



**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO
TOCANTINS
CAMPUS ARAGUATINS
CURSO SUPERIOR DE LICENCIATURA EM COMPUTAÇÃO**

ELIELTON PEREIRA DE SANTANA

**DETECÇÃO DE *DDOS*: um método de detecção para ataques *Syn Flood*
através da análise de características do tráfego de redes**

**ARAGUATINS - TO
2022**

ELIELTON PEREIRA DE SANTANA

**DETECÇÃO DE *DDOS*: um método de detecção para ataques *Syn Flood*
através da análise de características do tráfego de redes**

Trabalho de Conclusão de Curso apresentado à
Coordenação do Curso superior de Licenciatura
em Computação da Unidade de Araguatins, do
Instituto Federal do Tocantins, como exigência à
obtenção do título de Licenciado, em Computação.

Orientador: Prof. Me. Adeilson Marques da Silva
Cardoso

ARAGUATINS-TO
2022

Dados Internacionais de Catalogação na Publicação (CIP)
Bibliotecas do Instituto Federal do Tocantins

S232d Santana, Elielton Pereira de
 DETECÇÃO DE DDOS : Um método de detecção para ataques
 Syn Flood através da análise de características do tráfego de redes /
 Elielton Pereira de Santana. – Araguatins, TO, 2022.
 25 f. : il. color.

 Trabalho de Conclusão de Curso (Licenciatura em Computação)
 – Instituto Federal de Educação, Ciência e Tecnologia do Tocantins,
 Campus Araguatins, Araguatins, TO, 2022.

 Orientador: Me. Adeilson Marques da Silva Cardoso

 1. Detecção de ataques. 2. DDoS. 3. Syn Flood. I. Cardoso,
 Adeilson Marques da Silva. II. Título.

CDD 004

A reprodução total ou parcial, de qualquer forma ou por qualquer meio, deste documento é autorizada para fins de estudo e pesquisa, desde que citada a fonte.

Elaborado pelo sistema de geração automática de ficha catalográfica do IFTO com os dados fornecidos pelo(a) autor(a).

ELIELTON PEREIRA DE SANTANA

**DETECÇÃO DE *DDOS*: um método de detecção para ataques *Syn Flood*
através da análise de características do tráfego de redes**

Trabalho de Conclusão de Curso apresentado à
Coordenação do Curso superior de Licenciatura
em Computação da Unidade de Araguatins, do
Instituto Federal do Tocantins, como exigência à
obtenção do título de Licenciado, em Computação.

Orientador: Prof. Me. Adeilson Marques da Silva
Cardoso

Aprovado em: ____/____/____

BANCA EXAMINADORA

Prof. Me. Adeilson Marques da Silva Cardoso
Orientador

Instituto Federal de Educação, Ciência e Tecnologia do Tocantins - Campus Araguatins

Prof. Me. Rogerio Pereira de Sousa

Instituto Federal de Educação, Ciência e Tecnologia do Tocantins - Campus Araguatins

Prof. Me. Ancelmo Frank Coêlho Castro

Instituto Federal de Educação, Ciência e Tecnologia do Tocantins - Campus Araguatins

AGRADECIMENTOS

Agradeço a DEUS por me conduzir no caminho correto, e sempre prover condições para as minhas realizações. Agradeço a minha família pelo apoio e por me incentivar a continuar, e buscar sempre o melhor. Ao IFTO – Campus Araguatins e os servidores envolvidos, por proporcionar uma ótima qualidade de ensino. Ao meu orientador pela orientação na construção desse trabalho, e que sempre teve paciência e disposição para me ajudar. Aos meus professores por ter compartilhado seus conhecimentos comigo, certamente teve um grande peso no meu desenvolvimento, e pelo vínculo de amizade que criamos ao longo do caminho. Aos meus amigos e colegas de turma que estiveram juntos nessa caminhada, que por noites e madrugadas nos acudimos nas realizações dos trabalhos, e confraternizamos em momentos de alegria. A todos declaro o meu sincero respeito e admiração.

RESUMO

Diante das variedades de vias comunicacionais, a política de segurança é um fator indispensável para a segurança da informação. Garantir a disponibilidade dos serviços é um dos pilares principais da segurança da informação, e a aferição a este princípio pode causar um grande prejuízo para as grandes organizações, que precisam manter seus serviços disponíveis, online. Este artigo apresenta um método para detecção de ataques de negação de serviço, por meio da análise do tráfego de pacotes, de forma que identifique ataques do tipo *Syn Flood*, baseado na biblioteca *Jpcap*. O protótipo é baseado em assinaturas de ataques conhecidos e foi desenvolvido na linguagem *java*, utilizando a *IDE eclipse* instalado em um sistema operacional *linux*. A identificação é feita baseados nos eventos criados em uma janela de tempo de 30 segundos. Os resultados mostram uma constância no padrão de identificação, e as métricas consolidam a eficácia do método. Contudo, as contribuições desse trabalho podem servir para o desenvolvimento de sistemas, para detecção ataques de negação de serviços.

Palavras-chave: Detecção de ataques. *DDoS*. *Syn Flood*.

RESUMO EM LÍNGUA ESTRANGEIRA

Faced with the variety of communication channels, the security policy is an indispensable factor for information security. Ensuring the availability of services is one of the main pillars of information security, and measuring this principle can cause great harm to large organizations, which need to keep their services available online. This article presents a method for detecting denial of service attacks, through packet traffic analysis, in order to identify Syn Flood attacks, based on the Jpcap library. The prototype is based on signatures of known attacks and was developed in the java language, using the eclipse IDE installed on a linux operating system. Identification is based on events created in a 30 second time window. The results show consistency in the identification pattern, and the metrics consolidate the effectiveness of the method. However, the contributions of this work can serve for the development of systems to detect denial of service attacks.

