Detecção de Intrusões baseada em Séries Temporais[1]

Bruno Lopes Dalmazo, Francisco Vogt, Tiago Perlin, Raul Ceretta Nunes

Programa de Pós-Graduação em Informática - Universidade Federal de Santa Maria
Centro de Tecnologia. Campus UFSM – 97105-900 – Santa Maria – RS – Brasil
{falabruno, fcvogt, tiagoperlin}@gmail.com, ceretta@inf.ufsm.br

Sistemas de Detecção de Intrusão (SDI) [Northcutt, Novak e Mclachlan 2001] são utilizados para detectar ataques e uso malicioso ou inadequado da rede, sendo constituídos de três componentes fundamentais: *fonte de informação*, *análise* e *resposta*. A *fonte de informação* costuma ser um coletor associado a um host, rede ou segmento de rede. A *análise* é a parte do SDI que verifica os eventos derivados da fonte de informações, determinando quando estes eventos indicam que uma intrusão está ocorrendo ou já ocorreu. A *resposta* é o conjunto de ações que o SDI realiza quando detecta uma intrusão, por exemplo, a intervenção automatizada ou a geração de alertas e relatórios para a interpretação e intervenção humana. O principal desafio do desenvolvimento de um IDS é escolher um método eficiente que identifique uma intrusão de maneira correta, sem gerar um número excessivo de falsas detecções.

O presente trabalho propõe a utilização da teoria de séries temporais [Bowerman e O´Connel 1993] na fase de *análise* de um SDI com o objetivo de identificar com maior confiança uma intrusão e diminuir o número de *falsos positivos*. Uma série temporal é um modelo matemático para representar amostragens periódicas que apresentam dependência entre as amostras [Bowerman e O´Connel 1993]. Esta abordagem já foi explorada na Computação na predição de desempenho [Schulz, Hochberger e Tavangaria 2001] e na análise de atrasos de rede [Nunes e Jansch-Pôrto 2003].

Como *fonte de informação* está sendo utilizado os dados coletados pelo Sistema de Análise da Internet (IAS) baseado em *probe* do IFIS/FHGe (Fachhochschule Gelsenkirchen) [Pohlmann e Proest 2006]. Os *probes* do IAS passivamente acessam o tráfego de rede coletando informações e armazenando em um banco de dados. Como o IAS armazena e reinicializa seus contadores periodicamente, pode-se modelar a amostragem de contadores de pacotes de rede como séries temporais.

Atualmente o *sistema de avaliação* do IAS, em fase de desenvolvimento ainda, realiza a *análise* baseada em redes neurais. Entretanto, pode-se fazer uso de séries temporais para a detecção de intrusões, como visto por [Nunes e Jansch-Pôrto 2003] no contexto predição de tempos de comunicação. Com este objetivo, desenvolveu-se o programa DIBSeT (Detector de Intrusões Baseado em Séries Temporais) [Lunardi 2008].

O DIBSeT realiza previsões de acordo com o modelo ARIMA (*Autoregressive Integrated Moving Average*), um modelo de série temporal que possibilita tratar séries estacionárias ou não. Para sobrepor variações consideradas normais, o resultado da previsão é somado a uma margem de segurança baseada no erro quadrático médio. Esta margem tem o papel de um *threshold* adaptativo, o que possibilita uma análise que se adapta ao histórico dos dados observados. A característica típica da modelagem e

[1] Trabalho apoiado pelo Convênio UFSM/INPE e pela FAPERGS (Proc. 07503726).

análise de dados por séries temporais, a de poder realizar previsões correlacionadas a comportamentos passados, aliada ao uso de *threshold* adaptativo é o fator explorado neste trabalho para reduzir o número de falsos positivos em detectores de intrusão baseados em anomalia do tráfego de rede. O estabelecimento de limites estáticos produz muitos *falsos positivos* neste ambiente. Como *anomalias* são indícios de ataques, a *resposta* do DIBSeT a uma *anomalia* é um *alarme*, classificado em cinco *níveis de alarme*, com o valor zero indicando a inexistência de anomalias. O uso níveis de alarmes possibilita um segundo estágio de análise antes da tomada de decisão, que pode ser manual ou automática. Como resultado preliminar, os testes realizados com o DIBSeT demonstraram que a utilização de séries temporais para a detecção de ataques (negação de serviço com ataque SYN e SMURF) apresenta resultados satisfatórios quanto a identificação de um ataque, além de consumir pouco tempo de processamento.

Do ponto de vista algorítmico, o uso de séries temporais exige uma fase de preenchimento da série, apenas no início da computação, seguida de um ajuste do modelo de previsão, o qual pode ser revisto sempre que o erro de predição começar a aumentar. O ajuste do modelo significa determinar quais os parâmetros do modelo ARIMA (número de termos autoregressivos e de médias móveis, e número de integrações necessárias para tornar a série estacionária). Realizado os ajustes, o preditor possibilita realizar previsões na ordem de nano segundos.

Atualmente estamos investigando o uso de *níveis de alarmes* como ferramenta para possibilitar a redução do número de falsos positivos, bem como a separação do fluxo de dados analisadas em vários fluxos, de acordo com as informações nos descritores dos pacotes. A exploração de níveis de alarme visa identificar a maior concentração de alarmes e correlacioná-los com os tipos de ataques. A separação dos fluxos de dados (por tipo de pacote, *host* e porta) visa explorar correlações entre comportamentos de dois ou mais fluxos, o que possibilita estudar a correlação espacial entre os alarmes gerados pelas diferentes séries temporais, melhorando a detecção de anomalias na rede e reduzindo o número de falsos positivos.

Referências

Bowerman, B. L. e O´Connel, R. T. (1993) “Forescasting and Time Series: an Applied Approach”, Belmont: Duxbury Press.

Lunardi, R. C. (2008) “Um Analisador de Intrusões baseado em Séries Temporais”, TG 255. Universidade Federal de Santa Maria, Santa Maria.

Northcutt, S., Novak, J. e Mclachlan, D. (2001) “Segurança e prevenção em redes”, São Paulo: Berkley.

Nunes, R. C. e Jansch-Pôrto, I. (2003) “A Lightweight Interface to Predict Communication Delays using Time Series”, In: First Latin-American Dependable Computing Symposium, São Paulo-Brazil.

Pohlmann, N. e Proest, M. (2006) “Internet Warning System: The Global View”, In: Information Security Solutions Europe 2006: Securing Electronic Busniess Process, Vieweg.

Schulz J., Hochberger C. e Tavangarian D. (2001) “Prediction of Communication Performance for Wide Area Computing Systems”, Proceedings of 9th Euromicro Workshop on Parallel and Distributed Processing, IEEE Computer Society, Mantova-Italy.