Detecção de DDoS Através da Análise da Quantificação da Recorrência Baseada na Extração de Características Dinâmicas e Clusterização Adaptativa

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. *The high number of Distributed Denial of Service (DDoS) attacks have demanded innovative solutions to guarantee reliability and availability of internet services. In this sense, different methods have been used to analyze network traffic for denial of service attacks, such as neural networks, decision trees, principal component analysis and others. However, few of them explore dynamic features to classify network traffic. This article proposes a new method, called DDoSbyAQR,that uses the recurrence quantification analysis based on the extraction of dynamic characteristics and an adaptive clustering algorithm (A-kmeans) to perform better classification of the attack network traffic. The experiments were done using the CAIDA and UCLA databases and have demonstrated ability to increase the accuracy (98.41%) of DDoS detection.*

1. Introdução

Tradicionalmente, sistemas de detecção de intrusão (*Intrusion Detection System* – IDS) procuram por comportamentos maliciosos utilizando técnicas baseadas em assinaturas ou anomalias. A detecção por assinatura compara o tráfego de rede com uma base de dados de ataques previamente conhecidos (assinaturas), enquanto a detecção por anomalias compara os dados coletados com registros de atividades consideradas normais no sistema [Tsai et al. 2009].

A detecção de intrusão baseada em anomalias vem sendo muito explorada [Silva et al. 2012][Raut e Singh 2014] devido aos inúmeros e persistentes Ataques Distribuídos de Negação de Serviço (DDoS), os quais utilizam até milhares de computadores (pessoais ou servidores) para atacar uma determinada máquina, distribuindo a ação de ataque entre elas.

Para detecção de DDoS são utilizadas variadas técnicas [Raut e Singh 2014]. Entretanto, muitas ainda possuem limitações e a sua eficácia pode ser comprometida devido ao excesso de falsos alertas, como observado em [Raut and Singh 2014]. A existência de comportamentos dinâmicos não lineares e não estacionários na série de tráfego pode ser um dos fatores [Palmieri e Fiori 2010] para maior efetividade, dado que o tráfego de rede contém propriedades como auto-similaridade [Willinger et al. 1998], dependência de longo alcance [Grossglauser e Bolot 1999] e recorrência [Marwan e Webber 2015].

A Análise da Quantificação da Recorrência (AQR) [Webber e Marwan 2015], utilizada inicialmente com limitações em [Palmieri e Fiori 2010] [Kumar 2012] [Jeyanthi et al. 2014] e em outros domínios [Vieira et al. 2012], pode também proporcionar

soluções para segurança em redes de computadores de maneira mais eficaz e em tempo real [Righi e Nunes 2015], pois permite analisar o comportamento do tráfego não linear que se repete ao longo de um determinado intervalo de tempo e emitir alertas para reagir a um ataque DDoS.

Na AQR é possível extrair diversas características dinâmicas do comportamento específico para cada sistema, que são chamadas de Medidas de Quantificação da Recorrência (MQR), tais como Taxa da Recorrência (REC), Determinismo (DET), Entropia (ENTR), Tendência (TREND), Laminaridade (LAM), dentre outras. Tais medidas norteiam a AQR, o que resulta numa análise focada nas características dinâmicas extraídas ao invés de uma análise focada nas variabilidades momentâneas do tráfego. Esta propriedade foi preliminarmente explorada [Righi e Nunes 2015], tendo demonstrado melhor resultado quando comparado com medidas extraídas diretamente da análise de séries temporais por métodos estatísticos tradicionais.

Este trabalho propõe o DDoSbyAQR, um novo método para detecção de DDoS que utiliza a AQR baseada na extração de características dinâmicas e a clusterização adaptativa [Bhatia 2004] para classificar o tráfego de rede em tempo real. Os resultados dos testes realizados com as bases CAIDA e UCLA demonstraram incremento na acurácia para a detecção de ataques DDoS em redes de computadores. As principais contribuições deste trabalho são: (1) demonstrar que a partir de um conjunto de atributos que caracterizam ataques DDoS pode-se extrair características dinâmicas de recorrência; (2) demonstrar que a AQR pode ser utilizada para diminuir a proporção de falsos positivos e incrementar a de verdadeiros positivos, contribuindo para aumentar a acurácia dos IDS na detecção de DDoS; e (3) demonstrar que um clusterizador adaptativo (A-Kmeans), que calcula automaticamente o número de clusters, pode ser um bom aliado da AQR para aumentar a eficácia na classificação de ataque DDoS.

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados e a Seção 3 apresenta uma revisão teórica sobre a AQR; a Seção 4 apresenta detalhes da implementação do método proposto (DDoSbyAQR**)** e a Seção 5 apresenta os testes, os resultados e a comparação com outros métodos de detecção; finalmente, a Seção 6 apresenta a conclusão do artigo e indica possíveis trabalhos futuros.

2. Trabalhos Relacionados

Esta seção faz uma revisão de algumas técnicas existentes para detecção de DDoS, com a finalidade de apresentar o esforço dos pesquisadores em utilizar os melhores atributos e algoritmos para caracterizar esse tipo de ataque e, também, demonstrar que alguns métodos exploram características dinâmicas, porém com muitas limitações ainda.

A AQR foi utilizada em [Kumar 2012] [Jeyanthi et al. 2014], no entanto, a utilização é genérica, pois aplicam diretamente a extração de características dinâmicas nos traços de rede, gerando gráficos através do site http://www.recurrence-plot.tk/glance.php e visualizando-os de maneira empírica na ferramenta Weka para concluir que mudanças excessivas percebidas visualmente nos valores dessas características sinalizam um ataque ou anomalia, sem a preocupação em verificar os resultados, sua eficácia, falsos positivos e além disso, sem levar em conta o tempo de execução dessas ações e a geração de alertas em tempo real e sem definir atributos estatísticos que caracterizem um ataque DDoS.

