MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA

Felipe da Costa Rasinhas
Pedro Henrique Santos Ferreira

ESTUDO DE ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO

Rio de Janeiro
2012

INSTITUTO MILITAR DE ENGENHARIA

Felipe da Costa Rasinhas
Pedro Henrique Santos Ferreira

ESTUDO DE ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO

Iniciação à Pesquisa apresentada ao Curso de Graduação de Engenharia de Computação como requisito parcial para a obtenção do título de Engenheiro.

Orientador: Anderson Fernandes Pereira dos Santos

Rio de Janeiro
2012

INSTITUTO MILITAR DE ENGENHARIA
Praça General Tibúrcio, 80 – Praia Vermelha
Rio de Janeiro - RJ CEP: 22290-270

621.39
R225e

Rasinhas, Felipe da Costa. Ferreira, Pedro Henrique Santos.
Estudo de Ataques Distribuídos de Negação de Serviço / Felipe da Costa Rasinhas, Pedro Henrique Santos Ferreira; orientado por Anderson Fernandes Pereira dos Santos. -Rio de Janeiro: Instituto Militar de Engenharia, 2012.

34f: il.

Projeto de Iniciação à Pesquisa. - Instituto Militar de Engenharia. -Rio de Janeiro, 2012.

1. Engenharia de Computação. 2. DoS. 3. DDoS. I. Rasinhas, Felipe da Costa. II. Ferreira, Pedro Henrique Santos. III. Santos, Anderson Fernandes Pereira dos. IV. Instituto Militar de Engenharia.

CDD 621.39

INSTITUTO MILITAR DE ENGENHARIA

PEDRO HENRIQUE SANTOS FERREIRA

FELIPE DA COSTA RASINHAS

ESTUDO DE ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO

Iniciação à Pesquisa do Curso de Engenharia de Computação do Instituto Militar de Engenharia, como requisito para colação de grau no curso de Engenharia de Computação.

Orientador: Anderson Fernandes P. dos Santos

Aprovada em 25 de Junho de 2012 pela seguinte Banca Examinadora:

_____

Maj QEM Anderson Fernandes P. dos Santos, D.Sc., do IME – Presidente

_____

Maj QEM Claudio Gomes de Mello, D.C. , do IME

_____

Maj QEM Julio Cesar Duarte, D.C. , do IME

Rio de Janeiro

2012

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

DoS	*Denial of Service*
DDoS	*Distributed Denial of Service*
IP	*Internet Protocol*
CPU	*Computer Processing Unit*
CIAC	*Computer Incident Advisory Capability*
UDP	*User Datagram Protocol*
ICMP	*Internet Control Message Protocol*
HTTP	*Hypertext Transfer Protocol*
DNS	*Domain Name System*
WWW	*World Wide Web*
TCP	*Transmission Control Protocol*
RR	*Resource Records*
FTP	*File Transfer Protocol*
SMTP	*Simple Mail Transfer Protocol*
SYN	*Synchronize*
ACK	*Acknowledge*
VoIP	*Voice over Internet Protocol*
SIP	*Session Initiation Protocol*
DRDoS	*Distributed Reflector Denial of Service*

RESUMO

Os ataques distribuídos de negação de serviço são um método novo, iniciado no final da década de 90, para explorar vulnerabilidades encontradas na rede. Este trabalho consiste de um estudo sobre esses ataques, seus tipos específicos e do tráfego de redes, além da modelagem desses tipos de ataque. A modelagem é um ponto importante na detecção de ataques distribuídos, pois torna possível a analise do comportamento da vítima durante um ataque.

ABSTRACT

The distributed denial of service attacks are a new method, initiated at the end of 90’s to exploit network vulnerabilities. This research consists in studying DDoS and network traffic, in order to model the attacks. The modeling is an important aspect on the detection of distributed attacks, because it makes it possible to analyze the victim’s behavior during the attack.

1 INTRODUÇÃO

O objetivo original da *Internet* era possibilitar uma conexão aberta e escalável entre pesquisas e projetos educacionais. Dessa forma, a segurança foi deixada em segundo plano e, apesar de atingir os objetivos iniciais, a *Internet* tornou-se um ambiente muito vulnerável à ataques de agentes malicioso. O primeiro incidente de segurança observado foi em 1988, quando um aluno universitário utilizou um *worm* na *Internet*. Esse programa coletava informações dos usuários e se replicava, disseminando-se para outras máquinas utilizando falhas em *softwares*. Esse ataque inutilizou milhares de computadores ao redor do mundo na época, porém a *Internet* não era tão importante para o mundo como atualmente. Com o passar dos anos, o número de usuários cresceu exponencialmente e, junto com isso, o número de ataques também aumentou rapidamente.

A estrutura do protocolo IP permite que usuários maliciosos falsifiquem seu endereço, dificultando a identificação da fonte de possíveis ataques (IP *Spoofing*). Além disso, cabe ao servidor verificar a legitimidade dos dados que chegam até ele. Essa legitimação é mais custosa para a máquina do que o envio de requisições. Com isso, o envio de muitas requisições em um curto espaço de tempo pode sobrecarregar o servidor e fazer com que o serviço prestado pelo mesmo fique indisponível. Além dessa, existem outras falhas que podem ser utilizadas por usuários mal intencionados para paralisar serviços na internet. Esse tipo de incidente é conhecido como ataque de negação de serviço (DoS-*Denial of Service*).

Os ataques DoS impedem a continuidade da prestação de serviços da vítima, podendo causar grandes perdas financeiras aos alvos. Por exemplo, se um site de *e-commerce* atacado ficar fora do ar por algumas horas, haverá perdas, pois os clientes ficariam impossibilitados de fazer transações, além das perdas devido à imagem.

A defesa contra ataques DoS pode ser feita através de medidas preventivas, que visem impedir que ele ocorra; detecção dos ataques, que busca descobrir que está acontecendo um ataque; identificação da fonte, que tem por objetivo descobrir de onde os pacotes estão sendo enviados; e reação ao ataque, que visa eliminar ou reduzir os efeitos do ataque.[1]

1.1 Objetivo

Este trabalho é constituído de uma pesquisa bibliográfica sobre ataques DoS, DDoS (*Distributed Denial of Service*) e *Botnet*, estudando detalhadamente todos os tipos de ataques. Em seguida, será realizada uma pesquisa bibliográfica sobre tráfego de *Internet*. A finalidade principal do estudo é a realização de uma proposta de modelagem para os tipos de ataques.

1.2 Motivação

Na atualidade, a *Internet* é o meio de comunicação mais importante do mundo. Nela são realizadas diariamente inúmeras compras, transações bancárias, além de fluxo de dados confidenciais, tornando a segurança e a disponibilidade nesse meio um fator primordial. Por isso, faz-se necessário a análise e modelagem de possíveis maneiras que possam impedir a execução confiável destes serviços, além do estudo de possíveis métodos para impedir essas ações maliciosas.

Recentemente sites de vários bancos brasileiros foram vítimas de ataques, durante 5 dias, por *hackers* do grupo *Anonymous*. Os ataques, que começaram no dia 30/01/2012 e foram finalizados no dia 03/02/2012, tinham como alvos os sites dos maiores serviços de *internet banking* do Brasil, dentre eles, os serviços do Itaú, Bradesco, Banco do Brasil, HSBC, Citibank e da Caixa Econômica Federal, além do site da Febraban (Federação brasileira dos bancos).[2]

1.3 Metodologia

O trabalho consistirá de uma pesquisa bibliográfica sobre DoS, DDoS, *Botnet* e tráfego de *Internet*, utilizando como referências iniciais [1] e [13]. Em seguida, será realizado um estudo específico de cada tipo de ataque DDoS existente, ainda utilizando [1] e acrescentando como referências [9] e [10]. Por último será feita a proposta de

modelagem de cada tipo de ataque, para que possa ser estudado mais detalhadamente o problema.