Keywords: Attack detection. DDoS. Syn Flood.

LISTA DE SIGLAS

DoS	Denial of Service
DDoS	Distributed Denial of Service
IDS	Intrusion Detection System
IFTO	Instituto Federal do Tocantins
TCP	Transfer Control Protocol

SUMÁRIO

1. INTRODUÇÃO.....	10
2. REVISÃO DE LITERATURA.....	12
2.1 Segurança da informação	12
2.2 Ataques DoS e DDoS	12
2.3 SYN Flood.....	13
2.4 Sistema de detecção de intrusão.....	13
2.5 Métodos de detecção.....	14
2.6 Biblioteca para captura de pacotes.....	14
3. TRABALHOS RELACIONADOS.....	15
4. MATERIAIS E MÉTODOS	15
4.1 Modelo proposto	16
4.2 Características adotadas	16
4.3 Implementação	18
4.4 Testes.....	18
5. RESULTADOS E DISCUSSÕES	18
6. CONSIDERAÇÕES FINAIS.....	23
REFERÊNCIAS.....	24

1 INTRODUÇÃO

A era da informação e o avanço dos meios de comunicação, em especial a internet, cada vez mais evidente em nosso cotidiano, tornou mais fácil a troca de informações por vias digitais, possibilitando uma variedade de benefícios para a vida pessoal, acadêmica, profissional e empresarial.

Estas vias digitais podem ser entendidas como qualquer tecnologia digital que possibilite a comunicação, e a disponibilização de serviços online. Segundo Kappes (2019), a maioria dos acessos na *internet* ocorrem por meio de dispositivos móveis, principalmente *smartphones*, muito utilizados para acesso a aplicativos de banco e *sites* de compras dentre outros serviços disponíveis *online*. Sem dispensar computadores de grande porte responsáveis por prover os serviços *online*.

Diante das várias vias comunicacionais, a política de segurança é um fator indispensável para a segurança da informação, pois de fato os tipos de transmissão de informações que utilizam a *internet* como meio, abrem um leque de possibilidades no que se refere a exploração de vulnerabilidades na segurança dos sistemas de informação.

Neste contexto, o Centro de Estudos, Resposta e Tratamento de incidentes de segurança no Brasil (cert.br) destaca alguns ataques que foram reportados por usuários brasileiros. Dentre os principais tipos de ataques que são reportados ao cert.br encontram-se o Scanner de porta, ataques *Web*, Fraudes, *Worm* e o *DoS* – *Denial of Service*, também conhecido como negação de serviço.

Segundo os relatórios do cert.br, o tipo de ataque “*DoS*” obteve no ano de 2018 o segundo maior índice de reportagem de ocorrência, com 23,42%, ficando atrás apenas do Scanner de porta, com 58,77% de ocorrências (CERT.br, 2018). O *DoS* é um ataque que indisponibiliza os serviços e a rede da vítima, e essa indisponibilidade pode gerar muitos prejuízos (MORAIS, 2010).

A segurança da informação é uma premissa básica dentro de um ambiente corporativo, devido ao alto valor que seus ativos possuem. Tendo em vista que todas as transações são feitas eletronicamente por meio da internet, estas, necessitam da garantia de integridade e disponibilidade do serviço.

A melhor maneira de detectar um ataque *DoS*, é através da utilização de um sistema de detecção de intrusão (*Intrusion Detection System - IDS*), que tem como objetivo detectar atividades suspeitas, impróprias, incorretas ou anormal, sendo um elemento importante no arsenal de defesa da organização (NAKAMURA, 2007).

Quando ocorre um ataque a uma determinada rede, o administrador da rede necessita identificar essa ocorrência e descobrir a origem e o destino deste para criar medidas de proteção. E, a utilização de um *IDS* é um item importante para realizar o monitoramento do ambiente, tanto da rede quanto dos servidores, para controle de incidentes maliciosos. (NAKAMURA, 2007).

1.1 Problemática

A segurança da informação é impreterível dentro de uma organização que presa pela disponibilidade dos recursos, dessa maneira como detectar possíveis ataques maliciosos através da análise do tráfego de pacotes da rede?

1.2 Justificativa

Garantir a disponibilidade dos serviços é um dos pilares principais da segurança da informação, onde o ataque *DoS* fere diretamente este princípio e pode surtir maiores efeitos quando realizados de forma distribuída (*Distributed Denial of Service - DDoS*). Dessa forma, saber se estar ocorrendo um ataque *DoS*, vindo de dentro ou de fora é um privilégio para conseguir evitar danos maiores.

Portanto identificar ataques que afetam este princípio é importante para implementação de novas políticas de segurança. O método justifica-se, considerando a capacidade deste em realizar a captura e análise do tráfego da rede, a fim de detectar atividades maliciosas de modo a contribuir para o melhoramento das políticas de segurança e facilitar a intervenção durante um ataque.

1.3 Objetivo

Desenvolver um método de detecção de intrusão para ataques *DDoS* que identifique ataques do tipo *SYN Flood*, baseado na biblioteca *Jpcap*.

O restante do trabalho se organiza como segue. A seção 2 apresenta a revisão de literatura. A seção 3 os trabalhos que contêm relação com esta pesquisa. A seção 4 detalha os materiais e métodos. A seção 5 os resultados obtidos. E a seção 6 a conclusão do trabalho.

2 REVISÃO DE LITERATURA

Esta seção aborda os conceitos envolvidos no desenvolvimento deste artigo, através dos autores que norteia a pesquisa, trazendo uma abordagem conceitual sobre o tema apresentado.

