perfil normal de uso dos serviços). A comparação de gráficos de diferentes dias poderá inferir sobre o comportamento da rede em uma semana, por exemplo, e análises de gráficos semanais podem inferir sobre o comportamento da rede em um mês.

Uma fotografia do tráfego em determinado instante pode então ser comparada ao comportamento normal médio da rede modelado e, a apresentação de algum desvio significativo do padrão modelado, poderá indicar a presença de um ataque conhecido ou de um novo ataque que deverá ser sinalizado pelo sistema e cujo traço malicioso deverá ser posteriormente confirmado pelo analista de rede.

Alguns tipos de ataques podem ser observados pela avaliação de informações localizados em campos do cabeçalho dos pacotes, enquanto outras, a partir dos dados de carga útil (*payload*) do pacote. Porém, certos campos do cabeçalho são utilizados pelos atacantes de forma diferente do especificado nas RFCs, para burlar os sistemas de detecção. Neste caso, deve-se considerar a análise de cabeçalho dos pacotes e parte do conteúdo do *payload* para identificação de determinados tipos de ataques.

Dentre os próximos desafios a serem enfrentados destacam-se:

- Selecionar atributos e armazenar grande conjunto de dados para representação do perfil normal da rede;
- Mapear situações em que deve-se considerar parte do payload para identificar ataques;
- Modelar entradas para as redes neurais para treinamento da rede e classificação de eventos de rede;
- Utilizar diferentes abordagens de *dataming* para determinar técnica mais promissora para condução das pesquisas;
- Testar o desempenho e precisão do sistema;
- Reduzir a taxa de falsos-positivos e negativos do sistema.

Finalizando este artigo, apresentam-se alguns comentários sobre sistemas de detecção por anomalia. Sistemas deste tipo permitem a construção de modelos a partir de dados normais e detectam desvios do modelo normal nos dados observados. Uma grande vantagem do sistema é a capacidade de detectar novos tipos de intrusões como desvios do comportamento normal. Dado um conjunto de dados normais para treinamento e dado uma nova porção de dados de teste, o objetivo do algoritmo de detecção de intrusão é determinar se os dados de teste pertencem a um comportamento "normal" ou "anômalo". Entretanto, modelos de detecção por anomalia estão sujeitos a uma alta taxa de alarmes falsos (falsos-positivos). Isto ocorre, principalmente, porque comportamentos do sistema previamente não observados, ainda que legítimos, podem também ser reconhecidos como anomalias, e, conseqüentemente, sinalizados como intrusões potenciais. Estes problemas devem ser considerados no desenvolvimento do sistema ANIS.

6. Referências

[1] Ambwani, T., "Multi Class Support Vector Machine Implementation to Intrusion Detection", Proceedings of The International Joint Conference on Neural Networks, 2003, 3, 2300-2305.

[2] Caswell, B.; Beale, J.; Foster, J.C.; Posluns, J., *Snort 2 – Sistema de Detecção de Intruso*, Ed. Alta Books, Rio de Janeiro, 2003.

[3] Chaves, M.H.P.C., "Análise de Estado de Tráfego de Redes TCP/IP para Aplicação em Detecção de Intrusão", São Jose Dos Campos, INPE, 2002.

[4] Dhanjani, N., *Hack Notes – Linux and Unix Security Portable Reference*, Rio de Janeiro, Ed. Elsevier, 2003.

[5] Dokas, P.; Ertoz, L.; Kumar, V.; Lazarevic, A.; Srivastava, J.; Tan, P.; Ozgur, A. – Cyber Threat Analysis – A key enabling Technology for The Objective Force (A Case Study in Network Intrusion Detection), dezembro, 2002.

[6] Dokas, P.; Ertoz, L.; Kumar, V.; Lazarevic, A.; Srivastava, J.; Tan, P. "Data Mining for Network Intrusion Detection", Tutorial at the Pacific-Asia Conference on Knowledge Discovery in Databases, Seoul, 2003.

[7] Ertoz, L.; Eilertson, E.; Lazarevic, A.; Tan, P.; Dokas, P.; Srivastava, J.; Kumar, V., "Detection and Summarization of Novel Network Attacks Using Data Mining", disponível em: http://www.cs.umn.edu/ research/minds/papers/raid03.pdf, acesso em: jul 2004.

[8] Lazarevic, A.; Ertoz, L.; Ozgur, A; Srivastava, J.; Kumar, V., "A Comparative Study Of Anomaly Detection Schemes In Network Intrusion Detection", Proceedings of Third SIAM Conference on Data Mining, San Francisco, May 2003.

[9] Melo, S.,*Exploração de Vulnerabilidades em Redes TCP-IP*, Ed. Alta Books, Rio de Janeiro, 2004.

[10] Mukkamala, S.; Janowski, G.; Sung, A. H., "Intrusion Detection Using Neural Networks and Support Vector Machines", Proceedings of the International Joint Conference on Neural Networks, 2002, 2, 1702-1707.

[11] Northcutt, S.; Novak, J. *Network Intrusion Detection* – Ed. New Riders Publishing, 2003.

[12] Petrovskiy, M. A., "Fuzzy Kernel-Based Method for Real-Time Network Intrusion Detection, Innovative Internet Community Systems", Lecture Notes in Computer Science, 2003, 2877, 189-200.

[13] Ramaswamy, S.; Rastogi, R.; Shim, K., "Efficient Algorithms For Mining Outliers From Large Data Sets", Proceedings of the ACM Sigmod Conference, 2000.

[14] Silva, L. S.; Santos, A. C. F.; Silva, J. D. S; Montes A., "A Neural Network Application for Attack Detection in Computer Networks", International Joint Conference on Neural Networks, Budapeste , Hungria, 2004.

[15] Silva, L. S.; Montes A.; Silva, J. D. S, "Uma solução Híbrida para Detecção de Anomalias em Redes", Anais do IV Workshop de Computação Aplicada , INPE São José dos Campos, 2004.

[16] Silva, L. S.; Santos, A. C. F.; Silva, J. D. S; Montes A., "ANNIDA: Artificial Neural Network for Intrusion Detection Application – Aplicação da Hamming Net para Detecção por Assinatura", VII Congresso Brasileiro de Redes Neurais, Natal, 2005.

[17] Stevens, W.R.; *TCP-IP Illustrated Volume 1: The Protocols*, Ed. Addison-Wesley, 2001.

[18] Sung, A.H.; Mukkamala, S. "A Comparative Study of Techniques for Intrusion Detection", Proceedings of the International Conference on Tools with Artificial Intelligence, 2003, 570-577.

[19] Zhang, Z.; Li, J.; Manikopoulos, C.N.; Jorgenson, J.; Ucles, J. "Hide: A Hierarchical Network Intrusion Detection System Using Statistical Preprocessing ad Neural Network Classification", Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 2001, 5-6 June.