1.4 Organização da Monografia

O trabalho está distribuído em uma seção abordando o assunto dos ataques DoS e DDoS, abordando um histórico de ataques que ocorreram na *Internet* e outra subseção com uma explicação sobre *botnets*. Detalhamos cada tipo de ataque na subseção seguinte e finalizamos a seção 2 com uma explicação sobre tráfego de *Internet*. Na seção 3 é apresentado a proposta da modelagem dos tipos de ataques presentes na seção 2. O relatório é finalizado com uma conclusão do trabalho na seção 4.

2 ATAQUES

2.1 Ataques DoS

Ataques de Negação de Serviço (DoS) tem por objetivo impedir que seus usuários legítimos acessem algum tipo de serviço. No contexto da *Internet*, esses ataques negam o acesso a algum recurso fornecido por alguma aplicação ou servidor. Esse tipo de ataque normalmente é feito de duas maneiras, utilizando uma vulnerabilidade no protocolo ou em uma aplicação, ou então consumindo recursos da vítima.

No caso do primeiro método, houve o caso do *Ping of Death*, que é um ataque no qual o agente malicioso utiliza o fato do protocolo IP suportar um pacote com tamanho máximo de 65535 bytes.

Como exemplo do segundo método, temos a situação em que ocorre o envio de um volume muito alto de tráfego que apenas serviriam para ocupar os recursos da vítima que poderiam servir ao tráfego legítimo de dados. Caso a vítima não consiga realizar uma intervenção nesse ataque, seus recursos ficarão sobrecarregados, podendo causar um impedimento nos seus serviços.[1]

2.2 Ataques DDoS

Os ataques DoS podem ser efetuados em uma escala maior, ou utilizando-se de uma arquitetura diferente (máquinas mestres e zumbis), sendo feito por mais de uma fonte e, quando isso ocorre, recebe o nome de Ataques Distribuídos de Negação de Serviço (DDoS – *Distributed Denial of Service*). A utilização de mais de uma fonte dificulta ainda mais a autenticação do tráfego de dados pelos servidores.

De acordo com a CIAC (*Computer Incident Advisory Capability*), o ataque DDoS documentado mais antigo ocorreu em agosto de 1999 quando um grupo de mais de 100 computadores tentou sobrecarregar uma máquina da Universidade de Minnesota [3].

Os pacotes de dados enviados pelos atacantes são similares aos pacotes enviados por usuários legítimos, o que dificulta a ação de defesa. O envio de dados normalmente é grande e rápido o suficiente para consumir todos os recursos disponíveis do alvo, ou até mesmo pacotes pequenos que são enviados de milhares de fontes simultaneamente e com uma alta velocidade atingem o mesmo objetivo. Dessa forma, a análise para legitimar o tráfego demora mais do que o envio de pacotes não legítimos, afetando a capacidade da CPU de um servidor, largura de banda. Ao atingir esses recursos, usuários legítimos desses sistemas ficam impedidos de acessá-los.

No início do século XX, esse tipo de ataque se popularizou devido ao aumento das capacidades dos computadores, que inviabilizava o uso de ataques DoS, e à sua grande capacidade de realizar um ataque de alta escala. Um dos maiores ataques ocorreu em fevereiro de 2000, quando, durante uma semana, varios sites (*Yahoo, eBay, CNN,* e outros) foram atacados por um grupo de *hackers* [4]. Outro empreendimento que teve grandes perdas devido à ataques como esse foi o banco suíço PostFinance que foi o principal alvo da "*Operation Payback*" efetuada pelo grupo de *hackers* "*Anonymous*", como forma retaliação ao congelamento da conta do porta-voz da WikiLeaks [5].

Além disso, ataques DDoS já foram utilizados como instrumentos de guerra cibernética; em 2007 e 2008, a Rússia foi acusada de executar uma série de ataques contra a Estônia e a Geórgia respectivamente. Durante os ataques, organizações como bancos, jornais e emissoras tiveram seus serviços imensamente prejudicados [6].

Outro ataque de escala global ocorreu em outubro de 2002, quando 7 dos 13 servidores de DNS raiz foram desativados por cerca de 1 hora devido a um ataque DDoS. Apesar disso, os danos desse ataque não chegaram a ser perceptíveis pelos usuários normais da *Internet* [7].

Esses ataques normalmente são iniciados a partir de um controle prévio de muitas máquinas a partir do atacante. Essas máquinas infectadas são chamadas de computadores zumbis. Esses zumbis são afetados a partir de vulnerabilidades em seus sistemas ou então uma página da *web* ou *email* malicioso, que são atacados e dominados pelos responsáveis pela realização do ataque DDoS. Após o controle de diversas máquinas, é enviada uma mensagem de comando a todas essas máquinas para que sejam enviados pacotes de dados para o alvo. Na figura 2.1 pode ser observado o esquema de controle entre os atacantes e os zumbis. Os atacantes (*Botmasters*) invadem os computadores, transformando-os em zumbis (*Bots*). Esses computadores realizam

ataques para a vítima a partir de um comando recebido pelos computadores mestres.

A utilização de máquinas zumbis, visto que torna-se quase impossível saber a real fonte das informações, pois os verdadeiros atacantes estão se escondendo atrás das máquinas dominadas.

Alguns fatores ajudam para que esse tipo de ataque tenha uma grande eficiência e para que seja muito difícil impedí-lo. O volume de dados gerados por esses ataques pode atingir o valor de 10 Gb/s, ultrapassando a capacidade da grande maioria de serviços da *Internet*. Além disso, as informações enviadas em um ataque podem parecer muito próximas de um dado legítimo, chamada de *Flash Crowds*. Com isso, um método de defesa a partir da análise do tipo de dados poderia negar serviços a um usuário autêntico confundindo-o com um usuário malicioso.