Em [Oo et al. 2013], o método proposto procura caracterizar ataques DDoS com base em sete atributos extraídos diretamente do tráfego. Os atributos correspondem a parâmetros específicos do tráfego em situações de ataque e de normalidade e são utilizados diretamente pelo algoritmo classificador K-NN [Nguyen e Choi 2010], que faz a clusterização pela regra do vizinho mais próximo, na qual a escolha do número de clusters é fixa e determinada pelo pesquisador. No entanto, de acordo com a nossa

abordagem, a utilização de um classificador para operar diretamente a série temporal formada em cada atributo, bem como a escolha fixa do número de clusters, pode ser um limitador significativo para obtenção de uma boa eficiência do método de detecção.

Limwiwatkul e Rungsawang (2006) propuseram um método para detectar um ataque DDoS que analisa os cabeçalhos dos pacotes TCP/IP e procura criar um perfil de ataque concentrado principalmente em ICMP Flood, TCP Flood e UDP Flood. Este trabalho reforça a ideia de extração de atributos baseados no comportamento do tráfego de rede para caracterizar um ataque DDoS.

Em [Wu et al. 2011] os autores propõem a detecção de ataques DDoS utilizando um classificador baseado em árvore da decisão (algoritmo C4.5). No trabalho foram utilizados dezesseis atributos para descrever o padrão de tráfego em situação de normalidade. Porém a taxa de falsos positivos cresce quando o tráfego aumenta, conforme demonstrado nos gráficos do artigo, denotando uma menor eficácia do método em uma situação de aumento normal do fluxo da rede. Além disso, a escolha dos atributos não considerou características importantes para DDoS, dado que os atributos escolhidos não contemplam a variância do tamanho dos pacotes e a variância do tempo dos pacotes recebidos, que tendem a zero durante um ataque DDoS [Oo et al. 2013].

De maneira similar, em [Zhong e Yue 2010] os autores apresentam um método de detecção de ataques DDoS que captura o tráfego de rede e analisa o status da conexão do protocolo TCP/IP. Porém, os autores utilizam os algoritmos Apriori, FCM e K-Means, demonstrando que a combinação de múltiplos classificadores pode melhorar a acurácia da detecção, tal como também observado em [Silva et al. 2012].

Em [Grossglauser e Bolot 1999][Palmieri e Fiori 2010] é sugerido que o tráfego de rede se expõe a propriedades onipresentes de auto-similaridade e dependência de longa duração, ou seja, de correlações em uma ampla gama de escalas de tempo. Tais características, de acordo com [Marwan e Webber 2015], podem permitir a aplicação da Análise da Quantificação da Recorrência (AQR) como uma possível técnica para detecção de anomalias. É possível criar gráficos de recorrência e analisá-los através de características dinâmicas [Marwan e Webber 2015] que podem ser extraídas através de testes exaustivos que melhor caracterizam cada tipo de sistema avaliado. Em outras palavras, isto permite representar matematicamente as correlações dos pontos de recorrência e definir o comportamento da série temporal não estacionária.

Dos estudos, observou-se que a AQR, apesar de ser explorada em alguns trabalhos [Kumar 2012] [Jeyanthi et al. 2014] para caracterizar o tráfego de rede, ainda possui limitações e um dos poucos trabalhos que empregam características dinâmicas de uma maneira mais aprofundada é o de [Yuan et al. 2014], onde o autor combina um algoritmo de clusterização com a Transformada Wavelet (TW) e a AQR. Porém a quantidade de falsos positivos no trabalho de Yuan et al (2014) ultrapassa 8% quando utiliza a base de dados DARPA 1999, os dados estatísticos não caracterizam ataques DDoS e o clusterizador é o K-Means que possui a limitação de usar um número fixo de clusters, o que diminui sua eficácia. Diferentemente, neste trabalho exploramos em profundidade o uso da AQR baseada na extração de características dinâmicas, evitando observações apenas visuais dos Gráficos da Recorrência e análises estatísticas tradicionais de séries temporais. Nossa análise baseia-se nos limiares (*Thresholds*) das medidas de quantificação da recorrência (MQRs) para o tráfego considerado normal e na clusterização adaptativa, a qual calcula automaticamente o número de clusters necessários para formar o agrupamento para comparação com os limitadores definidos na fase de testes.

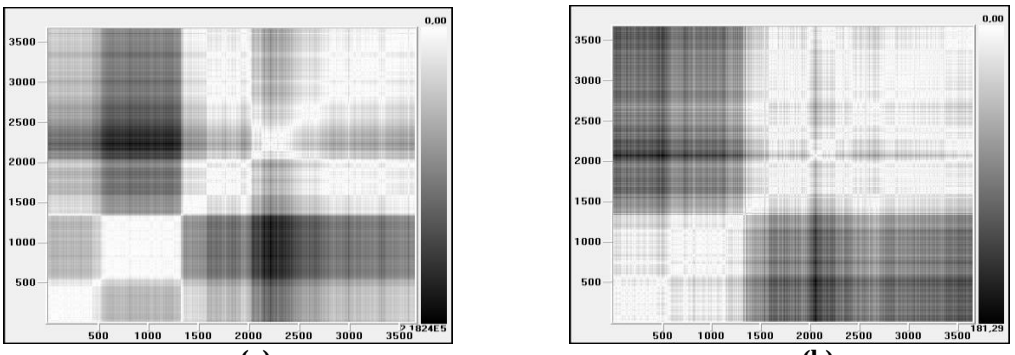
Complementarmente aos trabalhos descritos, foi observado que diversos autores [Rahmani et al. 2009][Bhaya e Manaa 2014][Suresh e Anitha 2011] utilizam as Bases de

Dados CAIDA 2008 e CAIDA 2007 para caracterizar tráfego normal e tráfego de ataque, indicando uma boa aceitação dessa base em pesquisas científicas na área de redes e detecção de DDoS. Tal observação foi fundamental para adoção destas bases nos experimentos deste trabalho.