2.1 Segurança da informação

A segurança da informação é algo preferível no processo de comunicação onde trafegam dados sigilosos de uma organização e até mesmo de usuários comuns. Criar formas de assegurar essa comunicação e identificar possíveis ataques, é tema de grandes estudos nessa área que incluem desde técnicas básicas até a utilização de inteligência artificial.

A análise do tráfego de rede é fundamental e necessária quando se pretende aumentar o nível de segurança em ambientes corporativos considerando os variados tipos de ataques existentes. Nesse sentido Cardoso (2018, p. 16) diz que “Existem muitos métodos de intrusão em redes de computadores, os quais configuram uma variedade de ataques que podem comprometer a segurança dos sistemas e a disponibilidades dos dados.”

A maior parte dos ataques não são divulgados e inclui uma grande quantidade de vítimas, a começar de pequenos sites comerciais até instituições educacionais, servidores públicos de bate-papo e organizações governamentais (MOORE, 2006).

2.2 Ataques DoS e DDoS

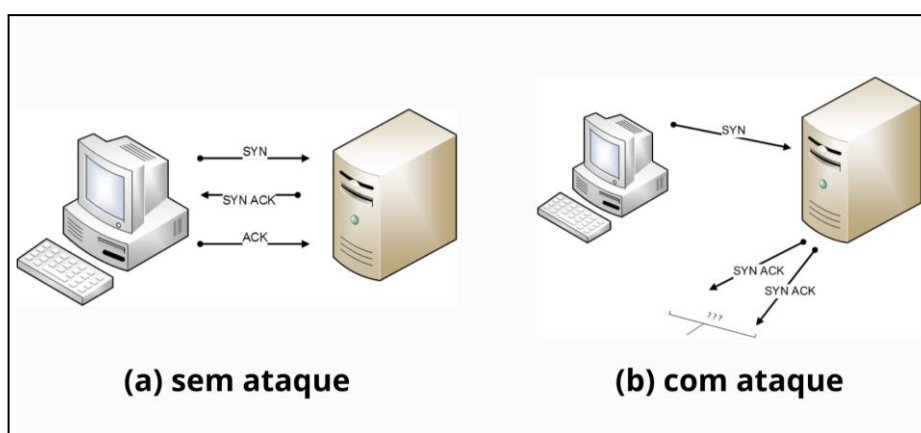
O tipo de ataque *DoS* busca esgotar os recursos da máquina vítima, por meio do envio de fluxo de pacotes, impedindo que ela disponibilize os serviços aos seus usuários legítimos. Neste ataque uma pessoa mal-intencionada utiliza apenas uma máquina para realizar o ataque, e leva um pouco mais de tempo para esgotar os recursos da vítima (MORAES, 2010) e (MEDEIROS, 2015).

Um único host pode causar muitos danos enviando várias requisições a uma vítima, e os atacantes podem ainda, potencializar esse ataque utilizando vários hosts, onde o atacante obtém o controle de vários computadores, sem que os usuários saibam que estão sendo utilizados para um ataque, que são os chamados “Zumbis” ou “escravos”. Esse tipo de ataque é conhecido como ataque de negação de serviço distribuído (*Distributed Denial of Service – DDoS*) onde várias máquinas atacam uma vítima simultaneamente. (MOORE, 2006) e (CARDOSO, 2018).

2.3 SYN Flood

O ataque por inundação *TCP SYN*, conhecido como *Syn Flood*, é um dos ataques de negação de serviço mais utilizados. Esse tipo de ataque explora uma falha do *TCP/IP* por meio do aperto de mão em 3 vias - *Three Way Handshake*, essa falha permite que seja enviado um grande fluxo de pacotes de requisições falsas para um servidor (CARDOSO, 2018). Pode ser visualizado na figura 1, um exemplo onde apresenta dois cenários, um com a comunicação normal e no outro um exemplo de comunicação com ataque.

Figure 1. comunicação sem e com ataque



Fonte: autor

Segundo Moraes (2010, p. 191) o “*SYN Flood*, dentro de *Three Way Handshake* do *TCP/IP*, o *hacker* envia pacotes *SYN* a vítima, mas nunca envia o *ACK* de confirmação do *SYN-ACK*. Assim as sessões vão ficando abertas, consumindo recurso da máquina” consequentemente causando a indisponibilidade do sistema ou serviço. Para isso, o atacante deve enviar uma quantidade grande de pacotes *TCP*, de forma que a vítima utilize toda sua largura de banda para responder as requisições de conexão.

2.4 Sistema de detecção de intrusão

O *IDS* “[...] é um componente essencial em um ambiente corporativo. Sua capacidade de detectar diversos ataques e intrusões auxilia na proteção do ambiente, e sua localização é um dos pontos a serem definidos com cuidado” (NAKAMURA, 2007, p. 264). Este trata-se de um sistema de monitoramento da rede onde realiza a análise do tráfego de pacotes na busca por atividades suspeitas que possam comprometer os serviços utilizados, e saber posicioná-lo na rede é um fator importante.

Os sistemas de detecção podem ser classificados como *HIDS*, *NIDS* e o *Hybrid IDS*:

- ***HIDS*** - *Host-Based Intrusion Detection System*: tipo de Sistema de detecção baseado em *host*. Este, monitora e coleta o tráfego que passa por um servidor que contém informações confidenciais (CARDOSO, 2018). Monitora os arquivos de logs uso da CPU, execução de programas dentre outros processos da máquina (NAKAMURA, 2007).
- ***NIDS*** - *Network-based Intrusion Detection System*: tipo de Sistema de detecção baseado em rede. A detecção é realizando analisando-se as informações contidas no cabeçalho dos pacotes (NAKAMURA, 2007).
- ***HIDS*** - *Hybrid Intrusion Detection System*: tipo de *IDS* que une o *HIDS* e o *NIDS*, monitorando o tráfego endereçado ao próprio sistema (NAKAMURA, 2007).