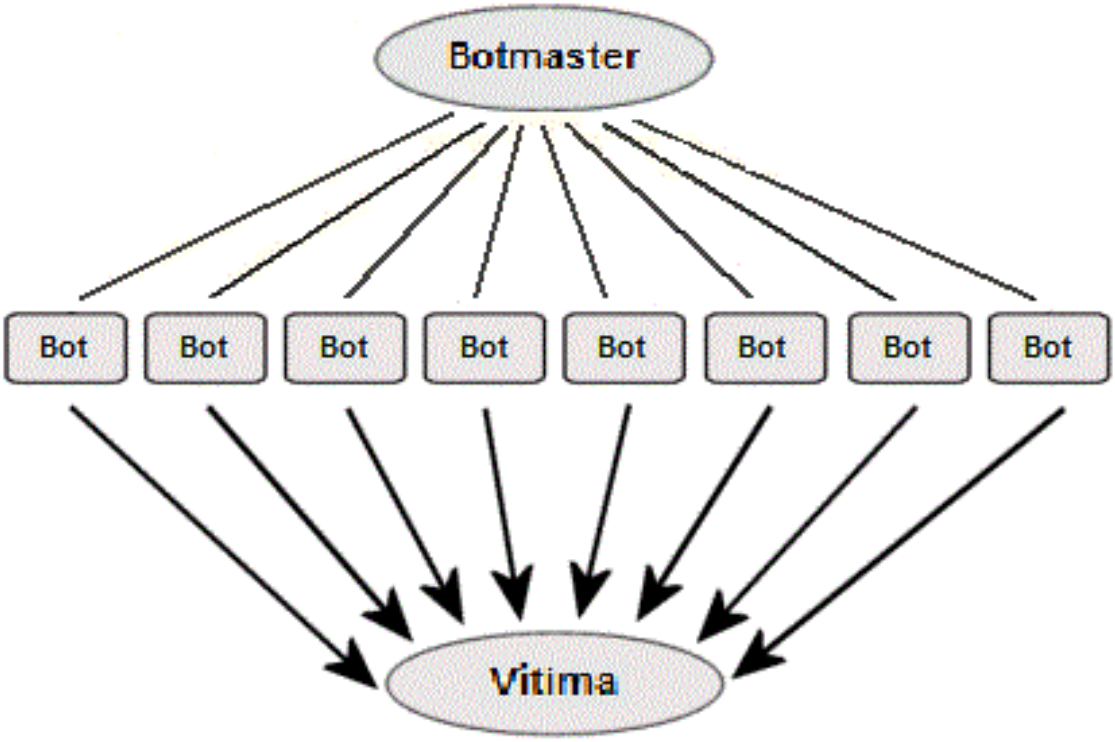


FIG 2.1 – Esquema de ataque DDoS

2.3 *Botnet*

Atualmente, o domínio remoto de máquinas, para serem usadas como fonte de dados maliciosos, não tem sido muito complicado devido à *softwares* modernos que facilitam esse acesso. Os atacantes podem controlar esses computadores de duas formas. O método direto é feito aproveitando-se da vulnerabilidade de algum software desse computador. Hoje em dia, as redes estão muito vulneráveis e essa vulnerabilidade vem crescendo com o decorrer dos anos, como mostrado na figura 2.2 [1]. Dessa forma, esse método vem sendo muito utilizado e está se tornando cada vez mais freqüente. O outro método seria uma forma indireta, sendo necessária uma ação equivocada do usuário do computador; seja abrindo página maliciosa da *Internet* ou até mesmo instalando um *software* com arquivos mal intencionados.

Após conseguir invadir o computador, os atacantes instalam um "*bot*", que é exatamente o que transforma essa máquina em um computador zumbi. Esse *bot* possui a capacidade de se comunicar com o atacante e realizar comandos indicados como iniciar ou parar um envio de tráfego a partir de uma instrução dada. Além de afetar o alvo, os ataques DDoS também podem prejudicar os usuários dos computadores zumbis, pois utilizam a banda de *Internet* deles para realizarem a transferência de tráfego de dados.

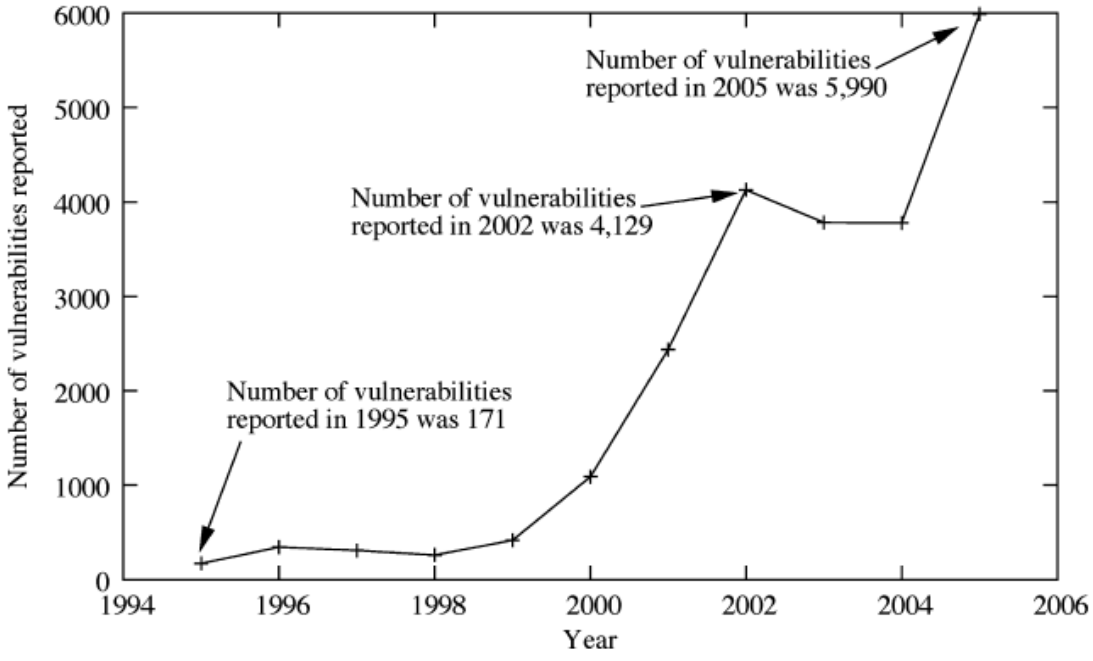


FIG 2.2 – Crescimento da vulnerabilidade dos computadores [1]

2.4 Tipos de Ataque

Os impactos gerados por ataque que consomem largura de banda impedem a continuidade do fornecimento de um determinado serviço. Existem dois impactos principais para esse tipo de ataque.

O primeiro deles é o consumo dos recursos de quem fornece o serviço, podendo ser um servidor *Web*, por exemplo. A vítima possui recursos limitados para processar os dados recebidos e, quando o tráfego de dados começa a ficar elevado, ela começa a descartar alguns pacotes e informa àqueles que estão enviando pacotes que reduzam a taxa de envio. Os usuários legítimos reduzem o envio, enquanto que as fontes de ataques continuam com a taxa elevada. Em pouco tempo os recursos da vítima, como CPU e memória, ficam completamente esgotados e ela fica impedida de fornecer o serviço a pacotes legítimos.

O segundo impacto é o consumo de largura de banda da rede, seja de DNS, roteadores ou *proxy*. Caso o fluxo malicioso de informações seja capaz de dominar o caminho que leva até a vítima, então o fluxo legítimo de dados pode ser bloqueado. Dessa forma, não só a vítima do ataque fica impedida de realizar seus serviços, mas também todos os outros que necessitam passar pelo mesmo caminho de comunicação. Embora os roteadores consigam descartar pacotes quando estão sobrecarregados, enquanto não houver um mecanismo que consiga distinguir pacotes maliciosos de pacotes legítimos, esses últimos também serão descartados.

Os ataques de largura de banda são divididos em quatro tipos. O primeiro tipo se aproveita de falhas nos protocolos da *Internet* (2.4.1). O segundo possui como alvo uma determinada aplicação (2.4.2). A terceira categoria utiliza terceiros sem que eles saibam para distribuir ou amplificar o ataque ao alvo (2.4.3). Por último, são ataques que afetam a infraestrutura da *Internet* (2.4.4). Na prática, hoje em dia um ataque pode fazer parte de mais de uma categoria.

2.4.1 Ataques de largura de banda baseados em protocolos

Esse tipo de ataque é baseado em uma falha de um procedimento normal de um determinado protocolo. Sua eficiência depende de haver uma fraqueza. Sendo assim, pode ser realizado por apenas uma fonte. Exemplos desse tipo são SYN *Flood*, ICMP *Flood* e UDP *Flood*.

2.4.1.1 SYN *Flood*

Esse tipo de ataque é um dos mais utilizados atualmente, afetando não apenas servidores *Web*, mas também qualquer serviço da *Internet* que forneça serviço de rede baseado em TCP, tais como servidores FTP e de *email*.

O SYN *flood* explora o mecanismo de abertura de conexão *three-way-hand-shake*, apresentado na figura 2.3 (A), do TCP e sua limitação em manter conexões parcialmente abertas. Quando um servidor recebe uma requisição SYN, retornando um pacote SYN/ACK para o cliente. Enquanto o cliente não responde para o servidor com um novo pacote ACK, a conexão permanece parcialmente aberta, até acabar o período de tempo limite do pacote. O servidor mantém em memória todas as conexões parcialmente abertas e, como essa memória é finita, o servidor suporta até um determinado limite de conexões simultâneas [8].

