ESTUDO DO USO DA *HAMMING NET* PARA DETECÇÃO DE INTRUSÃO

Lília de Sá Silva
Divisão de Desenvolvimento de Sistemas Solo
Instituto Nacional de Pesquisas Espaciais
São José dos Campos - SP
lilia@dss.inpe.br

Adriana C. Ferrari dos Santos
Laboratório de Computação Aplicada
Instituto Nacional de Pesquisas Espaciais
São José dos Campos - SP
adriana.ferrari@lac.inpe.br

Antonio Montes
Centro de Pesquisas Renato Archer - CenPRA
Campinas - SP
Antonio.montes@cenpra.gov.br

José Demísio da Silva Simões
Laboratório de Computação Aplicada
Instituto Nacional de Pesquisas Espaciais
São José dos Campos - SP
demisio@lac.inpe.br

RESUMO

Neste artigo é descrita a evolução de uma pesquisa baseada no uso da rede neural Hamming Net para o reconhecimento de padrões maliciosos em conjuntos de dados contendo assinaturas de ataques. São apresentadas as características da aplicação ANNIDA – Artificial Neural Network for Intrusion Detection Application, o progresso no desenvolvimento desta ferramenta e os resultados obtidos até o momento. Compreende também o relato de novas abordagens e informações de interesse que estão sendo exploradas para a melhoria da aplicação, em busca de resultados mais precisos.

ABSTRACT

This paper prescribes the evolution of a research based on the use of the neural network Hamming Net to recognize malicious patterns in a dataset containing attack signatures. Characteristics of ANNIDA - Artificial Neural Network for Intrusion Detection Application are presented, as well the application progress and test results. Also, new approaches and interesting information in study to improve the accuracy of ANNIDA are related.

1 INTRODUÇÃO

Quanto mais conhecimento se tem sobre análise de pacotes de rede e de sessões do tráfego, maior é a chance de se encontrar alguma informação maliciosa que caracterize um ataque conhecido ou que indique uma ameaça à rede. Na prática, o conjunto de dados do tráfego de rede a ser analisado é tão grande e diversificado, que faz-se necessário o uso de ferramentas de detecção de intrusão para realizar a identificação automática de dados ilegítimos ou anormais que trafegam pela rede.

Dentre as técnicas de detecção de intrusão existentes encontra-se o método baseado em assinaturas, o qual tem sido empregado nesta pesquisa. Além de métodos baseados em regras (Han et al., 2003), árvores de decisão (Kruegel, 2003), métodos de Markov e estatísticos, técnicas alternativas baseadas em inteligência artificial, incluindo redes neurais (Oz, 2005; Lee et al., 2001; Zhang et al., 2003; Cannady, 2001; Silva et al., 2004), têm sido utilizadas para melhorar a qualidade da análise do tráfego por assinatura.

Modelos baseados em redes neurais exploram simultaneamente várias hipóteses, ao invés de processarem instruções em seqüência. Para isto, fazem uso de vários elementos computacionais, denominados neurônios artificiais, que são interconectados através de pesos sinápticos. Considera-se, portanto, que o processamento paralelo possa prover economia de tempo na observação do tráfego capturado.

A motivação inicial deste trabalho surgiu em 2004 (Silva et al., 2004), com o estudo da possibilidade de aplicar a rede neural Hamming *Net* para classificar informações ilegítimas no tráfego de rede, sabendo-se que esta provê rápida classificação de dados, conforme descrito em (Fausset, 1994). Além de não precisar ser treinada de forma exaustiva, a *Hamming Net* requer menos conexões que outras redes classificadoras.

Basicamente, a finalidade da *Hamming Net* consiste em identificar a classe à qual uma dada entrada pertence, tomando como referência um conjunto de padrões previamente introduzidos na rede, denominados "exemplares". Em cooperação com a rede neural MAXNET (Fausset, 1994), a *Hamming Net* encontra o valor no conjunto de exemplares mais próximo de uma entrada a ser classificada.

Uma consideração importante ao usar a *Hamming Net* para detectar intrusões é que esta rede produz casamentos aproximados entre conjunto de dados de entrada e padrão de ataque (assinatura), ou seja, sempre retorna um valor aproximado, que, interpretado pelo observador humano, pode ser classificado como uma variação de um ataque ou traço de novo ataque.