2.5 Métodos de detecção

Existem diferentes tipos de detecção de ataques por um *IDS*, que podem ser por Assinaturas, por Protocolos ou por Anomalias.

- **Assinatura de Ataques**: a identificação é feita com base em um padrão ou assinatura de ataque que esteja na base de dados, baseia-se no conhecimento dos ataques existentes na base de dados sendo o método mais utilizado pelos *IDS*, onde a detecção é mais rápida e a taxa de falsos positivos é menor (NAKAMURA, 2007).
- **Análise de protocolo**: monitora os protocolos de aplicação para indicar se tem algo de errado (MORAES, 2010).
- **Detecção por anomalias**: realiza o monitoramento da *CPU*, *logs* do sistema operacional, memória e discos na busca por alguma anormalidade, podendo ser um ataque ou não, sendo uma das metodologias mais complexo para detecção (MORAES, 2010).

2.6 Biblioteca para captura de pacotes

Levando em consideração a necessidade de captura de pacotes que trafegam na rede, para que seja possível a análise, apresenta-se a seguir a biblioteca de código aberto *Jpcap* utilizada para tal.

Biblioteca Jpcap: Jpcap é uma biblioteca de código aberto para a captura do tráfego da rede, que consiste em um conjunto de classes e interfaces *java*, onde implementa chamadas para a biblioteca do sistema *Libpcap* através do *JNI* (*Java Native Interface*) (KUMAR, 2014). O *Jpcap* oferece dentre outras as seguintes facilidades:

- Captura de pacotes em tempo real;
- Armazena e ler pacotes capturados em arquivos *offline*;
- Detecta automaticamente os tipos de protocolos e gera objetos *Java* para (*Ethernet, IPv4, IPv6, ARP/RARP, TCP, UDP* e pacotes *ICMPv4*);
- Filtra os pacotes com base em regras especificadas pelo usuário;

3 TRABALHOS RELACIONADOS

O STARK é um sistema de detecção de ataques “DoS” que analisa o comportamento do tráfego da rede baseado no tamanho do pacote, a análise é feita em janelas de tempo em que cada janela é identificada anomalias no tráfego dos pacotes. O sistema realiza a predição dos ataques utilizando a biblioteca *Early Warnig Signats (EWS)* implementada em R. (PELLOSO, 2018).

Oliveira (2007) apresenta um sistema de detecção e prevenção de ataques *DDoS* em uma arquitetura modularizada. A forma de identificação dos ataques é baseada no histórico de conexões, onde dispositivos já conectados, tenham preferência no uso dos recursos.

Laufer, Velloso e Duarte (2005) propõe um sistema para ataques *DoS*, em que realiza o rastreamento de *IPs* forjados, baseado na teoria do filtro de bloom para analisar o tráfego de pacotes da rede.

As principais diferenças deste trabalho com os trabalhos apresentados aqui, está na forma de identificação do ataque, embora ambos se baseiam nas características do pacote *TCP*, este trabalho propõe a identificação de ataques em tempo real.

4 MATERIAIS E MÉTODOS

Nesta Seção é apresentado o modelo proposto para detecção do ataque, bem como, os materiais utilizados para o desenvolvimento do protótipo e as características adotadas para identificação do ataque.

4.1 Modelo proposto

O modelo proposto baseia-se na detecção de ataques por assinatura, onde os ataques podem ser identificados em tempo real, com base em assinaturas conhecidas. O modelo está estruturado da seguinte forma: Captura dos pacotes; Análise com base na assinatura do ataque; E a emissão de um alerta de ataque. A figura 2, representa a estrutura do modelo.

Figura 2: estrutura



Fonte: autor

O primeiro passo faz a captura de um pacote, em seguida é feita a análise para colher as características do pacote, após o tempo encerrar, é determinado se as características do fluxo de pacote consistem em um ataque ou não.

4.2 Características adotadas

O cabeçalho de um pacote apresenta a informação do *Three Way Handshake*, informando se é um pacote de requisição ou de resposta. No tráfego normal existe a presença das 3 flags: SYN, SYN/ACK e ACK, o que não ocorre no tráfego com ataque, em que há uma redução na incidência do pacote ACK. Na tabela 1 a seguir pode ser visualizado um exemplo.

Tabela 1

Tráfego normal (120 pacotes)			Tráfego com ataque (120 pacotes)		
SYN	SYN/ACK	ACK	SYN	SYN/ACK	ACK
40	40	40	60	60	0