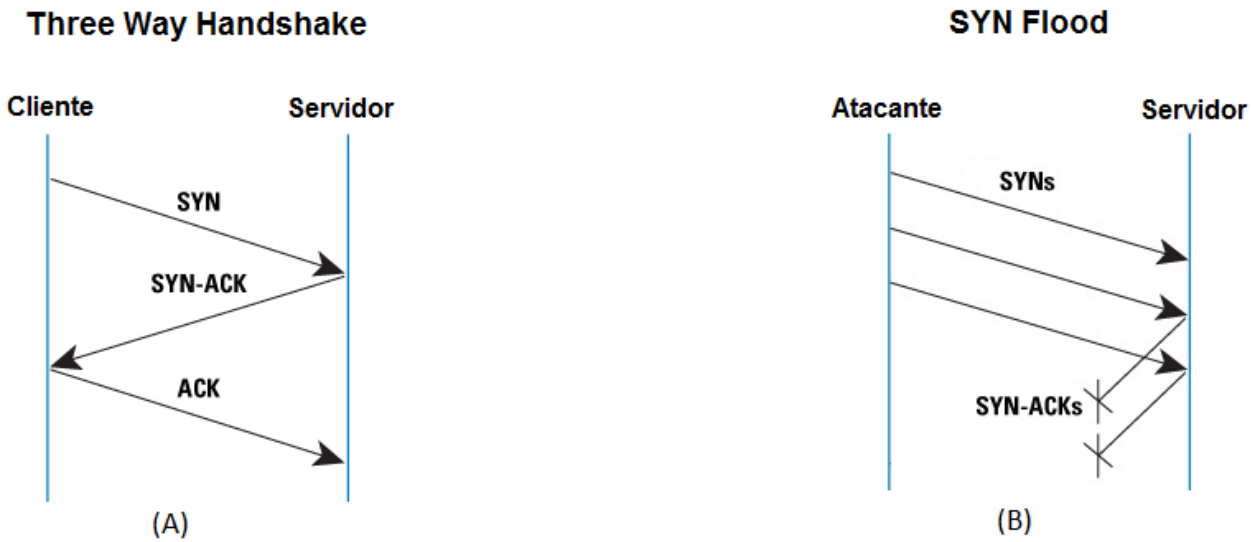


FIG 2.3 – Comparação entre abertura de conexão normal e SYN *Flood*

Esse tipo de ataque se aproveita desse fato a partir do envio de diversas *flags* SYN pelo agente malicioso, para iniciar uma conexão, e não envia a *flag* de confirmação ACK, como apresentado na figura 2.3 (B). Dessa forma, o servidor fica com a memória sobrecarregada, não conseguindo servir aos usuários legítimos que tentam estabelecer conexão.

Após um tempo sem resposta, toda conexão aberta é fechada, porém esse tempo não costuma ser baixo. Com isso, enquanto o *timeout* é aguardado, o atacante consegue esgotar os recursos de memória do servidor.

Algumas características tornam esse tipo de ataque um dos mais difíceis de serem defendidos. Primeiramente, ao contrário de ataques como o Ping da Morte, que podem ser evitados com uma proteção (firewall), os pacotes SYN fazem parte de qualquer abertura legítima de conexão, portanto dificilmente são filtrados. Além disso, pacotes SYN são pequenos e fáceis de serem enviados em grande quantidade, sem a necessidade de uma estrutura tecnologicamente avançada para isso. Por fim, os atacantes não precisam fazer contato com a vítima, podendo utilizar um IP falso ou até mesmo outro computador infectado para se camuflar, tornando difícil a prevenção e a descoberta do real causador. [9]

2.4.1.2 ICMP *Flood*

O Protocolo de Controle de Mensagem da *Internet* (ICMP) é baseado no protocolo IP e é utilizado para responder diagnósticos de informações da rede; um desses programas é o *ping*. [1] Uma requisição enviada em *broadcast* é recebida por todas as máquinas da rede. Dessa forma, caso seja feita uma consulta de um *ping* para um endereço de *broadcast*, todas as máquinas irão responder à requisição. Esse ataque corresponde ao atacante mascarar seu IP e enviar uma requisição ICMP para um endereço de *broadcast*, a resposta iria ser direcionada para o IP mascarado, que seria a vítima, a qual receberia todos os pacotes de resposta ICMP. Dessa forma, a vítima ficaria sobrecarregada com o excesso de pacotes recebidos.

2.4.1.3 UDP *Flood*

O protocolo UDP não possui abertura de conexão, ao contrário do TCP. Dessa forma, seu ataque ocorre com o envio de diversos pacotes UDP para portas aleatórias no servidor. Ao realizar isso, a vítima irá verificar a aplicação rodando na porta afetada e identificará que não há nada, enviando um pacote ICMP de destino inalcançável. O envio de diversos pacotes UDP leva a vítima a enviar muitos pacotes ICMP também, muitas vezes que não conseguem alcançar o destino, pois o atacante mascara o IP para garantir que o pacote ICMP nunca irá chegar nele. Com isso, o servidor fica sobrecarregado sendo obrigado a enviar uma grande quantidade de pacotes ICMP. [10]

2.4.2 Ataques de largura de banda baseados em aplicações

Outro modo de amplificar o poder dos ataques DDoS é forçando o alvo a executar uma operação de alto custo. Por exemplo, enviando um grande número de consultas à ferramenta de busca de um sistema *web*, forçando o servidor a executar operações custosas à CPU e à memória, diminuindo os recursos para usuários legítimos.

2.4.2.1 HTTP *Flood*

As aplicações da *World Wide Web* (WWW) estão entre as mais usadas em todo o mundo. A maioria delas utiliza o HTTP (*Hypertext Transfer Protocol*). Com isso, a maioria dos *firewalls* deixa essa porta aberta para ocorrer o tráfego de mensagens HTTP.

Genericamente, o HTTP *Flood* é um ataque em que servidores *web* são sobrecarregados com requisições HTTP. Estes ataques são implementados pela maioria dos *softwares* de *botnets*. Para enviar uma requisição válida, é necessária uma conexão TCP válida, que necessita de um endereço IP real. Os atacantes podem conseguir isto utilizando os endereços IP dos computadores da *botnet*, mascarando seu próprio IP. Além disso, a requisição HTTP pode ser enviada de modo a maximizar o poder do ataque, instruindo, por exemplo, os membros da *botnet* a carregarem um arquivo muito grande de um servidor, diminuindo sua disponibilidade de recursos. [1]

2.4.2.2 SIP Flood

Nos últimos anos, o VoIP (*Voice over* IP) tem se tornado bastante popular devido ao seu baixo custo. O protocolo padrão para abertura de uma conexão VoIP é o SIP (*Session Initiation Protocol*). Além disso, por motivos de escalabilidade o SIP é implementado usando como base o protocolo UDP, para que não seja necessária a abertura de conexão obrigatória no TCP, tornando ele sem estado.

Em um cenário de ataque, os atacantes podem sobrecarregar o Proxy SIP com muitos pacotes de convites SIP com um IP falso. Para evitar mecanismos de *antispoof* (impedem que o IP seja mascarado), os atacantes podem usar uma *botnet* usando os IPs reais das máquinas da rede. O ataque pode ser direcionado ao *proxy* SIP, fazendo com que o serviço fique inacessível a qualquer usuário, ou a um usuário, fazendo com que este não possa se comunicar com outros usuários legítimos [1].