Na próxima Seção, são apresentadas as características da aplicação de detecção de intrusão em desenvolvimento. O estudo de uso da rede neural *Hamming Net* para a melhoria desta aplicação, bem como os resultados obtidos até o momento são encontrados na Seção 3. Na Seção 4 são apresentadas as vantagens, limitações e os

estudos em andamento utilizando a *Hamming Net* para a melhoria da aplicação.

2 CARACTERÍSTICAS DA APLICAÇÃO

A aplicação ANNIDA - *Artificial Neural Network for Intrusion Detection Application* - foi implementada utilizando-se técnicas de programação convencional e orientada a objetos em C++ e consiste de dois módulos: o módulo PDE (Preparação dos Dados Exemplares) e o módulo CHN (Classificação *Hamming Net*). Através do módulo PDE são processados os arquivos de assinaturas do *Snort* (Snort, 2005) e, a partir destes, são gerados os padrões de ataque utilizados nesta aplicação. Os padrões de ataque correspondem a *strings* "*content*" do *Snort* e estes são organizados em conjuntos de dados.

No módulo CHN é utilizada a rede neural *Hamming Net* para a classificação dos dados. Com o módulo CHN são determinados os pesos da rede neural, calculados a partir do conjunto de dados de padrões de ataque (vetor de exemplares) gerado no módulo PDE, e, em seguida, é calculada a medida de similaridade (distância de *Hamming*) entre o vetor de entrada (entrada) de 14-bits apresentado à rede (fluxo de *strings* a ser classificado) e cada elemento do vetor de exemplares (exemplar), também de 14-bits, armazenado na rede (*strings* maliciosas conhecidas). A distância de *Hamming* (Fausset, L., 2004) entre a entrada e o exemplar corresponde à diferença obtida da comparação bit-a-bit entre eles, ou seja, é a quantidade de bits correspondentes que se diferem em ambos os elementos. Quanto menor a diferença de bits correspondentes (distância de Hamming), mais semelhante ao exemplar corrente é a entrada analisada. Com esta informação ocorre a classificação com o seguinte critério: 100% de semelhança significa que foi detectada uma string conhecida de ataque. A este critério pode ser atribuído um grau de tolerância, por exemplo, se ocorre 99% de semelhança entre a entrada e um exemplar, a entrada pode representar um traço ou variação de um ataque.

3 EVOLUÇÃO NO USO DA *HAMMING NET*

A seguir são descritos os estudos realizados desde o ano passado de aplicação da *Hamming Net* para o desenvolvimento da ferramenta de detecção baseada em assinaturas - ANNIDA.

3.1 Etapa Inicial

A primeira etapa deste trabalho (Silva et al., 2004) envolveu o estudo e a implementação da *Hamming Net* e testes com a rede, com a observação de seus resultados.

Em seguida, os dados foram preparados para serem introduzidos na aplicação da *Hamming Net*. Estes dados compreendem dados de carga útil de pacotes de rede dispostos em meio a informações ruidosas e assinaturas extraídas do *Snort*.

Nesta aplicação ainda hoje são utilizados a*rrays* de caracteres de 72 posições para armazenar os dados da rede (*stream* de *strings* para classificação e *strings* exemplares), os quais são reduzidos a um número de 4 dígitos via método *Hashing* e convertidos para um numero de 14 bits em representação bipolar. A técnica de redução dos dados do tipo string para um número bipolar de valor único permite a entrada de *strings* de qualquer tamanho na aplicação e o processamento destas na *Hamming Net*.

Na preparação dos dados exemplares para a *Hamming net* são consideradas as assinaturas (*strings contents*) contidas nos arquivos de regras do Snort. Apenas uma opção "*content*" de cada assinatura da base de assinaturas do *Snort* foi considerado neste trabalho. Os dados exemplares também são introduzidos na *Hamming Net* após convertidos para formato bipolar.

A saída da rede neural corresponde ao padrão de ataque do vetor exemplar que mais se assemelha ao fluxo de *strings* apresentado à rede.

A *Hamming Net* sempre realiza um casamento entre o conjunto de entrada e um padrão do conjunto de exemplares previamente apresentado à rede. E, através da definição de um limiar, pode-se estabelecer o grau de semelhança desejado na busca. Desta forma, pode-se descartar casamentos de baixa similaridade e considerar casamentos próximos. Com isto, é possível identificar não somente *strings* maliciosas já conhecidas, como *strings* cuja similaridade é bem próxima das conhecidas.