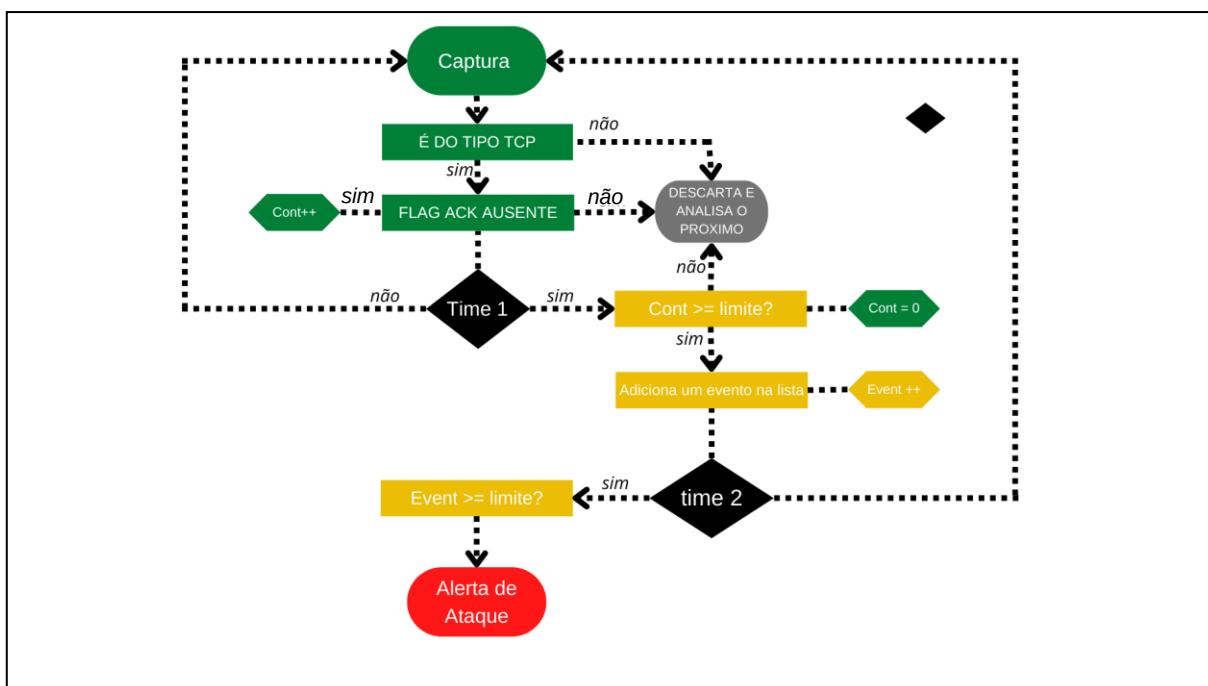
Fonte: Autor.

Os dados na tabela não representam uma situação real de tráfego de pacotes, é apenas um exemplo visual do que aconteceria no tráfego normal e no tráfego com ataque. Com este exemplo pode ser observado as mudanças no tráfego de pacotes, com a ausência do pacote ACK.

De acordo com as especificações da Cisco (2022), para que o atacante consiga exaurir os recursos da vítima, através de inundação de *TCP SYN*, é preciso enviar tráfego de pacotes a uma taxa de 200 pacotes por segundo fazendo com que os usuários legítimos não consigam estabelecer uma comunicação com o servidor. É com base nessa informação, que o modelo foi formulado para gerar os alertas.

A sintaxe do protótipo, conta com um laço que se repete durante 30 segundos. Durante esse tempo, o segundo laço com duração de um 1 segundo, verifica se o pacote é do tipo *TCP* ou não, e imprime as informações do pacote na tela. Em seguida é verificado se a *flag ACK* estar ausente, caso sim, incrementa a variável contadora de pacotes. Após o tempo determinado, o valor é calculado e comparado com a quantidade de pacotes que caracterizam um ataque por inundação *TCP SYN*, para determinar se há a existência de um ataque ou não. Podemos entender melhor observando o fluxograma na figura 3.

Figura 3: fluxograma do algoritmo



Fonte: autor

Nesse contexto, o método proposto, analisa a quantidade de pacotes em um espaço de tempo pré-definido, para determinar a ocorrência de um ataque por inundação. O código utilizado, extrai as características do pacote e incrementa os contadores, caso a condição seja satisfeita. Após a janela de tempo atingir o limite definido, as variáveis contadoras são analisadas, para determinar se o tráfego indica um ataque ou não.

5 RESULTADOS E DISCUSSÕES

Nesta seção são apresentados os aspectos de implementação do protótipo, os testes e a análise dos resultados obtidos.

5.1 Implementação

O protótipo do método de detecção, foi desenvolvido utilizando a linguagem *java*, através da *IDE Eclipse*, instalados no sistema operacional *linux*. Para o funcionamento da captura de pacotes, foi necessário a instalação do *JDK-8*, *libpcap*, e adicionar a *jpcap* dentro do projeto *java*.

A seguir na figura 4, é apresentado um exemplo do código em *java*.

Figure 4. Trecho do código que analisa os pacotes

```
while(time2 < 1000) {
    p = captor.getPacket();
    if(p instanceof TCPpacket){
        TCPCont++;
        TCPpacket tcp = (TCPpacket) p;
        System.out.println("TCP - " + "Origem: " + tcp.src_ip.getHostAddress()
            + " porta:" + tcp.src_port + " Destino: " + tcp.dst_ip.getHostAddress()
            + " porta:" + tcp.dst_port + " Tamanho = " + tcp.length + " bytes " + "Flag Syn: "
            + tcp.syn + "Flag: " + tcp.ack + " Total de Pacotes = " + TCPCont);

        if(tcp.syn == true) { Cont++; System.out.println("Cont: " + Cont);}
    }
}
```

Fonte: autor

A figura 4 apresenta um exemplo da lógica de caracterização do tráfego da rede, em que se baseia na quantidade de pacotes trafegando, e a informação das *flags* do pacote, com as informações do *Three Way Handshake*.

5.2 Testes

Os testes foram realizados em uma rede isolada, para que os resultados não tivessem influência da rede externa e, por sua vez, os ataques não refletissem na rede real, prejudicando o funcionamento da mesma, onde pode-se determinar a eficácia do modelo de detecção. Através da ferramenta *hping3*, foram realizadas as

simulações de tráfegos e ataques do tipo *TCP*. Um exemplo da simulação de ataque com o *hping3* é demonstrado na figura 6.

Figure 6. Código hping3

```
hping3 -flood -syn -c 100000 192.168.0.100 192.168.0.101
```

Fonte: autor.

