Universidade Federal do Ceará

Centro de Tecnologia

Departamento de Engenharia de Teleinformática

Curso de Engenharia de Computação

BRUNO RICCELLI DOS SANTOS SILVA

PROJETO DE UM FRAMEWORK DE DETECÇÃO DE ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO

Fortaleza, Ceará

2017

BRUNO RICCELLI DOS SANTOS SILVA

PROJETO DE UM FRAMEWORK DE DETECÇÃO DE ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO

Monografia apresentada ao Curso de Engenharia de Computação da Universidade Federal do Ceará, como requisito parcial para obtenção do Título de Bacharel em Engenharia de Computação.

Orientador: Prof. RICARDO JARDEL NUNES DA SILVEIRA

Co-Orientador: Prof. MARCELO ARAÚJO LIMA

Fortaleza, Ceará

2017

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

DDOS	Distributed Denial of Service

Lista de símbolos

X	Vetor de entrada para correlação NaHiD

Sumário

1 Metodologia

Neste capítulo, os detalhes do *framework* serão apresentados bem como a modelagem do ambiente de simulação utilizado para a detecção de Ataques [DDOS]

1.1 Modelo de correlação NaHiD

Neste trabalho, o *framework* utilizado baseia-se na correlação proposta por (HOQUE; KASHYAP; BHATTACHARYYA, 2017) chamada NaHiD, cujo objetivo é distinguir objetos de tráfego normais e maliciosos. Tal medida leva em consideração principalmente desvio padrão e média de cada objeto, ponderando cada elemento como mostrado na fórmula a seguir:

$$NaHiD(X,Y) = 1 - \frac{1}{n}\sum_{i=1}^{n}\frac{(|X(i) - Y(i)|)}{||\mu X - sX| - X(i)| + ||\mu Y - sY| - Y(i)|} \tag{1.1}$$

onde

- μX: Média do objeto de tráfego X.
- μX: Média do objeto de tráfego Y.
- sX: Desvio padrão do objeto de tráfego X.
- sY: Desvio Padrão do objeto de tráfego Y.

As provas de simetria e identidade da correlação podem ser encontradas em (HOQUE; KASHYAP; BHATTACHARYYA, 2017).

1.2 Framework de detecção de ataques DDOS

O *framework* tem como objetivo detectar ataques DDoS em tempo real no computador alvo a partir de dados de tráfego de rede com uma taxa aceitável de erros. Tal arcabouço possui três componentes: pré-processamento, um módulo de detecção e um gerente de segurança.Amostras de tráfego serão capturadas de uma porta do roteador como um pacote TCP/IP, que são enviadas ao módulo de pré-processamento. Nessa fase, a cada segundo, os pacotes recebidos são agrupados e essa instância de tráfego é enviada para o módulo de detecção de ataque, que irá classificar a instância como normal ou ataque. O gerente de segurança manterá um perfil normal e um valor limiar em sua base de perfis,

para ser usado pelo módulo de detecção. Incrementalmente, o gerente recalcula o perfil normal e o limiar baseado nos valores anteriores. O último módulo, que é o módulo de segurança irá operar offline e fará análises detalhadas dos *logs* de detecção usando técnicas de *machine learning* e estatística. Os componentes citados acima serão mais detalhados a seguir.

1.2.1 Pré-Processamento

Nessa etapa, os dados são coletados da rede e, a cada segundo, as métricas desejadas são calculadas para servirem de entrada para a correlação NaHiD.

1.2.1.1 Entropia de IPs origem

A entropia de IPs origem é uma medida do grau de desordem onde ela é máxima, caso todos os elementos sejam diferentes e o tamanho da entrada é máxima e será mínima (igual a 0) quando todos os elementos são iguais. Assim, a entropia é dada pela seguinte fórmula:

$$H(X) = -\sum_{i}^{n} p(x_i) log_2(x_i) \tag{1.2}$$

Onde X é a entrada e representa os IPs origem das requisições e n é o número total de valores possíveis para o IP origem.

