Uma Proposta de Utilização da Transformada de Wavelet e Redes Neurais para Detecção de Ataques em Redes Ad Hoc Sem Fio

Ed' Wilson Tavares Ferreira[1], Ruy de Oliveira[1], Gilberto Arantes Carrijo[2], Nelcileno Virgílio de Souza Araújo[3]

[1]Departamento de Informática – Centro Federal de Educação Tecnológica de Mato Grosso (CEFETMT)
Rua Zulmira Canavarros, 95 - Centro– 78.005-390 – Cuiabá – MT - Brasil

[2]Faculdade de Engenharia Elétrica – Universidade Federal de Uberlândia (UFU)
Uberlândia – MG - Brasil

[3]Departamento de Ciência da Computação - Universidade Federal de Mato Grosso (UFMT) – Cuiabá – MT - Brasil

{edwilson,roliveira}@inf.cefetmt.br, gilberto@ufu.br, nelcileno@yahoo.com.br

1. Introdução

Uma rede ad hoc sem fio pode ser formada em situações quando computadores necessitam de comunicação, enquanto uma infra-estrutura fixa não é disponível ou não se deseja utilizá-la. Neste caso, os nós formam uma rede para uso temporário com o objetivo de suprir as necessidades de comunicação naquele momento.

As redes ad hoc sem fio são muito vulneráveis a ataques de usuários mal intencionados devido, sobretudo, à necessidade de cooperação entre os nós que a compõem. Sempre que uma rede ad hoc se encontra sob ataque, alguma anomalia é esperada na caracaterística de seu tráfego. A principal vantagem da análise de anomalias é a possibilidade que ela garante de se identificar mesmo os ataques que não tenham sido descobertos previamente. Este trabalho apresenta uma proposta de uso das transformadas de wavelets para detecção de anomalias com classificação dos ataques através de redes neurais artificiais.

A transformada de Wavelet é uma técnica matemática com capacidade de realizar a decomposição de funções. Usando-se Wavelet, como ferramenta de análise de sinais, pode-se avaliar o comportamento da rede ad hoc em janelas de tempo, e assim identificar anomalias tais como variações abruptas no tráfego da rede. Wavelets têm sido usadas eficientemente para Detecção de Intrusos em redes cabeadas [Hamdi and Boudriga 2007]. E as Redes Neurais Artificiais possuem funcionamento similar ao cérebro humano e, por isso, são usadas no reconhecimento de padrões. Essas redes possuem capacidade de aprendizado e podem realizar generalizações, de acordo com o conhecimento acumulado. Assim, as Redes Neurais Artificias representam uma abordagem promissora para os Sistemas de Detecção de Intrusos [Hu and Maybank 2008].

2. Uma Proposta de Utilização da Transformada de Wavelet para Detectar Comportamentos Anômalos em Redes Ad Hoc Sem Fio e Redes Neurais Artificiais para Classificação dos Ataques

O emprego de Wavelets para a detecção de anomalias requer o uso de uma função (ou conjunto de dados) que represente o comportamento da rede de forma mais realística possível. Além disso, as métricas utilizadas para identificação do comportamento da rede devem ser escolhidas mediante dois fatores importantes: facilidade de uso e independencia dos sistemas operacionais em cada nó da rede. Exemplos de métricas incluem: Banda Disponível ou utilizada, Número de Conexões ou Fluxos Ativos; Número de Pacotes Transmitidos ou Recebidos, entre outros.

Em nossa avaliação preliminar, foram realizadas simulações, utilizando o software NCTUns, de uma rede com 5 (cinco) nós. Um ataque DoS foi representado por transferências, com elevada taxa de transmissão, baseada no protocolo UDP, e a métrica utilizada para análise foi o número de pacotes descartados nas interfaces dos nós. Para a Wavelet, utilizou-se a função Daubenchies, e o a resultado foi promissor. O algoritmo simulado detectou a mudança abrupta no comportamento da rede, com a indicação exata do período de ataque. Outros experimentos foram realizados em "testbed", através de 2 notebooks e 1 PDA. Neste cenário, foram executados ataques do tipo TCP RPC [Pajwani et al 2006], que também foram identificados após a utilização da Wavelet.

Em seguida, uma rede neural contendo 13 neurônios de entrada, 4 na camada oculta, e 1 na camada de saída, previamente treinada para detectar ataque TCP RPC, conseguiu identificar o período exato da ofensiva.

3. Conclusões Parciais e Proposta de Trabalhos

A proposta deste trabalho demonstrou que é possível utilizar transformadas de wavelet para detectar anomalias na rede. As utilizações em conjunto com as Redes Neurais Artificiais podem realizar então a classificação dos ataques. Os resultados iniciais são promissores.

Como continuidade desta pesquisa, pretende-se integrar as duas soluções, reduzindo ao máximo o custo computacional da solução integrada. Isso é fundamental para as redes ad hoc porque os nós dessas redes são alimentados por baterias. Também planeja-se treinar a rede neural para identificar outros ataques. Será realizada a comparação com outras propostas, e também a análise para identificar o percentual de falsos positivos e falsos negativos.

Referências

Hamdi, M., Boudriga, N. (2007) "Detecting Denial-of-Service attacks using the wavelet transform", Comput. Commun, vol.30, no. 16, pp 3203-3213.

Hu W., Maybank, S. (2008) "AdaBoost-Based Algorithm for Network Intrusion Detection", Systems, Man and Cybernetics, IEEE Transactions, vol 38, n.2, pp 577.

Pajwani, S., et al. (2005),"An Experimental Evaluation to Determine if Port Scan are Precursors to an Attack", dsn, pp.602-611, 2005. International Conference on Dependable Systems on Networks (DNS'05).