3. Análise da quantificação da recorrência (AQR)

A quantificação da recorrência corresponde à quantificação do que os gráficos da recorrência mostram. Os Gráficos da Recorrência (vide exemplo na Figura 1) foram propostos em [Eckmann et al. 1987] como uma técnica de análise não linear de sistemas dinâmicos e proporcionam uma visualização do comportamento da trajetória do espaço de fases multidimensional [Webber e Marwan 2015].

Na prática, os Gráficos de Recorrência são matrizes bidimensionais quadradas que representam a evolução dos estados do sistema dinâmico e que são preenchidas por pontos pretos e brancos (vide Figura 1). Os pontos pretos indicam que há recorrência, ou seja, os estados do sistema dinâmico referentes a esses pontos orbitam em regiões próximas uns dos outros na trajetória do espaço de fases. Tais regiões são chamadas de Raio da Recorrência. Um ponto preto marcado na coordenada (i, j) do gráfico representa a recorrência do estado do sistema $e(i)$ no instante j [Eckmann et al, 1987][Webber e Marwan 2015]. Em outras palavras, considerando os gráficos da recorrência da Figura 1, gerados na fase de testes deste trabalho, cada estado do desvio padrão (Figura 1(a)) e média do tamanho dos pacotes (Figura 1(b)) em um determinado instante (i) é comparado com todos os outros estados em cada instante correspondente ($j, j+1, \ldots, n$). No caso de recorrência, um ponto preto será marcado a partir de cada resultado de cada comparação, caso contrário será marcado um ponto branco. No instante ($i+1$) seu estado será novamente comparado com todos os outros estados ($j, j+1, \ldots, n$) e assim sucessivamente até o término da série temporal para cada atributo utilizado. O resultado deste processo é uma matriz quadrada de pontos pretos e brancos que indicam a recorrência do atributo de interesse.



(a) **(b)**

Figura 1. Gráficos da recorrência para atributos do tráfego normal: (a) série temporal do Desvio Padrão do tamanho dos pacotes e seu Gráfico da Recorrência; (b) série temporal da Média do tamanho dos pacotes e seu Gráfico da Recorrência.

A expressão matemática que define a formação do gráfico da recorrência (estados definidos pela Equação 1) é computada com base em uma série temporal $X = \{ e_i, \ldots, e_n\}$ com seus estados e_i, onde $i = 1, 2, 3, \ldots, n$ [Eckmann et al. 1987][Marwan e Webber 2015]. Na equação, m é a dimensão de imersão (representa quantos atrasos são utilizados em relação à série temporal inicial), que neste trabalho é 1, n é o número total de

amostras que contém a série temporal, τ é o tempo de atraso (tempo de espera entre um estado e o outro) e *N* é o número de estados, sendo $N = n - (m-1)\tau$.

$$E = [e_j, e_{j+\tau}, ..., e_N],\ j = 1,2,3,...,N \quad (1)$$

Depois de calcular os estados de tráfego a partir de atributos pré-definidos (para o DDoSbyAQR os 7 atributos que expressam ataques de DDoS, conforme Seção 4), para cada um deles utiliza-se a análise dos fenômenos de recorrência que é realizado segundo a Equação da Recorrência (2).

$$R_{ij} = \theta(\varepsilon - \| e_i - e_j \|) \quad (2)$$

Onde, R_{ij} corresponde a um elemento da matriz de recorrência, ε ao limiar adotado, e_i e e_j aos estados do sistema no espaço de fase *m*-dimensional ora em análise, *N* ao número de estados considerados e θ a função de decisão definida pela Equação (3). De acordo com a Equação (3), se a distância entre os estados e_i e e_j é menor do que o limiar ε, então o valor de $\theta(\varepsilon)$ é 1 e existe um ponto preto na posição (*i*, *j*) do Gráfico da Recorrência; caso contrário, o valor de $\theta(\varepsilon)$ é 0 e existe um ponto branco em (*i*, *j*).

$$\theta(f(\varepsilon)) = \begin{cases} 0 & (\varepsilon - \|e_i - e_j\|) \leq 0 \\ 1 & (\varepsilon - \|e_i - e_j\|) > 0 \end{cases} \quad (3)$$

Cabe salientar que um parâmetro importante na AQR é o raio de vizinhança. Este raio é quem define os pontos recorrentes no gráfico de recorrência, logo é um parâmetro chave na AQR. Como este limiar depende de cada tipo de sistema que está sendo analisado e dos seus objetivos [Marwan e Webber 2015], a literatura não apresenta um método específico para estabelecer o raio da vizinhança ideal que defina os pontos recorrentes, tendo este que ser ajustado de acordo com o tipo de aplicação, no nosso caso detecção de DDoS.

Para o raio da vizinhança foi utilizada a taxa de 10%, com base na observação de valores de outros trabalhos como o de [Yuan et a. 2014]. Porém, para chegar a este valor foi utilizada, também, a técnica em que usa-se, inicialmente, o máximo do valor do raio da vizinhança e tem-se uma recorrência máxima no Gráfico da quantificação da Recorrência (GQR) e gradativamente ela é decrescida ao ponto de termos uma mudança abrupta na observação visual do GQR chegando-se a uma taxa relativamente próxima da ideal. O impacto do raio da vizinha é extremamente relevante, pois se tivermos uma taxa alta haverá muita recorrência no GQR e não se poderá visualizar suas mudanças de comportamento, por outro lado, se a taxa for muito baixa não haverá pontos de recorrência no GQR e nenhuma MQR poderá ser extraída.