2.4.3 Ataques distribuídos de refletores

Uma meta importante para os atacantes é esconder a verdadeira fonte do ataque. Um dos meios de se alcançar esse objetivo é utilizando o DRDoS (*Distributed reflector denial of service*); este ataque visa esconder o IP da fonte do ataque utilizando terceiros (roteadores e servidores *web*) para gerar tráfego para a vítima. Estes terceiros são chamados refletores. Toda máquina com a capacidade de responder a um pacote é um refletor em potencial. A diferença entre o DRDoS e o DDoS original é que, ao invés de mandar os computadores zumbis trocarem tráfego com a vítima diretamente, estes enviam pacotes para os terceiros utilizando o IP da vítima. Então os terceiros respondem à vítima, consumindo seus recursos. A figura 2.3 representa um possível esquema onde ocorre uma realização desse tipo de ataque.

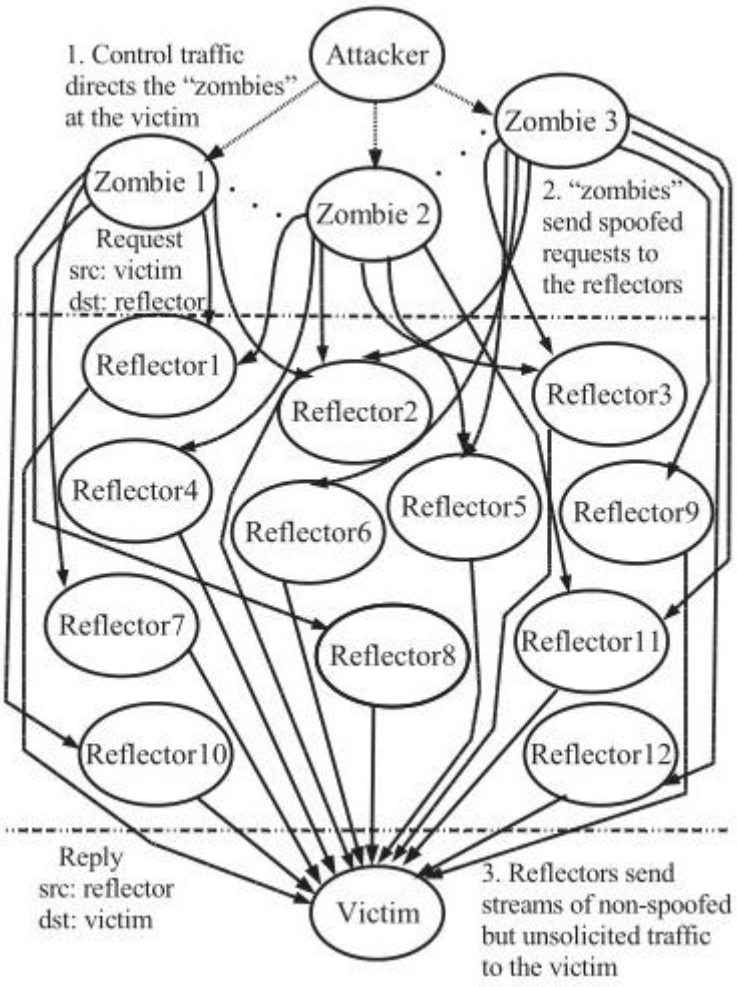


FIG 2.4 – Estrutura de um ataque DRDoS [1]

2.4.3.1 Ataques amplificados de DNS

Um tipo de ataque DRDoS bastante efetivo faz uso dos servidores DNS já existentes. O trabalho dos servidores de DNS é prover uma infraestrutura distribuída para armazenar e associar diferentes tipos de RR (*resource records*) a nomes de domínios na *Internet*. Um servidor DNS recursivo atende a uma consulta e associa o nome do domínio para o requisitor contatando um servidor de DNS autoritário. O grande problema é que a resposta da consulta é desproporcional a mesma. A resposta da consulta geralmente inclui a consulta original, então o pacote de resposta é sempre maior que o pacote da consulta. É possível que o pacote de resposta seja mais de 70 vezes maior que o pacote da consulta original [1].

2.4.4 Ataques de Infraestrutura

O objetivo principal desse tipo de ataque é derrubar um componente essencial para a *Internet*, sendo seu resultado uma grande tragédia que afetaria todos os lugares do mundo. Um exemplo desse tipo é um ataque a um servidor raiz de DNS (DNS *Poisoning*), visto que para acessar qualquer página da *Internet* o serviço DNS é necessário para traduzir o endereço em IP, ataques desse gênero causariam uma calamidade no mundo inteiro.

Além disso, como roteadores atuam como pontes entre a *Internet* e os usuários, qualquer ataque que afete o funcionamento de um roteador, como a tabela de rotas, pode constituir um ataque de infraestrutura, pois afetaria o acesso mundial à rede. Alguns roteadores possuem falhas de segurança e essas podem ser exploradas para esse tipo de ataque.

Para ser eficiente, esse tipo de ataque necessita de várias máquinas atuando em conjunto, gerando uma alta quantidade de tráfego para o serviço. [1]

2.5 Tráfego de *Internet*

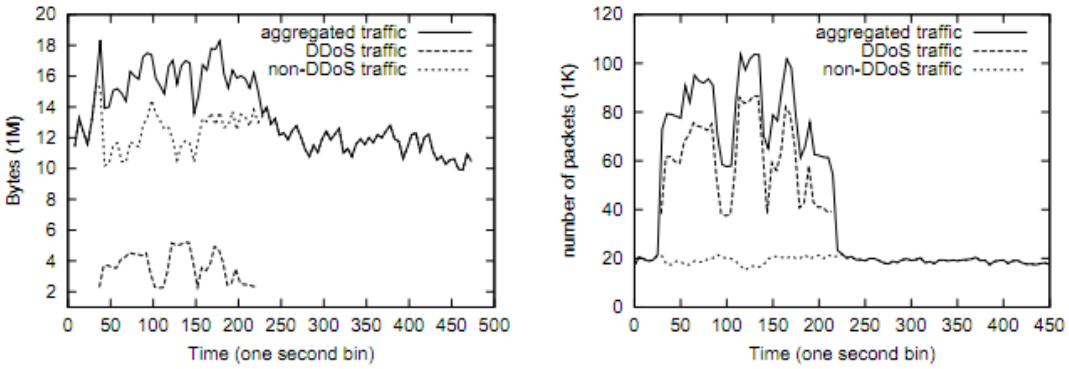
O número de usuários da *Internet* pode ser estimado em 2,3 bilhões de pessoas [11] e cresce exponencialmente a cada dia, da mesma forma que os serviços prestados pela mesma. Dessa forma, ao invés de ocorrer uma invasão de um sistema de segurança prejudicando ele, a ameaça presente tornou-se um crescimento do tráfego de dados na rede trocados de forma maliciosa. [12]

Tráfego de rede é definido como o fluxo gerado pelos pacotes de serviços e aplicações normais da *Internet*, como *web*, FTP, SMTP. A análise desse fator pode identificar um ataque DDoS, o que um *firewall* comum não conseguiria fazer. Como ataques DDoS são direcionados para uma vítima normalmente, o monitoramento do tráfego pode indicar um crescimento fora do normal para apenas um local, indicando que ele está sendo alvo de um ataque.

A figura 2.4 mostra o crescimento do tráfego de dados em *bytes* (gráfico a) e número de pacotes (gráfico b) em relação ao progresso de um ataque DDoS. A magnitude do tráfego de um ataque é três vezes maior do que um tráfego normal em relação ao número de pacotes, conforme mostra o gráfico b [13]. Isso mostra o quanto a vítima fica comprometida, pois não espera uma quantidade de dados grande dessa forma, além de mostrar formas de reconhecer quando um ataque está ocorrendo.

