Detecção de DDoS Através da Análise da Recorrência Baseada na Extração de Características Dinâmicas

Marcelo Antonio Righi[1], Raul Ceretta Nunes[1]

[1]Programa de Pós-Graduação em Informática – CT – UFSM
Av. Roraima, 1000, B. Camobi – Santa Maria (RS) – Brasil

marcelo.righi@mail.ufsm.br, ceretta@inf.ufsm.br

Abstract. *With the increasing number of Distributed Denial of Service (DDoS) attacks, detect them has become essential to maintaining the reliability of institutions using the internet. In this sense, different algorithms have been used to analyze network traffic, such as neural networks, decision trees, principal component analysis and others. However, these algorithms do not use dynamic features to classify network traffic. This article proposes to use the Analysis Quantification of Recurrence based on the extraction of dynamic characteristics combined with the clustering algorithm A-Kmeans to perform traffic classification. The results confirm the accuracy of the model that reached minimal number of false alarms when tested with the CAIDA data set.*

1. Introdução

A detecção de intrusão baseada em anomalias de redes, que compara os dados coletados com registros de atividades consideradas normais no sistema [Tsai et al. 2009], vem sendo muito explorada atualmente devido aos inúmeros e persistentes Ataques Distribuídos de Negação de Serviço (DDoS), os quais utilizam até milhares de computadores para atacar uma determinada máquina, distribuindo a ação entre elas. A análise baseada em anomalia pode ser usada para alerta e prevenção de ataques que ainda não possuem uma assinatura, fornecendo também conhecimento para futuros estudos e definição de novos comportamentos anômalos. Entretanto, as técnicas existentes para detecção de ataques DDoS ainda possuem muitas limitações e a sua eficácia pode ser comprometida devido ao excesso de falsos alertas que são emitidos, como observado por [Ganame et al. 2008].

Embora o tráfego de rede demonstre a existência de comportamentos dinâmicos não lineares, dentre os quais a recorrência, não foram identificadas propostas que explorem, simultanemente, características dinâmicas e análise da quantificação da recorrência para classificação do tráfego de rede. A Análise da Quantificação da Recorrência (AQR) [Webber e Zbilut 1994] pode proporcionar um valoroso campo para pesquisa científica na área de Segurança Cibernética, pois analisa uma tendência que determina o comportamento do tráfego não linear que se repete ao longo de um determinado intervalo de tempo.

Levando-se em consideração a AQR, é possível extrair diversas características dinâmicas do comportamento específico para cada sistema, que são chamadas de medidas de quantificação da recorrência, tais como Taxa da Recorrência (REC), Determinismo (DET), Entropia (ENT), Tendência (TREND), Laminaridade (LAM) e outras. Essas características dinâmicas extraídas da AQR, tem grande vantagem sobre as extraídas diretamente da análise de séries temporais, por exemplo, pois a AQR diminui os falsos alarmes, tendo em vista que picos de elevação do tráfego momentâneos não são levados em consideração, a não ser que eles delimitem uma tendência e provoquem uma mudança considerável e acima dos limites dos valores das características dinâmicas normais obtidas durante a fase de treinamento.

A AQR vem sendo utilizada com sucesso para o reconhecimento de sinais de voz patológicos, conforme [Lopes et al. 2013] e [Vieira et al. 2012], onde são utilizadas amostras para aplicar a análise da recorrência, construção do gráfico da recorrência, e extração de diversas características dinâmicas que melhor se adequam ao tipo de sinal que está sendo verificado, usando ao final um classificador para determinar se é patológico ou não.

Um dos poucos trabalhos que empregam características dinâmicas para detectar anomalias no tráfego de rede, embora não analise sua recorrência, está caracterizado no modelo utilizado em [Yuan et al. 2014]. O autor combina o algoritmo K-Means (com número fixo de clusters) com a Transformada Wavelet (TW) e a AQR, porém a quantidade de falsos positivos ultrapassa 8% quando utiliza a base de dados DARPA 1999. Além disso, os dados estatísticos caracterizam apenas ataques DoS, enquanto a grande maioria dos ataques atuais ocorre de maneira distribuída (DDoS).

Este trabalho apresenta um método para detecção de DDoS que utiliza a AQR baseada na extração de características dinâmicas, com emprego da clusterização A-Kmeans, que calcula automaticamente o número de clusters, para classificar o tráfego de rede. Os resultados preliminares com a base CAIDA demonstraram eficiência do método.

2. Detalhamento da Solução

Visando diminuir a quantidade de alarmes falsos na detecção de DDoS, este trabalho explora a aplicação da Análise de Quantificação da Recorrência baseada na extração de características dinâmicas em uma série temporal não estacionária, em conjunto com a clusterização pelo algoritmo A-Kmeans, algoritmo onde o cálculo do número de clusters é feito automaticamente. O cálculo automático evita erros de acurácia do K-Means, no qual o número de clusters é determinado pelo pesquisador.