A partir do Gráfico da Recorrência, a Análise de Quantificação de Recorrência (AQR) permite realizar e potencializar avaliações visuais da recorrência. Entretanto, a análise visual dos gráficos de recorrência é subjetiva e pode levar a diferentes interpretações. Por isso, com o objetivo de trazer mais precisão às análises, as estruturas presentes nos gráficos de recorrência foram quantificadas através de Medidas de Quantificação de Recorrência (MQR).

De acordo com Marwan (2003), as principais MQRs são:

a) Razão de Recorrência (RR) - mede a densidade dos pontos de recorrência no gráfico de recorrência;

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

c) Comprimento médio das linhas diagonais (L) – indica o tempo médio que dois segmentos de uma trajetória se mantêm próximos um do outro, podendo ser interpretado como o tempo médio de predição;

d) Comprimento máximo das linhas diagonais (Lmax) – indica o tempo máximo que dois segmentos de uma trajetória se mantêm próximos um do outro. Mais utilizado na análise de quantificação de recorrência do que o comprimento médio das linhas diagonais;

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

f) Tendência (TREND) - é um coeficiente de regressão linear sobre a densidade dos pontos de recorrência das diagonais paralelas a diagonal principal (linha de identidade). Essa medida fornece informações a respeito da não-estacionariedade do processo;

g) Laminaridade (LAM) - razão entre os pontos de recorrência que formam as estruturas verticais e todo o conjunto de todos os pontos de recorrência presentes no gráfico;

h) Comprimento médio das estruturas verticais (TT) – também conhecida como tempo de permanência em um estado (*Trapping Time*). Essa medida contém informação acerca da quantidade e do comprimento das estruturas verticais no gráfico de recorrência. Ela mede o tempo médio que o sistema permanece em um estado específico.

As Linhas diagonais mostram a evolução dos estados similares em tempos diferentes e as Linhas Verticais indicam os estados que não mudam ou mudam lentamente ao longo do tempo [Marwan e Kurths 2005].

Note que através da AQR e suas MQRs é possível avaliar computacionalmente o comportamento recorrente de sistemas dinâmicos não estacionários independentemente da dimensionalidade dos mesmos, mesmo sob variabilidade do tráfego na rede. Esta propriedade da AQR elimina a necessidade de considerar a estacionariedade da série temporal, tal como necessitam os métodos estatísticos tradicionais, permitindo seu uso inclusive na análise de séries curtas e não-estacionárias. Em síntese, uma das principais vantagens oferecidas pela AQR, em comparação a outras técnicas de análise dinâmica não-linear, é habilitar a análise de pontos de recorrência no espaço de fase bidimensional de um sistema não-estacionário, o que pode evitar desvios (bias) na análise sujeita a sobrecargas eventuais nos parâmetros amostrais do sistema.

4. Detalhamento do Método *DDoSbyAQR*

Nesta seção é apresentado o método de detecção de anomalias *DDoSbyAQR.* A Figura 2 apresenta a arquitetura modular da solução de detecção, onde o módulo de detecção de ataques DDoS que abriga o método proposto é destacado. As seções 4.1, 4.2 e 4.3 detalham cada módulo e a seção 4.4 apresenta o algoritmo que implementa o método *DDoSbyAQR.*

De maneira geral o *DDoSbyAQR* pode ser visto como um método que combina a Análise da Quantificação da Recorrência (AQR) e a Clusterização Adaptativa (A-Kmeans). No contexto da arquitetura da solução proposta (Figura 2), cabe salientar que a extração de atributos corresponde à fase de seleção de atributos de rede que forneçam informações relevantes ao problema de interesse (detecção de DDoS).

Diferentemente, numa das fases da AQR são extraídas características dinâmicas do tráfego de rede e que visam habilitar a análise da recorrência através de MQRs. A clusterização adaptativa flexibiliza o cálculo do número de clusters utilizados para classificar o tráfego, feito automaticamente no A-Kmeans. O cálculo automático potencializa a minimização dos erros de acurácia do classificador. Por exemplo, no Kmeans o número de clusters é determinado pelo pesquisador.

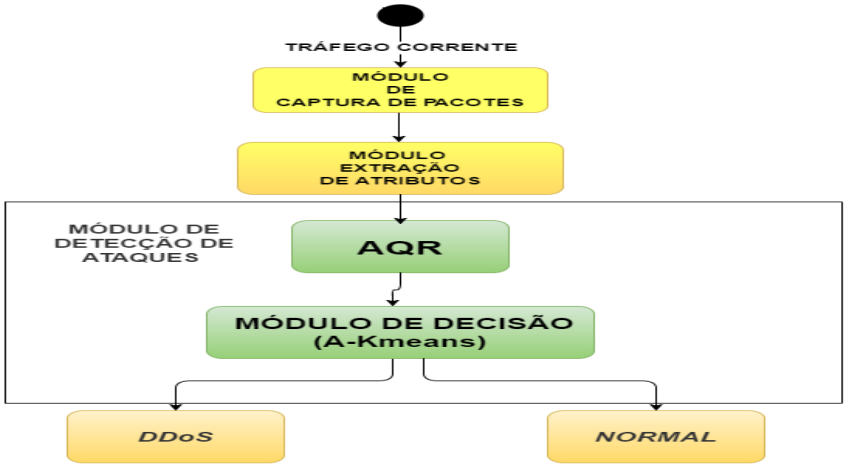


Figura 2. Arquitetura da solução de detecção com o método *DDoSbyAQR*.

4.1. Módulo de Captura de Pacotes

Este módulo seleciona o tráfego de entrada de rede, em intervalos de tempo de 60 segundos, que serão utilizados pela AQR e serve como estação de captura de pacotes, recebendo, periodicamente, dados coletados por um sensor posicionado estrategicamente na rede que utiliza a ferramenta TCPDump para coleta dos traços.

Após coletados, os dados são enviados ao Módulo de Extração de Atributos.

4.2. Módulo de Extração de Atributos

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. 2013], os quais verificaram em seus experimentos que os atributos que se adequam melhor ao tipo de ataque DDoS são sete, conforme ilustra a Tabela 1.