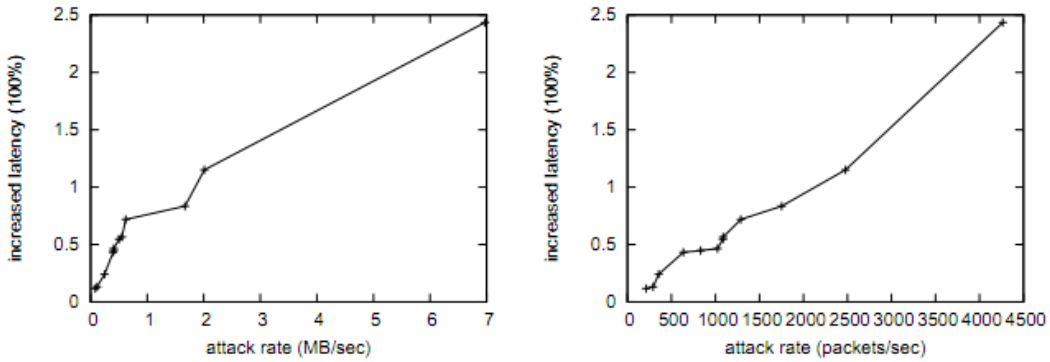
Um crescimento no tráfego trocado na rede influencia diretamente a latência do serviço de DNS. [13] Latência de DNS é definida como o tempo que demora entre o recebimento da requisição pelo servidor e o envio de uma resposta ou aviso de falha. A latência da *web* afeta o desempenho das transações HTTP, transferência de arquivos. As figuras 2.5 e 2.6 mostram como variam as latências do DNS e da *web*, respectivamente, em relação a uma variação do ataque DDoS. A latência do DNS aumenta em até 250% ao longo de um ataque e a latência da *Web* aumenta em até 40% [13]. Esses dados mostram o quanto o acesso à *Internet* fica prejudicado para usuários legítimos durante um ataque DDoS.

Atualmente um ataque DDoS ultrapassa os 100 Gb por segundo de dados enviados com o uso de *botnets*. Dessa forma, a análise do tráfego de dados na *Internet* é capaz de detectar a ação de um agente malicioso utilizando uma *botnet*.



(a) Volume de tráfego em *bytes* (b) Volume de tráfego por número de pacotes

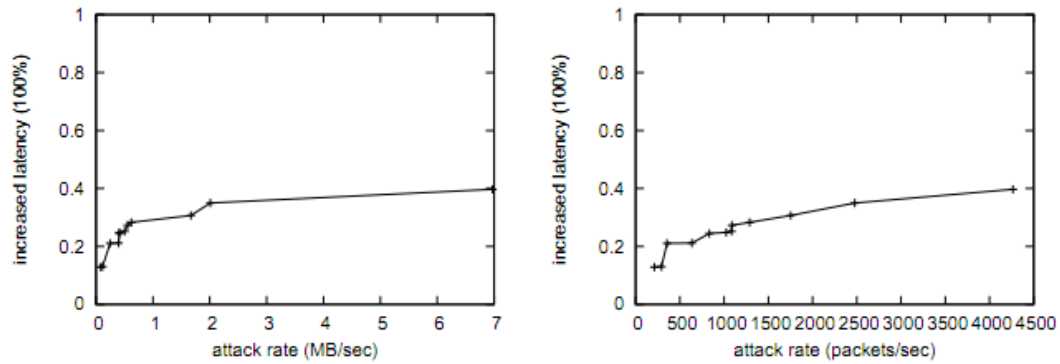
FIG 2.5 – Tráfego de dados gerado por um ataque DDoS [13]



(a) Ataques DDoS em *bytes* variando a latência de DNS

(b) Ataques DDoS em número de pacotes variando a latência de DNS

FIG 2.6 – Aumento da latência de DNS com diferentes variações de DDoS [13]



(a) Ataques DDoS em *bytes* variando a latência da *web*

(b) Ataques DDoS em número de pacotes variando a latência da *web*

FIG 2.7 – Aumento da latência da *web* com diferentes variações de DDoS [13]

3 Modelagem dos Ataques

Nessa seção será realizada a modelagem dos ataques SYN *Flood* e UDP *Flood*. O objetivo é permitir um estudo mais profundo dos ataques a partir da simulação dos mesmos. A modelagem prevê uma distribuição matemática para cada campo dos pacotes e informações do tráfego de dados.

3.1 Fundamentação Matemática

Nessa seção será apresentada a teoria matemática na qual se baseiam as distribuições utilizadas na modelagem dos pacotes UDP e TCP.

3.1.1 Distribuição de *Poisson*

A distribuição de *Poisson* é uma distribuição discreta de probabilidade que calcula a probabilidade de um número de eventos ocorrerem em um período de tempo fixo. Pode ser utilizado também utilizando outros intervalos fixos, como distância, área ou volume [14].

Uma variável é dita obedecer a uma distribuição de *Poisson* com parâmetro $\lambda>0$, para k = 0,1,2,..., se a função de probabilidade dela é dada por:

$$f(k,\lambda) = \Pr(X = k) = \frac{\lambda^k e^{-\lambda}}{k!}$$

Onde,

e é o número neperiano (e=2,71828...);

k! é o fatorial de k.

3.1.2 Distribuição Exponencial

A distribuição exponencial é uma distribuição contínua de probabilidade que descreve o tempo entre eventos em um processo no qual eventos ocorrem continuamente e independentemente em uma taxa média constante. [15]

Sua função de distribuição de probabilidade é dada por:

$$f(x,\lambda) = \begin{cases} \lambda e^{-\lambda x}, & x \geq 0 \\ 0, & x < 0 \end{cases}$$

Sua função de distribuição cumulativa é dada por:

$$F(x,\lambda) = \begin{cases} 1 - e^{-\lambda x}, & x \geq 0 \\ 0, & x < 0 \end{cases}$$

3.2 UDP *Flood*

Para a modelagem de datagramas UDP foram analisados os seguintes parâmetros: endereço das portas de origem e destino, tamanho do pacote, soma de verificação (*checksum*), que são os campos do cabeçalho UDP, como visto na figura 3.1; e o tempo de intervalo de chegada de pacote.

Porta de Origem	Porta de Destino
Tamanho UDP	Soma de Verificação UDP

FIG 3.1 – Cabeçalho UDP [16]

3.2.1 Tempo de intervalo de chegada de pacote

Considerando a chegada de pacotes um evento que ocorre apenas uma vez em um intervalo de tempo infinitesimal, isto é, não há duas chegadas de pacote no mesmo instante exato de tempo, essa quantidade pode ser modelada a partir de uma distribuição

de Poisson, visto na seção 3.1.1, considerando a chegada de um pacote como o evento apresentado [17]. Apesar de algumas complexidades no tráfego de dados não poderem ser explicadas por essa distribuição quando olhado separadamente, o tráfego agregado continua obedecendo à distribuição de Poisson. Dessa forma, o tempo de intervalo de chegada de pacote é modelado a partir de uma distribuição Exponencial, visto na seção 3.1.2, que descreve o tempo entre cada chegada pacote. [18]

3.2.2 Endereço de Portas de Origem e Destino

As portas são utilizadas para identificar as aplicações que estão gerando o tráfego de informações. A distribuição deste número de porta é criada baseando-se na probabilidade de um tipo de aplicação iniciar um novo fluxo de dados. Esta distribuição pode então ser formulada através da observação do tráfego em uma rede. Em um determinado espaço de tempo é possível contar a quantidade de pacotes destinados a determinada porta. Para facilitar este trabalho, podemos dividir os números de portas em 4 tipos: Conhecidas (0 à 1023), registradas (1024 à 49151), dinâmicas (49152 à 65535) e outras (pacote não IP) [18].