1.2.1.2 Variação de IPs Origem

Essa medida, diferentemente da entropia, trata-se da taxa de mudança dos IPs origem e é calculada da seguinte forma:

$$V_{Ip}(X) = \frac{\delta}{N} \tag{1.3}$$

Onde δ é o número de mudanças de IPs origem e N é o numero total de IPs de entrada. Neste trabalho consideramos uma variação cada troca de valores como no exemplo:

$$X = 1, 2, 1, 2, 3 \tag{1.4}$$

Assim, nesse vetor consideram-se 4 variações ainda que sejam para um valor que repetiu-se. Assim se os IPs origem mudarem frequentemente, a variação será alta. (HOQUE; KASHYAP; BHATTACHARYYA, 2017)

A observação do comportamento de ataques por *flood* mostra que esse tipo de ameaça pode ser gerada por atacantes reais como zumbis. Se endereços de IP origem falsificados forem utilizados durante um ataque DDOS TCP SYN, a entropia e variação de IPs origem serão altas e esse comportamento também ocorre em um tráfego normal. (HOQUE; KASHYAP; BHATTACHARYYA, 2017). Assim faz-se necessário o uso da taxa de pacotes em bits como terceiro medida de entrada para o cálculo da correlação NaHiD.

1.2.2 Módulo de Detecção

O modulo de detecção consiste no uso da correlação NaHiD utilizando os três parâmetros de entrada:

- Variação de IPs origem
- Entropia de IPs origem
- Taxa de pacotes

Onde um tráfego normal deve ser fixado para a comparação com o tráfego a ser analisado. Além disso,define-se um limiar do resultado da correlação para distinguir pacotes normais de maliciosos

1.2.3 Gerenciador Offline

Nessa etapa, os *logs* são salvos e se o módulo de detecção identificar que o tráfego em questão é normal, este será atualizado com os valores do mesmo para a próxima análise

1.3 Detecção de Ataques DDOS usando NaHiD

Para a avaliação do trabalho, duas bases de tráfegos de rede foram escolhidas: DARPA e DataMining[escolher melhor esse nome] os quais serão mais detalhados aa seguir

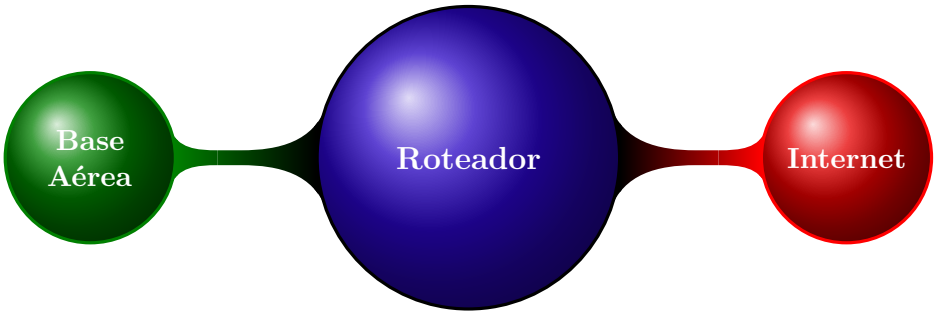
1.3.1 DARPA - MIT

A base de dados DARPA foi produzida por pesquisadores do *Lincoln Laboratory* do Instituto de Tecnologia de Massachusetts nos Estados Unidos e tem por objetivo coletar dados de tráfego de rede da Força Aérea do país para encontrar vulnerabilidades em seu sistema bem como ser utilizado para avaliações futuras . Os dados foram coletados e passaram por uma fase de treinamento de 7 semanas com 38 tipos de ataques para simular ameaças internas a rede. O ambiente de rede era composto por duas partes: a rede interna da Força aérea e a rede externa que representava a Internet; ambos conectados por meio de um roteador como mostra a Figura 1.1
Tal banco de dados é disponibilizado pela DARPA em um arquivo de extensão tcpdump, bem como a listagem de tráfegos normais e ataques rotulados como mostrados nas tabelas seguir

No presente trabalho ferramentas como edicap e tcpdump foram utilizadas para o tratamento desse dataset. Assim, algumas considerações devem ser feitas:

- Janela de um segundo de tráfego

Figura 1.1 – Estrutura de rede Base Aérea dos EUA



Fonte: Elaborada pelo autor.