Neste primeiro estágio de uso da *Hamming Net*, a aplicação apresentou uma boa precisão (70% de casamento correto entre dados de entrada e dados exemplares), e constatou-se a viabilidade de uso desta rede neural para se detectar *strings* maliciosas em um conjunto de dados exemplares com aproximadamente 1000 assinaturas de ataques.

Um grande desafio superado nesta etapa foi a correta modelagem e tratamento dos dados para inserção e processamento na rede neural.

3.2 Expansão de Uso da Hamming Net

O uso da *Hamming Net* foi expandido (Silva 2005) de modo a se buscar novas informações de ataque. O aprimoramento deste trabalho consistiu da realização de uma nova modelagem dos dados de entrada e a alteração no código da aplicação para processamento da *Hamming Net* em vários níveis com o objetivo de introduzir na aplicação uma combinação de múltiplas *strings* maliciosas representativas de um único ataque.

Nesta etapa da pesquisa a aplicação recebeu o nome ANNIDA (Silva et al., 2005) e foi projetada

para identificar mais de uma *string* maliciosa de um ataque. Para isto, foram utilizadas as assinaturas *Snort* constituídas de mais de uma opção "*content*", além daquelas com apenas uma opção "*content*". A Figura 1 ilustra um exemplo de pesquisa de duas *strings* (múltiplos *contents*) em um *payload* de pacote, por exemplo as duplas "SITE" e "CHMOD" ou "SITE" e "Cl3A5Cl", cada dupla representando uma assinatura de ataque. Um conjunto de assinaturas formadas por *strings* "*content*" dispostas em arquivos diferentes é percorrido, coluna por coluna, e o procedimento de busca de *strings* ilegítimas ocorre até que não existam mais associações em uma determinada linha investigada.

A classificação final é obtida como a combinação de todos os conteúdos associados que foram sinalizados nos estágios anteriores. No exemplo apresentado na Figura 1, é ilustrada a saída da aplicação que corresponde, neste caso, a uma dupla de *strings* "SITE" e "Cl3A5Cl" que, encontradas no *payload* do pacote, representam um ataque. Além de apresentar as múltiplas *strings* maliciosas, a aplicação retorna a posição em que esta combinação de "*contents"* (assinatura) se encontra no fluxo de *strings* analisado.

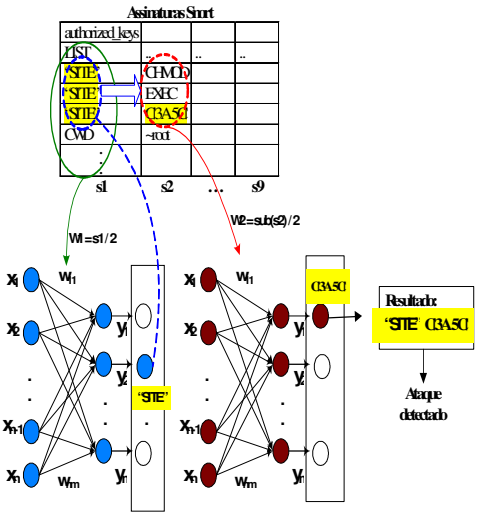

Figura 1 –Um Exemplo do Uso Expandido da *Hamming Net*

O principal desafio deste projeto foi estabelecer uma metodologia para tratamento dos dados de entrada para a rede neural, tal que várias *strings* associadas fossem manipuladas e tivessem sua dependência preservada quando pesquisando um padrão de ataque.

Presume-se que a pré-filtragem de dados correspondentes antes da apresentação destes à *Hamming Net* possa ter reduzido o tempo de processamento da aplicação.

Os resultados obtidos nesta fase foram satisfatórios, principalmente na observação de assinaturas compostas por até 2 níveis de *strings* associadas que resultou, em média, 90% de classificação correta, considerando o número máximo de 500 entradas apresentadas à rede. Para a busca de nível maior, ou seja, por exemplo, a pesquisa da combinação máxima de 6 *strings* de assinaturas em um conjunto de 500 entradas, o resultado médio obtido foi de 70% de classificação correta. Para um conjunto de 227 exemplares e 3 *strings* associadas ocorreu uma classificação à taxa de 70% também.

4 CONCLUSÃO

Os estudos realizados até o momento apresentam resultados satisfatórios na busca de informações maliciosas em conjuntos de dados, através do uso da *Hamming Net* e assinaturas, e apontam a possibilidade de aplicação de outras redes neurais conjugadas a esta para uma melhor classificação dos dados.