Utilizando este conhecimento podemos fazer a modelagem baseando-se na informação sobre o conjunto ao qual o último pacote recebido pertence, podemos calcular a probabilidade de o próximo pacote pertencer a um destes conjuntos. Como feito na figura 3.2.

Previous packet/next packet	Well-known	Registered	Dynamic	Other
Well-known	0.4	0.5	0.1	0.0
Registered	0.3	0.2	0.3	0.2
Dynamic	0.4	0.2	0.2	0.2
Other	0.6	0.1	0.3	0.0

FIG 3.2 – Distribuição probabilística das portas [18]

Essa figura apresenta a probabilidade proposta, na qual dado o datagrama anterior, dependendo do tipo ao qual ele pertence, há uma determinada probabilidade de

ele pertencer a cada tipo. Por exemplo, se o pacote anterior for conhecido, o próximo tem 40% de chances de também ser conhecido. Dado que o tipo da porta foi descoberto, no intervalo proposto é calculado um número randômico para ser destinado à porta desse datagrama.

Os endereços de porta de origem e destino seguem a mesma distribuição de probabilidade.

3.2.3 Tamanho do Pacote

Analisando pesquisas existentes na área, pode-se verificar o uso de duas formas principais de se modelar o tamanho do pacote de um datagrama UDP. O primeiro método consiste na divisão de diversos tamanhos de pacote em grupos, e na utilização de dados previamente capturados a fim de gerar uma distribuição de probabilidade para esses conjuntos [18]. O outro método consiste apenas na utilização de números aleatórios definidos em certo intervalo pré-definido, com o objetivo de obter um fluxo de dados mais próximo da realidade [19].

3.2.4 Soma de Verificação

Esse campo é utilizado para detectar erros em todo o datagrama (cabeçalho e dados) e é um campo opcional. Ele é calculado a partir de um pseudocabeçalho, o cabeçalho UDP e os dados. Esse pseudocabeçalho é parte do cabeçalho IP, com alguns campos preenchidos com o valor 0. Esse pseudocabeçalho inclui os endereços IP de origem e destino, o protocolo utilizado e o comprimento total do UDP. Podemos ver a estrutura do pseudocabeçalho na figura 3.3.

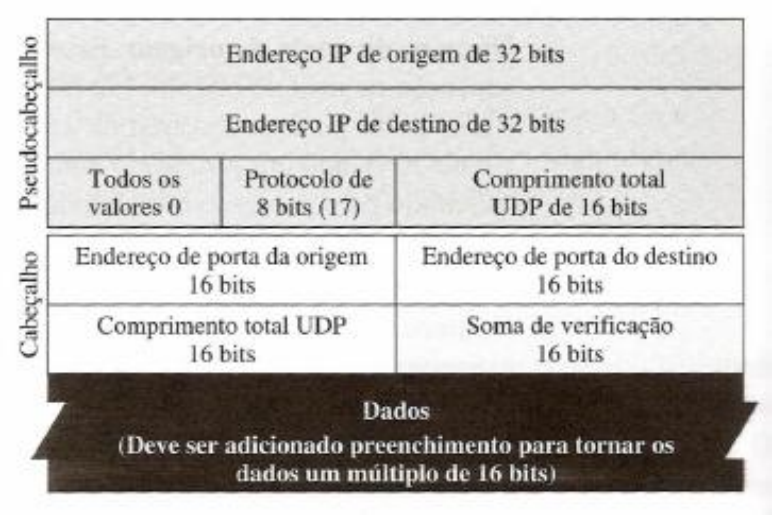


FIG 3.3 – Estrutura para calculo do *checksum* [20]

Caso a soma de verificação não incluísse o pseudocabeçalho, o datagrama poderia ser enviado para o *host* errado, caso o cabeçalho IP fosse corrompido. O campo protocolo é utilizado para garantir que o pacote pertence ao UDP e não TCP.

A soma de verificação é calculada no remetente a partir das seguintes etapas [20]:

1. Adicionar o pseudocabeçalho no datagrama de usuário UDP;
2. Preencher o campo de soma de verificação com zeros;
3. Dividir os bits totais em palavras de 16 bits (2 bytes);
4. Se o número total de bytes não for par, adicionar 1 byte de preenchimento (todos bits 0);
5. Somar todas as seções de 16 bits utilizando aritmética de complemento um;
6. Complementar o resultado (todos bits 1 viram 0 e todos 0 viram 1), que é um campo de 16 bits, e insere-o no campo de soma de verificação;
7. Eliminar o pseudocabeçalho e o preenchimento adicionado.

3.3 SYN *Flood*

Para a modelagem dos pacotes TCP foram analisados os seguintes parâmetros: endereços de porta de origem e porta de destino, número de sequência, número de reconhecimento (ack), comprimento do cabeçalho, um campo reservado (que não é

utilizado na emissão do pacote TCP), controle, tamanho da janela, soma de verificação (*checksum*), ponteiro urgente e opções extras (que não serão utilizados), que são os campos do cabeçalho TCP, como visto na figura 3.4; além do tempo de intervalo de chegada de pacote.

Os endereços de porta de origem e de destino seguem a mesma distribuição daqueles dos datagramas UDP, como visto na seção 3.2.2. O tempo de intervalo de chegada de pacotes também é modelado conforme feito na seção 3.2.1. A soma de verificação para o TCP segue o mesmo procedimento daquele descrito na seção 3.2.4, com a única modificação que no campo de protocolo está representado o protocolo TCP.

O campo de controle possui 6 *flags* de controle de fluxo. Os campos urgente, *push* e *reset* são definidos como desativados. A *flag* SYN é definida como ativada, para validar a abertura de conexão. As *flags* ACK e FIN não são utilizadas, pois não há necessidade do número de reconhecimento (ack) e nem do fechamento de conexão. Dessa forma, o campo do número de reconhecimento do cabeçalho pode ser utilizado como sendo 0 [21].

Como o tamanho do cabeçalho modelado é fixo, o comprimento do cabeçalho pode ser definido como um número fixo. O campo reservado é destinado para uso futuro do pacote. O ponteiro urgente é utilizado apenas nos casos em que o *flag* urgente está ativado, não sendo necessário para essa modelagem, bem como as opções extras adicionais.

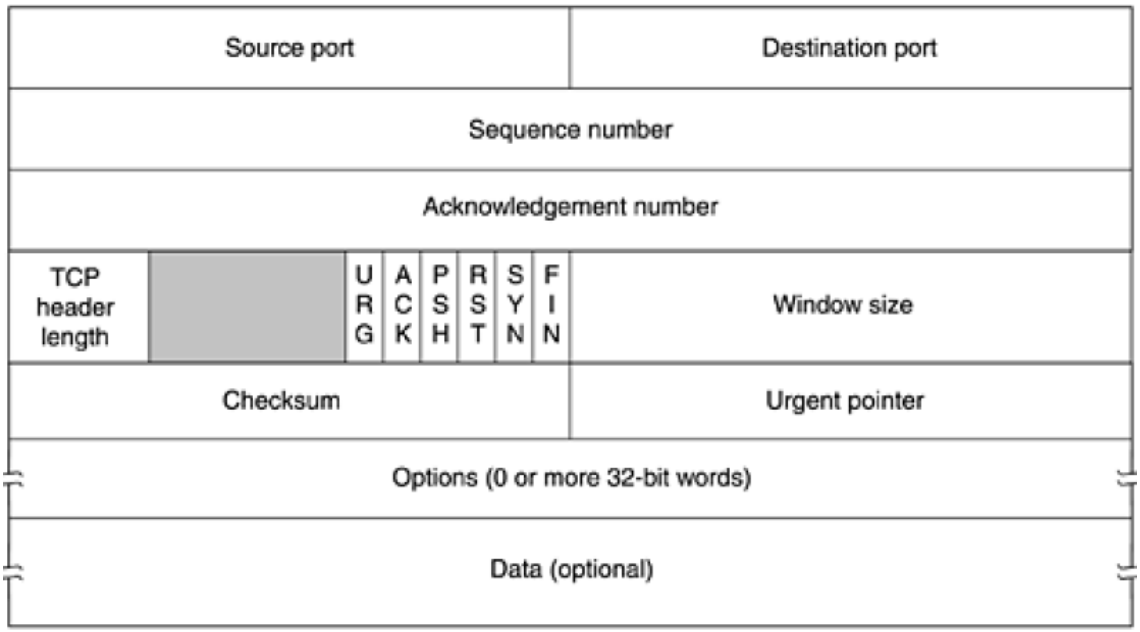


FIG 3.4 – Cabeçalho TCP [16]

3.3.1 Tamanho da Janela

O tamanho da janela define o máximo de *bytes* que o receptor suporta e é essencial para o controle de fluxo no protocolo TCP. O tamanho máximo desse campo é de 16 bits, portanto o maior tamanho possível é de 65535 *bytes*.