Para detecção de ataques DDoS, a aplicação da AQR exige a utilização de atributos que caracterizem as anomalias de interesse em uma série temporal. A identificação destes atributos foge ao escopo deste trabalho, tendo sido adotados os atributos identificados em [Oo et al. 2014], os quais usaram métodos estatísticos para testar e validar os atributos que permitem a caracterização de DDoS. De acordo com [Oo et al. 2014], os atributos que se adequam ao tipo de ataque DDoS são: Número de Pacotes (Num_Pac), Número de Bytes (Num_Bytes), Média do Tamanho dos Pacotes (M_Pac), Variância de Tempo dos Pacotes (Var_Tem_Pac), Variância de Tamanho dos Pacotes (Var_Tam_Pac), Taxa de Pacotes (Tax_Pac), Taxa de Bytes (Tax_Bytes).

Conhecidos os atributos, cada um é amostrado na forma de uma série temporal, em períodos equidistantes. Para adequação dos limites ou parâmetros que serão utilizados no Algoritmo A-Kmeans, na classificação do tráfego, em cada série temporal não estacionária, será aplicada a Análise da Quantificação da Recorrência. Inicialmente, para aferição do modelo, uma base de dados com tráfego normal (sem ataques) é utilizada.

A Equação da Recorrência, segundo [Vieira et al. 2012], é computada com base em uma série temporal $x = \{xi\}$, $i = 1, 2, ..., n$, onde o estado Xj da série representa o estado do tráfego e é expresso conforme Equação (1), sendo m a dimensão de imersão, τ o tempo de atraso e $N = n - (m-1)\,\tau$.

$$Xj = [xj, xj+\tau, xj+(m+1)\tau], j = 1,2,...,N \quad (1)$$

Depois de calcular os estados de tráfego, utiliza-se a Equação da Recorrência (2) para analisar os fenômenos de recorrência de cada um deles.

$$Rij = \theta(\varepsilon - \| Xi - Xj \|),\ j = 1,2...,N \quad (2)$$

Na Equação (2), Rij é um elemento da matriz de recorrência, ε é o limiar, Xi é um estado do sistema no espaço de fase m-dimensional, N é o número de estados e θ é a função definida pela Equação (3).

$$\theta(y) = \begin{cases} 0 & y \leq 0 \\ 1 & y \geq 0 \end{cases} \quad (3)$$

Se a distância entre os estados *Xi* e *Xj* é menor do que o limiar (ε), então o valor de *Rij* é 1 e existe um marcação "ponto preto" em (*i*, *j*) no Gráfico da Recorrência; caso contrário, o valor de *Rij* é 0 e existe uma marcação "ponto branco" em (*i*, *j*).

Na fase de extração de características dinâmicas, foram utilizadas a Razão da Recorrência (RR), a Entropia (ENT) e o Determinismo (DET), tal como [Vieira et al. 2012], sendo estas características testadas neste trabalho com enfoque em Ataques DDoS. Para poder avaliar qualquer série de tráfego, as texturas da estrutura (Gráfico da Recorrência) são quantificadas através do cálculo da RR, DET e ENT, como segue:

1) Razão de Recorrência (RR) **-** mede a densidade dos pontos de recorrência no Gráfico da Recorrência;

2) Determinismo (DET) **-** razão entre o número de pontos de recorrência que formam as estruturas diagonais e todos os pontos de recorrência. Está relacionado com a previsibilidade do sistema.

3) Entropia de Shannon (ENT) - representa a distribuição de frequências dos comprimentos das linhas diagonais e reflete a complexidade da estrutura determinística presente no sistema.

A última fase aplica o Algoritmo A-Kmeans, onde foi estabelecido que, se a maioria dos clusters existentes forem anômalos, o tráfego será classificado como Ataque DDoS.

3. Resultados Preliminares

Nos experimentos, o método proposto calcula as características dinâmicas do tráfego de rede (RR, ENT e DET) para cada série temporal referente à janela deslizante de 60 (sessenta segundos) cada uma. O fato do número de clusters do K-Means ser fixo, como visto em [Yuan et al. 2014], foi testado comparativamente com o algoritmo A-Kmeans (vide Tabela 1), que utiliza o cálculo automático do número de clusters.

Na fase de treinamento do modelo, foi utilizada a Base de Dados CAIDA 2008 [CAIDA 2008] para caracterizar o tráfego normal e a CAIDA 2007 [CAIDA 2007] para classificar o tráfego de Ataque DDoS. Ressalta-se que nos testes foram intercaladas linhas de tráfego de ataque com linhas de tráfego normais, da seguinte maneira:

- **CAIDA 2008** - Tráfego Normal – 3661 segundos (1 hora de tráfego);
- **CAIDA 2007** - Tráfego Ataque DDoS – 3955 segundos (1 hora de ataque);
- **CAIDA 2007/2008**- Tráfego Ataque/Normal- 7616 segundos (2 horas de trafego misto).