As seguintes vantagens são apresentadas pela ferramenta ANNIDA:

- Independentemente do tamanho do fluxo de *string* a ser analisado, a aplicação converte a entrada em um número único de 14 bits em formato bipolar para ser processado, resolvendo o problema de classificação de fluxos de string de tamanho variável;
- Devido às características da rede neural utilizada e a flexibilidade na determinação do grau de similaridade entre a string de ataque conhecida (exemplar) e a string analisada (entrada), é possível configurar a aplicação para detectar, além de ataques conhecidos, informações de tentativas de ataques ou de novos ataques e realimentar a base de assinaturas com estas informações;
- Existe a possibilidade de ser usada para a rápida classificação de um grande volume de dados.

Neste trabalho, subconjuntos da base de assinaturas do *Snort* foram utilizados para construir os conjuntos de exemplares da *Hamming Net* processados para a classificação de *strings* de entrada. Entretanto, estudos mais aprofundados podem inferir sobre a possibilidade de conjugação da *Hamming Net* ao *Snort* para acelerar a busca de strings maliciosas e prover a detecção de *strings* bem similares às assinaturas em conteúdos de pacotes.

A ferramenta de detecção em desenvolvimento possui limitações que podem ser reduzidas ou abolidas a partir das seguintes ações:

- Capacitar a aplicação a receber um conjunto maior de dados exemplares (padrões de ataque) para a rede neural

(acima de 1000 assinaturas). Para isto, o código deverá ser reescrito utilizando-se apontadores e estruturas de dados do tipo lista dinâmica, em substituição às matrizes atualmente utilizadas para a manipulação dos dados.

- Capacitar a aplicação para produzir resultados mais precisos, principalmente quando for introduzido um conjunto maior de padrões de ataque e prover estatística do número total de falso-positivos encontrados nestes casos;
- Estudar a possibilidade de utilização de outras opções relevantes contidas nas regras do *Snort* para melhorar a qualidade do processo de busca. Um novo desafio é a compreensão de outros parâmetros envolvidos na semântica das regras *Snort*, tais como as opções "*depth*" e "*offset*" que são utilizadas em conjunto com a opção "*content"*.

Em um estágio de desenvolvimento mais avançado, após realizadas as atualizações anteriormente descritas, será possível medir o desempenho da aplicação e avaliá-la em relação a outras aplicações existentes de detecção de intrusão por assinatura.

A pesquisa mais recente com o ANNIDA envolve a aplicação da rede neural *Multi-Layer Perceptron* para a classificação de ataques ocorridos.

REFERÊNCIAS BIBLIOGRÁFICAS

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 in Neural Networks (IJCNN2004), Budapeste, Hungria, 2004.

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, trabalho aceito para apresentação no VII Congresso Brasileiro de Redes Neurais (CBRN2005), Natal, Rio Grande do Norte, Brasil, Oct, 2005.

LEE, S.C.; HEINBUCH, D.V., Training a neural-network based intrusion detector to recognize novel attacks Systems, Man and Cybernetics, Part A, IEEE Transactions on Volume 31, Issue 4, Jul 2001, Page(s):294 – 299.

OZ, C., Signature recognition and verification with artificial neural network using moment invariant method, Lecture Notes In Computer Science, 3497: 195-202, 2005.

ZHANG C.L., JIANG J., KAMEL M., Intrusion detection using hierarchical neural networks, Source: Pattern Recognition Letters 26 (6): 779-791, May 2005.

HAN S.J., CHO S. B., Detecting intrusion with rule-based integration of multiple models, Computers & Security 22 (7): 613-623, 2003.

CANNADY J, GARCIA R.C., The application of fuzzy ARTMAP in the detection of computer network attacks, **S**ource**:** Artificial Neural Networks-Icann 2001, Proceedings Lecture Notes In Computer Science 2130: 225-230, 2001.

KRUEGEL C., TOTH T., Using decision trees to improve signature-based intrusion detection, Lecture Notes In Computer Science 2820: 173-191, 2003.

SNORT - http://www.snort.org/, página acessada em 2005.

FAUSSET, L. Fundamentals of Neural Networks: architectures, algorithms, and applications, New York: Prentice Hall, 1994. ISBN 0-13-334186-0.