O Módulo de Extração de Atributos consiste na extração, do tráfego de rede com os listados na Tabela 1, os quais são repassados ao Módulo de Detecção, sendo a ferramenta TCPSTAT utilizada para extração dos atributos estatísticos do tráfego de uma série temporal de 60 segundos, ou seja, são formadas sete séries temporais, uma para cada atributo extraído com o TCPSTAT e aplicada a AQR para extração das características dinâmicas (3 para cada série temporal – Entropia, Determinismo e Razão da Recorrência).

Tabela 1. Atributos utilizados pela AQR. Adaptado de [Oo et al. 2013]

ATRIBUTOS	DESCRIÇÃO
NUM_PAC	Número de pacotes recebidos na rede
NUM_BYTES	Número de bytes recebidos na rede
M_PAC	Média do tamanho dos pacotes recebidos
VAR_TEM_PAC	Variância do tempo dos pacotes (Timestamp) recebidos
VAR_TAM_PAC	Variância do tamanho dos pacotes recebidos
TAX_PAC	Taxa total de pacotes
TAX_BYTES	Taxa total de bytes

4.3. Módulo de Detecção de Ataques

O Módulo de Detecção de Ataques é o módulo central da solução proposta (vide Figura 2), sendo composto pelo Módulo de Análise da Quantificação da Recorrência (seção 4.3.1) e pelo Módulo de Decisão centrado em um classificador adaptativo (seção 4.3.2).

4.3.1. Módulo AQR

No Módulo AQR cada atributo passado pelo Módulo de Extração de Atributos é representado na forma de uma série temporal (60 segundos), modelada por amostras realizadas em períodos equidistantes. A cada série temporal, correspondente a um dos 7 atributos que expressam ataques de DDoS (vide Tabela 1), é aplicada a Análise da Quantificação da Recorrência, conforme definida na seção 3.

Após a formação do gráfico da recorrência, para cada atributo representado como uma série temporal são extraídas três características dinâmicas: a Razão de Recorrência (RR), a Entropia (ENTR) e o Determinismo (DET). Estas características correspondem a Medidas de Quantificação de Recorrência e foram utilizadas em [Vieira et al. 2012] para detecção de anomalias no sinal de voz, sendo reutilizadas no *DDoSbyAQR* para detecção de DDoS por análise de anomalias. Naturalmente, outras medidas, tais como as citadas na seção 3, também podem ser aplicadas nesta etapa do método *DDoSbyAQR.*

Para extrair as características dinâmicas a serem repassadas ao Módulo de Decisão, os cálculos de quantificação (computo da RR, DET e ENTR) aplicados ao Gráfico da Recorrência são feitos como segue.

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

$$RR = \frac{1}{N^2} \sum_{i,j=1}^{N} R_{i,j} \tag{4}$$

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.

$$DET = \frac{\sum_{l=l\min}^{N} lP(l)}{\sum_{i,j=1}^{N} R_{i,j}} \tag{5}$$

Onde $P(l)$ é o número de pontos de recorrência para cada diagonal formada.

3) **Entropia de Shannon (ENTR) -** representa a distribuição de frequências dos comprimentos das linhas diagonais e reflete a complexidade da estrutura determinística presente no sistema. Está relacionada com a incerteza do sistema.

$$ENT = \sum_{l=l\min}^{N} p(l) \log_2 p(l) \tag{6}$$

$$p(l) \frac{P(l)}{\sum_{l=l\min}^{N} P(l)} \tag{7}$$

Salienta-se que as três características dinâmicas utilizadas neste módulo são descritores dinâmicos de comportamento que mantêm a estacionariedade em seus resultados durante o tráfego livre de ataques, mesmo em momentos de alta variabilidade dos estados dos atributos (sete) utilizados para cada uma das séries temporais. Esta propriedade dos descritores pode evitar alarmes falsos na presença de *outliers* não relacionados a ataques de negação de serviço, ou seja, analisar as MQRs geradas é mais eficaz na detecção de DDoS do que analisar a série temporal de origem para cada atributo.

As estruturas diagonais e verticais citadas são parâmetros que se formam no Gráfico da Quantificação da Recorrência, mas que podem ocorrer em maior ou menor quantidade,

ou seja, são linhas verticais ou diagonais que são moldadas pela quantidade de pontos pretos que as formam, sendo que em um determinado sistema pode haver formação maior de estruturas diagonais do que verticais e em outro os valores sejam totalmente inversos. Portanto, cada medida é uma maneira de visualizar matematicamente o GQR e aproveitar cada mínimo detalhe para verificar se há recorrência ou não em uma determinada série temporal de diferentes sistemas.

O Módulo AQR, através das 21 características dinâmicas (3 para cada um dos 7 atributos), forma um conjunto que procura expressar através das propriedades de recorrência o comportamento dos sete atributos analisados. Este conjunto é então encaminhado ao Módulo de Decisão para ser clusterizado e classificado.

4.3.2. Módulo de Decisão

Dado o conjunto de características dinâmicas recebido do Módulo AQR, o Módulo de Decisão tem a função de organizar os dados, particionando-os em grupos por similaridade (*clusters*) e classificando-os como ataque DDoS (anômalos) ou não (não anômalos).

Para contornar a dificuldade de definir o número ideal de clusters, o método *DDoSbyAQR* aplica o algoritmo A-Kmeans [Bhatia 2004] que processa um conjunto com 21 características dinâmicas, três para cada atributo (sete), sendo em cada atributo utilizados os valores da Entropia, o Determinismo e a Razão ou Taxa de Recorrência. Após isso o A-Kmeans calcula automaticamente o número de clusters (valor de "k" é automático) e compara cada um deles com os limiares pré-estabelecidos na fase de treinamento com as bases de traços normais. Na sequência, se a maioria dos clusters for considerada anômala, então o tráfego será nominado como ataque DDoS.