Os testes foram procedidos em quatro fases, sendo que a primeira utilizou a Base CAIDA 2008 para treinar o modelo, determinando os limitadores e os parâmetros a serem utilizados para a classificação de tráfego normal. A segunda fase utilizou a Base CAIDA 2007 (Ataque DDoS) para verificar se os ataques seriam detectados. A terceira fase mesclou tráfego normal com Ataque DDoS. Na quarta fase foram realizados testes com o modelo de [Yuan et al. 2014] com a base de dados CAIDA, pois o autor usou a DARPA 1999 para seus testes, a fim de permitir a comparação do modelo proposto com o de Yuan. Testes de desempenho ainda não foram realizados de maneira sistemática, porém observou-se baixo custo computacional para a utilização da AQR com base em características dinâmicas, quando combinada com o algoritmo A-Kmeans.

Conforme mostra a Tabela 1, os resultados demonstram melhor acurácia da solução proposta (95.38% contra 89.23%) e significativa redução nas taxas de falsos positivos (de 4.62% para 1.54%) e falsos negativos (de 10.77% para 4.62%). Observou-se também o forte impacto relacionado a troca do classificador K-Means pelo A-Kmeans (95.38% contra 83.08% na acurácia; 1.54% contra 13.54% nos falsos positivos;

4.62% contra 16.92% nos falsos negativos), demonstrando a potencialidade da combinação AQR+A-Kmeans.

ALGORITMO	RESULTADOS		
	Acurácia (%)	Falso Positivo (%)	Falso Negativo (%)
TW+AQR+K-Means	89.23	4.62	10.77
AQR+K-Means	83.08	13.54	16.92
K-Means	69.23	38.33	30.77
A-Kmeans	**75.35**	**12.31**	**24.75**
AQR+A-Kmeans	**95.38**	**1.54**	**4.62**

Tabela 1 - Taxas de acertos obtidas (CAIDA 2007/2008).

3. Considerações finais

A eficácia de métodos de detecção de DDoS baseados em análise de anomalias tem sido um desafio para projetistas de algoritmos de detecção. O uso de Análise da Quantificação da Recorrência, mesmo utilizada com sucesso em outras áreas, é pouco explorada no contexto de análise de anomalias no tráfego de rede. Este trabalho explorou sua aplicação na detecção de DDoS, avaliando-a conjuntamente com a extração de características dinâmicas e o classificador A-Kmeans, tendo verificado acurácia elevada quando comparada com o trabalho similar [Yuan et al. 2014]. Os resultados preliminares foram obtidos com as bases de dados CAIDA 2007 e 2008 e serão expandidos com o uso de outras bases em testes mais exaustivos que também devem incluir testes de desempenho. Testes de outros algoritmos juntos com a AQR e A-Kmeans, tais como a Transformada Wavelet também serão avaliados em trabalhos futuros.

4. Referências

Ganame AK, Bourgeois J, Bidou R, Spies F (2008). A global security architecture for intrusion detection on computer networks. Elsevier Comput Secur 27:30-47.

Lopes LW, Costa SLNC, Costa WCA, Correia SEN, Vieira VJD (2013). Análise da dinâmica não linear de vozes infantis: nova proposta de avaliação e monitoramento vocal. *In:* Pesquisas em Fonoaudiologia. Sociedade Brasileira de Fonoaudiologia.

Oo TT, Phyu T. (2014). "Analysis of DDoS Detection System based on Anomaly Detection System", International Conference on Advances in Engineering and Technology (ICAET'2014). Singapore.

The CAIDA "DDoS Attack 2007" Dataset - < Acesso em 15 maio 2015 11:12h > https://data.caida.org/datasets/security/ddos-20070804/

The CAIDA UCSD Anonymized Internet Traces 2008 - < Acesso em 05 maio 2015 11:12h > https://data.caida.org/datasets/passive-2008/

Tsai CF, Hsu YF, Lin CY e Lin WY. (2009). Intrusion detection by machine learning: A review. *Expert Systems with Applications*, v. 36, n. 10, p. 11994–12000.

Vieira VJD, Costa SC, Costa WCA. (2012). Análise de Quantificação de Recorrência e Análise Discriminante Aplicadas à Classificação de Sinais de Vozes Saudáveis e Sinais de Vozes Patológicas. In: Anais do VII CONNEPI©2012; ISBN 978-85-62830-10-5; Palmas-TO, Brasil.

Webber C L, Zbilut JP. (1994). Dynamical assessment of physiological systems and states using recurrence plots strategies. J. Appl. Physiol., 76:965-973.

Yuan J, Yuan R, Chen X (2014). Network Anomaly Detection based on Multi-scale Dynamic Characteristics of Traffic. INT J COMPUT COMMUN, ISSN 1841-9836, 9(1):101-112, February.