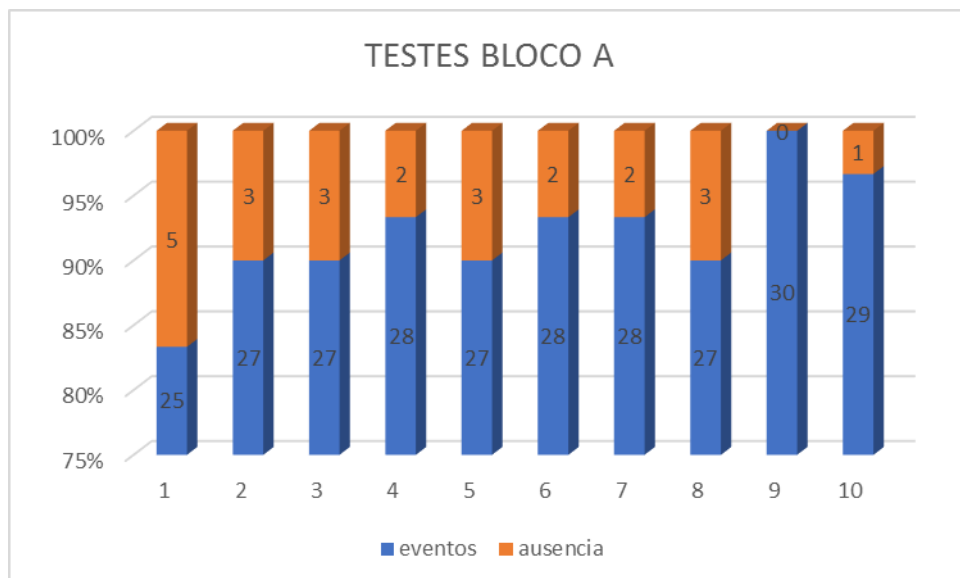
O código da figura 6, envia tráfego de pacotes *TCP* a um endereço determinado pelo atacante. Neste exemplo é enviado uma sequência de requisições ao máximo de pacotes por segundos com origem no endereço 192.168.0.101, destinados ao endereço da vítima 192.168.0.100.

5.3 Análise dos testes

Os resultados foram obtidos em 3 blocos de teste: A, B e C, cada bloco foi analisado em 10 janelas de tempo com 30 segundos cada. Os blocos A, B e C, foram expostos a ataques em taxas diferentes para observar se o padrão de detecção iria mudar. O tráfego é analisado a cada 1 segundo, dessa forma, em uma janela de tempo de 30 segundo, deve haver 30 eventos de alertas, durante a exposição do protótipo a um ataque, para que se considere 100% de identificação.

O gráfico a seguir apresenta os dados dos testes realizados no bloco A, com exposição ao ataque por inundação *TCP SYN*, em taxa máxima de pacotes por segundo.

Gráfico 1: testes bloco A

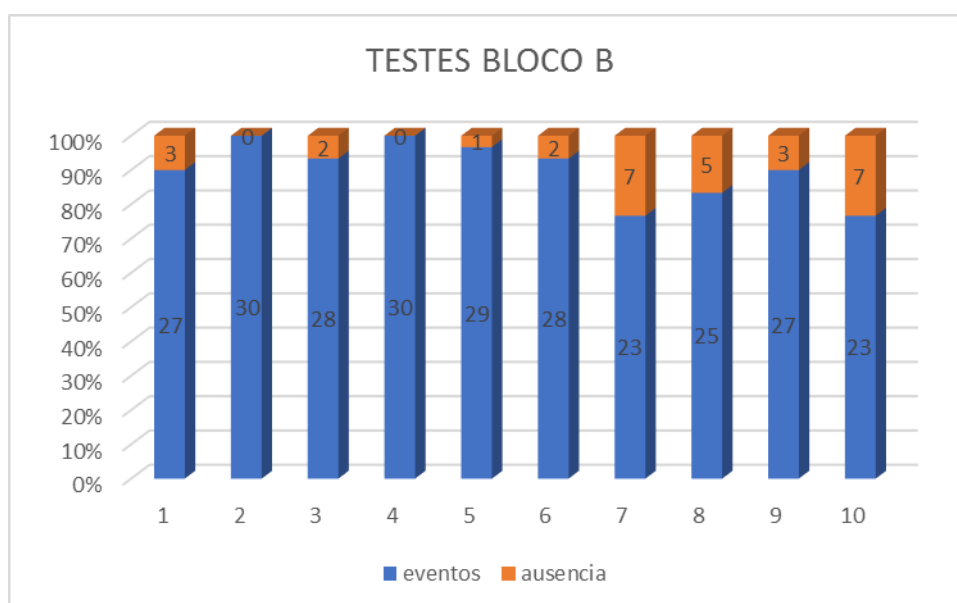


Fonte: autor.

No gráfico são apresentadas as janelas de tempo em sequência numérica, e podemos observar que a janela de tempo 1, foi a menor com a emissão de 25 eventos, aproximadamente 83% de identificação, e 17% de casos que deveriam constar na lista, porém não foram identificados. Neste bloco temos as maiores altas nas janelas 9, com 100% de identificação, e a 10 com aproximadamente 96% de identificação.

A seguir apresenta-se os dados obtidos com os testes do bloco C, que não se diferencia muito os padrões de identificação. Neste foi realizado com uma taxa média de requisições em ataque, especificando no comando o envio de no mínimo 1000 pacotes por segundo.