A decisão do módulo está então centrada no cálculo dos centroides (pontos centrais de cada cluster) do conjunto de características dinâmicas recebidas do Módulo AQR e na análise se a maioria dos agrupamentos formados forem classificados como anômalos, situação em que o tráfego será classificado como Ataque DDoS.

4.4. Algoritmo do DDoSbyAQR

A seguir o detalhamento das etapas do algoritmo que implementa o método DDoSbyAQR.

Entrada: séries temporais de tráfego (sete atributos).
Saída: indicação de ataque DDoS ou tráfego normal
Etapa 1: para cada série de tráfego *X* (uma para cada um dos sete atributos), utilizar a AQR para calcular as características dinâmicas (Taxa de Recorrência, Entropia e Determinismo).

$$F_1 = f(X_{NUM\_PAC}) \quad F_2 = f(X_{NUM\_BYTES}) \quad F_3 = f(X_{M\_PAC}) \quad F_4 = f(X_{VAR\_TEM\_PAC})$$

$$F_5 = f(X_{VAR\_TAM\_PAC}) \quad F_6 = f(X_{TAX\_PAC}) \quad F_7 = f(X_{TAX\_BYTES})$$

$$F_n = \{RR_n, ENT_n, DET_n\}, \quad n = 1,2,3,4,5,6,7$$

Etapa 2: combinar as 21 características dinâmicas resultantes da Etapa 1 para descrever os padrões dinâmicos de comportamento do tráfego sintetizados em *F*.

$$F = \{[RR_n, ENT_n, DET_n]\}$$

Etapa 3: usar o algoritmo A-Kmeans para agrupar as características dinâmicas em *F* dentro de diferentes clusters e classificar o comportamento do tráfego como Ataque DDoS ou Normal.

Note que de maneira geral de cada atributo o algoritmo extrai três MQRs (RR, DET e ENTR) através da AQR e permite que o A-Kmeans opere um conjunto de 21 (vinte e uma) características dinâmicas do intervalo de tempo de análise definido pela série temporal.

5. Experimentos e Resultados

5.1. Organização dos Experimentos

Nos experimentos do DDoSbyAQR foram usadas três bases de dados: CAIDA 2007, CAIDA 2008 e UCLA CSD. A base de dados CAIDA 2007 possui cerca de uma hora de ataques DDoS (ICMP *Flood* e TCP *Flood*) divididos em arquivos "pcap" sanitizados de 5 minutos cada. A base de dados CAIDA 2008 possui cerca de 16 horas de tráfego sem ataque divididos em arquivos "pcap" sanitizados de uma hora cada um, colhidos durante dezesseis dias na rede CAIDA de Chicago e San Jose nos EUA. A base de dados UCLA CSD possui traços de uma hora de ataques DDoS (UDP Flood) e traços de tráfego sem ataque coletados em dez dias diferentes. Dos dados, foram extraídos sete atributos, conforme Tabela 1, resultando em uma série temporal *X* para cada atributo de interesse.

Os experimentos foram organizados em duas fases, uma de treinamento e outra de testes. Em ambas fases foram utilizadas séries temporais correspondentes a uma amostragem de 60 segundos. Os dados usados nos experimentos foram organizados tal como ilustra a Tabela 2.

Na fase de treinamento o experimento teve como objetivo calibrar os limiares do método DDoSbyAQR, identificando o comportamento de cada característica dinâmica em traços com e sem ataques. Para tal, o experimento utilizou um conjunto de dados com 62 minutos de traços da Base de Dados CAIDA 2008 e 152 minutos da base UCLA CSD sem traços de ataques, para caracterizar o tráfego normal, e um conjunto de dados apenas com traços contendo ataques DDoS, com 66 minutos de amostragem da base CAIDA 2007 e 56 minutos da base UCLA CSD, para caracterizar o tráfego anômalo.

Na fase de testes o experimento teve como objetivo avaliar a acurácia do método, ou seja, a proporção de predições corretas. Para tal, foram intercaladas linhas de tráfego contendo ataque DDoS com linhas de tráfego sem ataque, sendo que a inserção de linhas de ataque foi feita de forma aleatória em pontos variados no tráfego normal, porém a quantidade de linhas de ataque foi sempre a mesma (300 linhas ou 300 segundos), ou seja, o sistema deverá detectar em cada série de ataque no máximo cinco alertas de ataque DDoS. Neste experimento foram utilizados 128 minutos de dados intercalando dados da base CAIDA 2007 (com ataques) e da base CAIDA 2008 (sem ataques) e 210 minutos de dados intercalando dados da base UCLA CSD com e sem ataques.

Tabela 2. Bases de Dados Utilizadas

BASE DE DADOS	*Tipo de Tráfego*	*Qtde Linhas (1 seg)*	*Tempo (min)*
CAIDA 2008	**Normal**	**3661**	**62**
UCLA CSD Normal	**Normal**	**9155**	**152**
CAIDA 2007	**Ataque DDoS**	**3955**	**66**
UCLA CSD DDoS	**Ataque DDoS**	**3354**	**56**
CAIDA 2007/2008	**Normal/DDoS**	**7616**	**128**
UCLA CSD Normal/DDoS	**Normal/DDoS**	**12509**	**210**

5.2. Testes e Resultados

A Figuras 3 ilustra o resultado da fase de treinamento para uma das MQRs (RR) dos sete atributos de tráfego utilizados, a média do tamanho dos pacotes (M_PAC). A análise das características dinâmicas dos demais atributos seguem a mesma metodologia e sua demonstração foi suprimida para eliminar redundância. Para o primeiro conjunto de dados (Série Normal), a Razão da Recorrência do atributo M_PAC demonstrou ser estacionária, com a taxa em torno de 25%. Já no segundo conjunto de dados, contendo apenas traços de ataques, o comportamento estacionário se manteve, mas os níveis de RR se elevaram para praticamente o dobro do observado em séries sem ataque. Para fins de detecção isto indica a viabilidade da adoção de limiares que permitam realizar a distinção entre tráfego normal e com ataques DDoS usando as MQRs.