- Cálculo de entropia, variação de IPs origem e taxa de pacotes média
- Cálculo da correlação NaHiD

.

1.3.2 DataMining

Outra base de dados estudada no trabalho foi a desenvolvida por (ALKASASSBEH *et al.*, 2016) a qual consta em sua totalidade por ataques DDOS de quatro tipos:

- SIDDOS
- HTTP Flood
- UDDP Flood
- Smurf

Tabela 1 – Exemplo base de dados DARPA

Número	**Tempo**	**Origem**	**Destino**	**Protocolo**	**Tamanho**[bytes]
1	18:56:12.1386	192.168.0.20	192.168.0.30	TCP	60
2	18:56:12.1391	192.168.0.30	192.168.0.20	TCP	60
3	18:56:12.1588	192.168.0.30	192.168.0.20	TELNET	84
4	18:56:12.2099	192.168.0.20	192.168.0.30	TCP	60
5	18:56:13.0567	192.168.0.20	192.168.0.30	TELNET	69
6	18:56:13.0584	192.168.0.30	192.168.0.20	TELNET	66
7	18:56:13.0626	192.168.0.20	192.168.0.30	TELNET	72
8	18:56:13.0821	192.168.0.30	192.168.0.20	TCP	60

Fonte: Elaborada pelo autor, baseada em (**??**).

A Tabela abaixo mostra os campos do *dataset*

Tabela 2 – Estrutura base de dados (ALKASASSBEH *et al.*, 2016)

Número	**Tempo**
1	Endereço IP origem
2	Endereço IP destino
3	Id do pacote
4	Nó origem
5	Nó destino
6	Tipo de pacote
7	Tamanho do pacote
8	Flags
9	Id da flag
10	Número de sequência
11	Número de pacotes
12	Número de bytes
13	Nome do nó origem
14	Nome do nó destino
15	Entrada de pacote
16	Saída de pacote
17	Taxa de pacotes Recebidos
18	Atraso de nó do pacote
19	Taxa de pacotes
20	Taxa de bytes
21	Tamanho médio do pacote
22	Utilização
23	Atraso de pacote
24	Tempo de envio do pacote
25	Tempo de pacote reservado
26	Primeiro pacote enviado
27	Último pacote reservado

Fonte: Elaborada pelo autor, baseada em (ALKASASSBEH *et al.*, 2016).

Algumas considerações foram tomadas para a análise dessa base de dados:

- Para construir a janela de um segundo, considerou-se a soma de todos os atrasos por pacote:
  - Atraso de nó do pacote.
  - Atraso de pacote.
  - Tempo de pacote reservado.
- A média das taxas dos pacotes foi considerada dentro da janela de um segundo.
- Por ser um dataset composto apenas por ataques, a comparação com o limiar inverte-se para denotar o quanto dois pacotes são parecidos na correlação.

Para o processamento dos dados, o MATLAB foi utilizado

Referências

ALKASASSBEH, M. *et al.* Detecting Distributed Denial of Service Attacks Using Data Mining Techniques. v. 7, 01 2016. Citado 3 vezes nas páginas 3, 10 e 11.

HOQUE, N. *et al.* Real-time DDoS Attack Detection Using FPGA. **Computer Communications**, v. 110, n. Supplement C, p. 48 – 58, 2017. ISSN 0140-3664. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0140366416306442>. Citado 2 vezes nas páginas 7 e 8.