Gráfico 2: testes bloco B

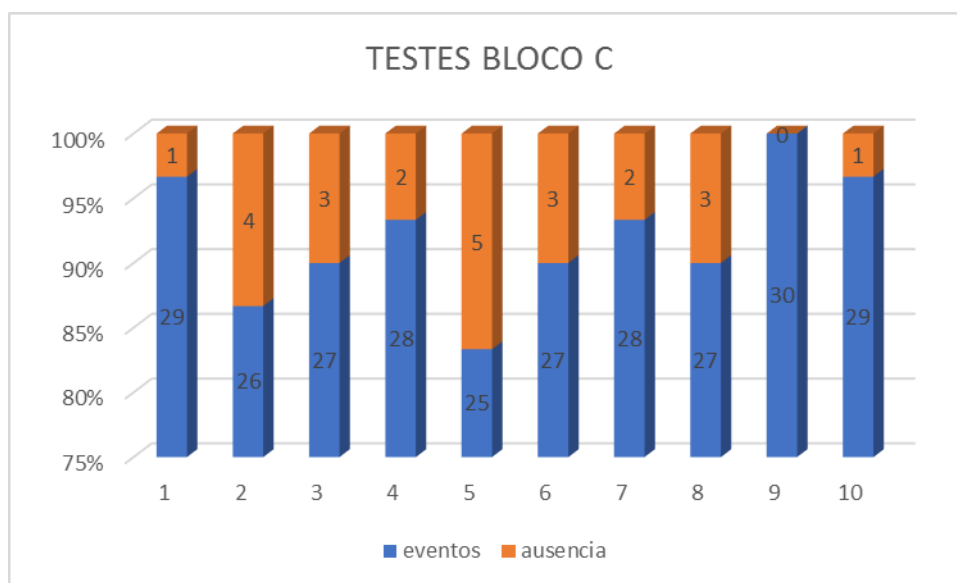


Fonte: autor.

Como pode ser observado, as janelas de tempo 7 e 10, são as menores desse bloco, com aproximadamente 72% de eventos identificados. Em comparação com o gráfico do bloco A, somente essas duas janelas de tempo ficaram com uma taxa menor de identificação. Contudo, as demais janelas permaneceram com uma taxa acima de 80% de identificação.

Nos testes do bloco B, a taxa mínima de envio de tráfego por segundo, foi reduzida a no mínimo 200 pacotes por segundo,

Gráfico 3: testes bloco C



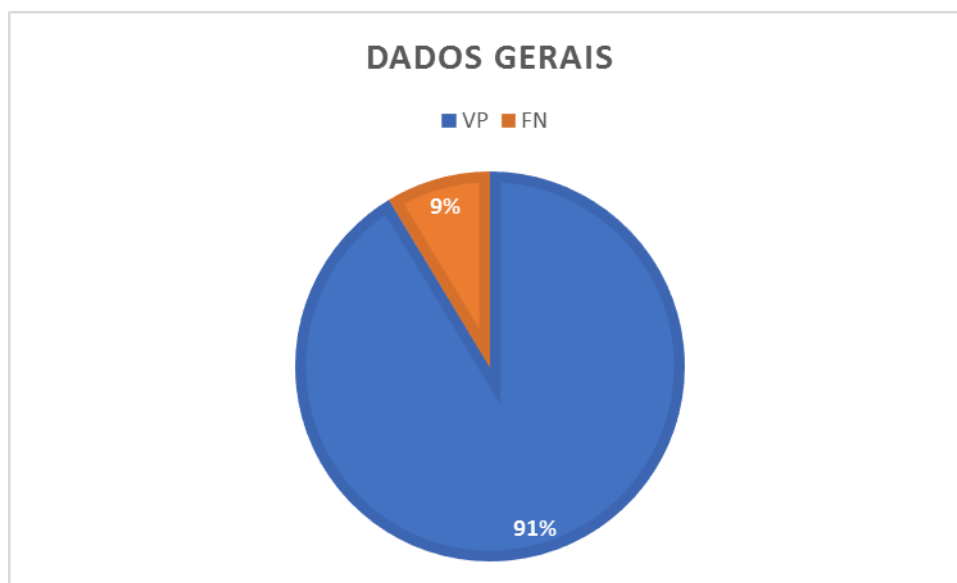
Fonte: autor.

Neste bloco de teste observa-se que houve muitas mudanças nas porcentagens de identificação. A menor taxa de identificação, a que costuma na janela de tempo 5, manteve o valor igual a janela de tempo 1 do bloco A, e o padrão de identificação em relação aos demais blocos também se acemelham.

Dentre todos os testes realizados, os casos que não chegaram aos 100%, devem-se ao controle de tempo dentro do código, pois o tempo baseia-se na execução dos ciclos de análise, e durante os testes foi possível observar um pequeno atraso na finalização do ciclo que determina a emissão de um evento de alerta, de aproximadamente 12 milésimos de segundo, o que influencia na contagem de tempo final da janela de tempo de 30 segundos.

Os dados gerais de todos os testes, são apresentados no gráfico a seguir, pontuando as taxas de verdadeiros positivos, e falsos negativos, que trata-se, respectivamente, das vezes em que o protótipo realizou a identificação das mudanças do tráfego na rede, criando um evento de alerta, baseados nas características adotadas por este método e as vezes em que não houve identificação dessas características ou não houve identificação do tráfego.

Gráfico 4: dados gerais



Fonte: autor.

Os dados gerais, mostram as taxas de acertos, constatando a incidência de verdadeiros positivos (VP) em 91% das vezes, e ausência de identificação, constatando os falsos negativos (FN) em 9%. Essas métricas mostram o potencial deste método, como proposta de identificação de ataques *DDoS*,

Para fins de observação e validação do modelo, o código que determina a ultrapassagem do limite de pacotes por segundo, imprime na tela um “evento de alerta”. Contudo a determinação de um ataque em andamento é concretizada quando o número de alertas ultrapassa o limite definido dentro da janela de tempo.

Configura-se um ataque em andamento, a emissão de no mínimo 10 eventos de alerta, dentro da janela de tempo definida. O caso em que fique abaixo de 10 alertas, considera-se que o fluxo de pacotes estar normal, onde mesmo que tenha um atacante enviando tráfego junto com o fluxo normal da rede, enviará em taxa bem baixa e não conseguirá exaurir os recursos da máquina vítima. E por conseguinte, este resolver enviar um fluxo maior de pacotes, haverá uma quantidade maior de eventos, configurando-se um ataque em andamento.