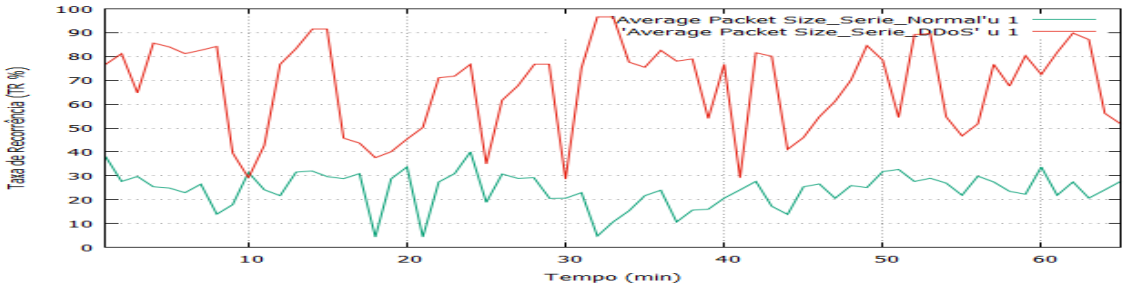


Figura 3. Taxa de Recorrência para Média do Tamanho dos pacotes (M_PAC)

As Tabelas 3 e 4 apresentam os resultados da fase de testes. O experimento avaliou a proporção de verdadeiros positivos (VP), de falsos positivos (FP) e a acurácia resultante (AC), sendo a acurácia definida como segue.

$$AC = \frac{VP}{(VP + FP)} \tag{8}$$

Para fins de comparação foram realizados testes com os algoritmos K-Means, AQR + K-Means, A-Kmeans e AQR + A-Kmeans, este último correspondendo ao método *DDoSbyAQR*, permitindo avaliar o impacto tanto da inclusão da AQR quanto da clusterização adaptativa, sendo que o valor escolhido para o parâmetro *k* (número de clusters) do K-Means e AQR + K-Means foi 4 (quatro), comparando-se com o A-Kmeans e AQR + A-Kmeans, nos quais o parâmetro *k* é calculado automaticamente, com o objetivo de ser mais eficaz. Os testes também consideraram dois conjuntos de dados, um intercalando dados das bases de dados CAIDA 2007 e CAIDA 2008 (Tabela 3) e outro intercalando dados das bases de dados UCLA CSD Normal e UCLA CSD com DDoS.

Os resultados obtidos com os dados intercalando traços com e sem ataques (Tabelas 3 e 4) indicam, para ambos conjuntos de dados, uma melhora dos classificadores quando aplicados em conjunto com a AQR. A proporção de verdadeiros positivos quando a AQR é associada ao K-Means melhorou mais de 13% (13,88% para dados da CAIDA e 18,15% para dados da UCLA CSD) e mais de 19% quando associada ao A-Kmeans (20,03% para dados da CAIDA e 19,69% para dados da UCLA CSD). A redução da proporção de falsos positivos também foi significativa (vide Tabelas 3 e 4). Como resultado, em ambos os conjuntos de dados, houve um incremento na acurácia dos classificadores, chegando a uma melhora de 10,54% para o A-Kmeans na base CAIDA. A associação do AQR+A-Kmeans também se mostrou mais eficaz do que a AQR+KMeans, demonstrando a eficácia da clusterização adaptativa no método *DDoSbyAQR*. Com dados da CAIDA a acurácia melhorou 12,42% e com dados da

UCLA CSD melhorou 8,62%, demonstrando incremento de acurácia na detecção de DDoS quando aplicado o método *DDoSbyAQR*.

Tabela 3. Resultados para o conjunto de dados CAIDA 2007/2008

ALGORITMO	AC (%)	VP (%)	FP (%)
K-Means	**70,96**	**69,23**	**28,33**
AQR+K-Means	**85,99**	**83,08**	**13,54**
A-Kmeans	**85,96**	**75,35**	**12,31**
AQR+A-Kmeans	**98,41**	**95,38**	**1,54**

Tabela 4. Resultados para o conjunto de dados UCLA CSD Normal/DDoS

ALGORITMO	AC (%)	VP (%)	FP (%)
K-Means	**84,34**	**60,63**	**11,25**
AQR+K-Means	**88,26**	**78,78**	**10,48**
A-Kmeans	**94,23**	**74,24**	**4,54**
AQR+A-Kmeans	**96,88**	**93,93**	**3,03**

6. 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 explorada com limitações no contexto de detecção 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 clusterizador adaptativo A-Kmeans.

O trabalho demonstrou que a partir de atributos que caracterizam DDoS (sete coletados a partir do tráfego de rede) é possível extrair características dinâmicas da recorrência, e que a análise destas permite incrementar a acurácia da detecção de DDoS. Salienta-se que a análise da recorrência ao permitir uma avaliação do tráfego num outro domínio, o de comportamento dinâmico da recorrência, possibilita sobrepor a influência negativa de variabilidades nos atributos do tráfego que poderiam levar a detecções errôneas.

Os experimentos demonstraram que a utilização da AQR incrementa a acurácia na identificação de ataques DDoS. Quando avaliado o benefício de classificar características dinâmicas de recorrência ao invés de classificar atributos de tráfego (avaliação dos classificadores com e sem a AQR), observa-se incrementos de até 10,54% na acurácia da detecção. Este resultado está associado a significativo incremento nos verdadeiros positivos e decremento nos falsos positivos. Porém, é consequência do método que, em tráfego aparentemente sem variações bruscas, permite observar mudanças nos padrões comportamentais da recorrência que auxiliam os classificadores a gerar agrupamentos que indicam anomalias e, em tráfego com variações bruscas não oriundas de ataques, permite observar regularidade no comportamento da recorrência.

A utilização do algoritmo A-Kmeans, um clusterizador adaptativo que calcula automaticamente o número de clusters, também demonstrou se adequar bem à detecção de DDoS baseada na AQR, tendo melhorado, no pior caso, 8,62% a acurácia da detecção quando comparado com um clusterizador não adaptativo (K-Means). A dificuldade encontrada pelo K-Means reflete a dificuldade de calibrar um clusterizador não adaptativo, o que pôde ser observado pela variabilidade de acurácia quando explorados dois conjuntos de dados com características distintas.

O método *DDoSbyAQR*, embora eficaz para a detecção de DDoS, também pode ser explorado em outros contextos de análise comportamental de rede, principalmente

pela sua característica de permitir a análise no domínio da recorrência, minimizando a influência negativa de variabilidades que causam desvios na análise de estatísticas tradicionais do tráfego.

7. Referências

Bhatia, S. K. (2004). Adaptive K-Means Clustering. *Proc. of the Int. Florida Artificial Intelligence Research Society Conference*, Miami, AAAI, pp. 695-699.

Bhaya, W., Manaa, M. E. (2014). A Proactive DDoS Attack Detection Approach Using Data Mining Cluster Analysis. Journal of Next Generation Information Technology (JNIT) Volume 5, nº 4.

Eckmann, J. P., Kamphorst, S. O., Ruelle, D. (1987). Recurrence plots of dynamical systems. Europhys. Lett., 56(5), p. 973–977.

Grossglauser, M., Bolot, J. C. (1999). On the relevance of long-range dependence in network traffic. IEEE/M Transactions on Networking, 7(5): p. 629-640.

Jeyanthi, N.; Thandeeswaran, R.; Vinithra, J. (2014). RQA based approach to detect and prevent DDoS attacks in VoIP networks, Cybernetics and Information Technologies. v. 14, p. 11-24.

Kumar, C. A.; Bhargavi, K.; Garima, J. (2012). A Note on Implementing Recurrence Quantification Analysis for Network Anomaly Detection. Defence Science Journal, [S.l.], v. 62, n. 2, p. 112-116.

Limwiwatkul, L., Rungsawang, A. (2006). Distributed denial of service detection using TCP/IP header and traffic measurement analysis. Proceedings of the IEEE International Symposium Communications and Information Technology, Sapporo, Japan, 26-29 October, p. 605–610. IEEE CS.

Marwan, N. (2003). Encounters With Neighbours - Current Developments of Concepts Based on Recurrence Plots and Their Applications. Ph.D. thesis, University of Potsdam.

Marwan, N., Kurths, J. (2005). Line structures in recurrence plots. Physics Letters A, 336(4–5), p. 349–357.

Marwan, N., Webber, C.L., Jr. (2015). Mathematical and computational foundations of recurrence quantifications. In: Recurrence Quantification Analysis: Theory and Best Practices. Springer Series: Understanding Complex Systems. Springer International Publishing, Cham, Switzerland, p. 1-41.

Nguyen, H. and Choi, Y. (2010). Proactive Detection of DDoS Attacks Utilizing k-NN Classifier in an Anti-DDos Framework. International Journal of Electrical and Electronics Engineering, Vol. 4, nº 4.

Oo, T. T., Phyu, T. (2013). A Statistical Approach to Classify and Identify DDoS Attacks using UCLA Dataset. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 5.

Palmieri, F., Fiore, U. (2010). Network anomaly detection through nonlinear analysis, Computers & Security, 29(7), p. 737–755.

Rahmani H., Sahli, N., Kammoun, F. (2009). Joint Entropy Analysis Model for DDoS Attack Detection. In International Conference on Information Assurance and Security, p. 267-271.

Raut, A.S., Singh, K. R. (2014). Anomaly Based Intrusion Detection-A Review. Int. J. on Network Security, Vol. 5.

Righi, M. A., Nunes, R. C. (2015). Detecção de DDoS Através da Análise da Recorrência Baseada na Extração de Características Dinâmicas. Anais do XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg 2015, p. 314-317.

Silva, J. L. C., Maia, J. E. B., Fonseca, N. L. S. (2012). Identificação de Ataques em Redes de Computadores usando Comitê de Classificadores. Anais do XXX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, p. 263-276.

Suresh, M., Anitha, R. (2011). Evaluating Machine Learning Algorithms for Detecting DDoS Attacks. In 4th international Conference on Advances in Network Security and Applications (CNSA), p. 441-452.

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, C. F., Hsu, Y. F., Lin, C. Y. e Lin, W. Y. (2009). Intrusion detection by machine learning: A review. Expert Systems with Applications, v. 36, n. 10, p. 11994–12000.

UCLA CSD packet traces. http://www.lasr.cs.ucla.edu/ddos/traces/public/usc

Vieira, V. J. D., Costa, S. C., Costa, W. C. A. (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., Marwan, N. (2015). Recurrence Quantification Analysis: Theory and Best Practices. Springer series: Understanding Complex Systems. Springer International Publishing, Cham Switzerland.

Willinger, W., Paxson, V., Taqqu, M. S. (1998). Self-similarity and heavy tail: structural modeling of network traffic, A Pratical Guide to Heavy Tails: Statistical Techniques and Applications. ISBN:0-8176-3951-9, p. 27-53, BirkhRäuser, Boston, USA.

Wu, Y. C., Tseng, H. R., Yang, W., and Jan, R. H. (2011). DDoS detection and traceback with decision tree and grey relational analysis. International Journal of Ad Hoc and Ubiquitous Computing, 7, p. 121–136.

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), p. 101-112.

Zhong, R. and Yue, G. (2010). DDoS detection system based on data mining. Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China, 2-4 April, p. 062–065. Academy Publisher.