6 CONSIDERAÇÕES FINAIS

A segurança da informação é impreterível dentro de uma organização que presa pela disponibilidade dos recursos, dessa maneira detectar possíveis ataques de negação de serviço através da análise do tráfego de pacotes da rede, contribui significativamente para a proteção dos ativos dela.

Este trabalho apresentou um método de detecção de ataque *Syn Flood*, baseado na análise das características do tráfego de rede. Com base na captura de pacotes utilizando a biblioteca *Jpcap*, foi possível implementar um protótipo em java e criar regra para determinar a ocorrência de um ataque baseado em assinatura.

Contudo, o processo de ataque se inicia com um scanner, para reconhecimento dos recursos e os serviços disponibilizados. Embora haja a possibilidade de executar um ataque de grande porte, o atacante pode reduzir a quantidade de tráfego enviado, baseado nos recursos que a máquina vítima possui. Dessa forma o atacante não precisa enviar uma grande quantidade de tráfego para exaurir os recursos, sendo que a capacidade de resposta da vítima é baixa.

Para tanto é preciso analisar a configuração da rede e os padrões de tráfego desta, e configurar as métricas de identificação baseada nessa análise. O Cert.br propõe alguma maneira de lidar com ataques *DoS* que se inicia com a preparação para tratar essas ocorrências, em casos de ataques futuros. Algumas das recomendações é identificar a média de tráfego da rede, tanto no quantitativo de pacotes quanto no tamanho dos dados no pacote para registrar o que é normal ou não dentro da rede (CERT.br, 2016). Dessa forma o modelo pode ser configurado com os parâmetros de cada rede, para se adequar a cada ambiente.

Portanto, este trabalho pode contribuir significativamente com o desenvolvimento de sistemas, para detecção ataques de negação de serviços. E embora este trabalho aborde a detecção de ataques *Syn Flood*, baseado em assinatura, o método proposto pode ser utilizado também, para implementar sistemas que detectem outros tipos de ataques e que as características dos ataques possam ser dinamizadas conforme o usuário necessite.

REFERÊNCIAS

- CARDOSO, Adeilson Marques da Silva et al. **CEPIDS: Um IDS baseado no Processamento de Eventos Complexos para Internet de Coisas**. 2018. Disponível em:< <https://tedeabc.ufma.br/jspui/bitstream/tede/2360/2/Adeilson%20Marques.pdf>> Acesso em: 25 maio 2019.
- CERT, B. R. **Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil**. 2018. Disponível em:< <https://www.cert.br/stats/incidentes/> Acesso em: 25 jun. 2019.
- CERT, B. R. **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)**. 2016. Disponível em:<<https://cert.br/docs/whitepapers/ddos/>> Acesso em: 25 nov. 2022.
- CISCO. **Firepower Management Center Configuration Guide**. 2022. Disponível em:< https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/threat_defense_service_policies.html#id_71090> Acesso em: 20 julho 2022.
- KAPPES, Leonardo Henrique. **Segurança da informação na internet: por que se preocupar?**. 2019. Disponível em:<<https://itmidia.com/seguranca-da-informacao-na-internet-por-que-se-preocupar>> Acesso em: 26 jun. 2019.
- KUMAR, G. Dileep et al. **Using jpcap api to monitor, analyze, and report network traffic for ddos attacks**. In: 2014 14th International Conference on Computational Science and Its Applications. IEEE. 2014 p. 35-39. Disponível em:< <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6976660>> Acesso em: 26 jun. 2019.
- LAUFER, Rafael P.; VELLOSO, Pedro B.; DUARTE, O. C. M. B. Um novo sistema de rastreamento de pacotes ip contra ataques de negação de serviço. In: **XXIII Simpósio Brasileiro de Redes de Computadores-SBRC'2005**. 2005. Disponível em:< <https://www.gta.ufrj.br/~rlaufer/publications/sbrc05.pdf>> Acesso em: 25 set. 2022.
- MEDEIROS, Tiago Fonseca. **Ataque distribuído de negação de serviço por reflexão amplificada usando Simple Network Management Protocol**. 2015. Disponível em:< <http://bdm.unb.br/handle/10483/11152>> Acesso em: 25 jun. 2019.
- MOORE, David et al. (2006) Inferring internet denial-of-service activity. **ACM Transactions on Computer Systems (TOCS)**, v. 24, n. 2, p. 115-139. Disponível em:< http://delivery.acm.org/10.1145/1140000/1132027/p115-moo-re.pdf?ip=200.137.132.10&id=1132027&acc=ACTIVE%20SERVICE&key=344E943C9DC262BB%2E9AA1CD66052D340C%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1561560384_1d964a61b4c37ed63219e9b32e41ad3f> Acesso em: 26 jun. 2019.

MORAIS, Alexandre Fernandes de. **Segurança em Redes: fundamentos**. 1. Ed. -- São Paulo: Érica. 2010.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. -- São Paulo: Novatec Editora. 2007.

OLIVEIRA, Luis et al. Avaliação de proteção contra ataques de negação de serviço distribuídos (DDoS) utilizando Lista de IPs Confiáveis. In: **Anais do VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. SBC, 2007. p. 177-190. Disponível em: <<https://sol.sbc.org.br/index.php/sbseg/article/view/20926/20752>> Acesso em: 25 set. 2022.

PELLOSO, Mateus et al. Um sistema autoadaptável para predição de ataques ddos fundado na teoria da metaestabilidade. In: **Anais do XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. SBC, 2018. p. 726-739. Disponível em: <<https://sol.sbc.org.br/index.php/sbrc/article/view/2454/2418>> Acesso em: 25 set 2022.