A figura 3.5 expressa a distribuição de probabilidade acumulada do tamanho da janela do receptor para cinco medidas realizadas. De forma geral, o tamanho da janela é múltiplo do tamanho do pacote, isso explica os saltos presentes na figura 3.5 [22]. Podemos notar nessa figura que uma fração significante de conexões utiliza uma janela de conexão pequena em todas as medidas. Por exemplo, entre 45% e 65% das conexões o tamanho da janela é inferior a 20000 *bytes* e entre 50% e 70% utilizam tamanho de janela inferior a 30000 *bytes*.

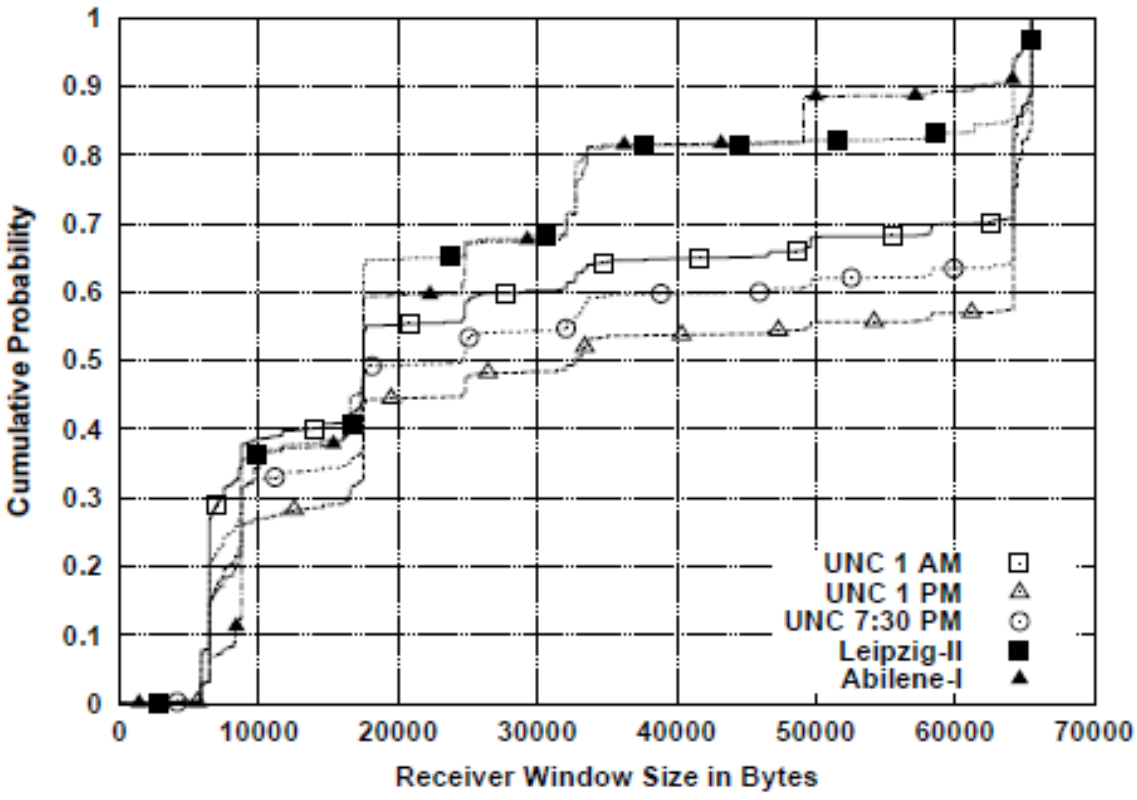


FIG 3.5 – Probabilidade acumulada do tamanho da janela [22]

3.3.2 Número de Sequência

Para a modelagem do número de sequência foram analisados 4 diferentes ferramentas utilizadas para a realização de ataques DDoS: o Agobot, o SDbot, o Rbot e o Spybot.

O AgoBot é um dos *bots* mais populares na *Internet*. Existem cerca de 600 diferentes versões para este *bot*. Este *software* foi desenvolvido em C++ e estruturado de forma modular, facilitando a adição de novos métodos de ataque. Este *software* tem atualmente suporte a ataques como o SYN *Flood*, UDP *Flood*, HTTP *Flood*, e outros [21].

O SDBot é outro *bot* bastante popular que tem mais de 1800 variantes existentes. Este *software* foi escrito em C++ e suporta ataques do tipo UDP *Flood*, e apenas algumas versões tem suporte a ataques SYN *Flood* [21].

O RBot tem mais de 1600 variantes e tem como alvo sistemas *Windows* e suporta ataques como o SYN *Flood*, ICMP *Flood*, UDP *Flood* e outros [21].

O SpyBot tem mais de 200 diferentes variantes e também tem como alvo sistemas *Windows* e tem suporte para o SYN *Flood* [21].

Foi verificado que todas as 4 ferramentas de ataques utilizam o mesmo método para gerar os números de sequência, este método consiste em realizar a operação OR entre 2 números aleatórios de 32 bits e efetuar 16 operações de *shift left* no resultado, gerando o número a ser utilizado neste campo [21].

4 CONCLUSÃO

Observa-se que os ataques DDoS tornaram-se uma grande preocupação no meio da Internet, por serem incidentes muito difíceis de serem prevenidos e identificados. Além disso, podem causar muitos prejuízos àqueles que possuem serviços na Internet e mesmo àqueles que querem apenas utilizá-la para tarefas pessoais.

Dessa forma, os esforços estão sendo voltados para o estudo de técnicas de defesa, porém antes de implementar uma defesa é necessária a análise e entendimento detalhado de cada tipo de ataque para que seja desenvolvida uma defesa específica para cada um.

A proposta de modelagem dos ataques realizada pode ser utilizada para simular ameaças semelhantes a um ataque DDoS. Dessa forma, é possível estudar métodos para prevenção, defesa e até mesmo detecção de um possível invasor.

5 REFERÊNCIAS

[1] PENG, Tao. LECKIE, Christopher. RAMAMOHANARAO, Kotagiri. **Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems**

[2] **TERRA.** Disponível em <tecnologia.terra.com.br/noticias/0,,OI5592929-EI15608,00-Em+dia+de+ataques+hackers+derrubam+sites+de+varios+bancos.html> Acesso em 27 de Outubro de 2011.

[3] SPECHT, Stephen. LEE, Ruby. **Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures**

[4] **FOXNEWS.** Disponível em <www.foxnews.com/story/0,2933,55382,00.html> Acesso em 27 de Outubro de 2011.

[5] **EWEEK.** Disponível em <www.eweek.com/c/a/Security/PayPal-PostFinance-Hit-by-DoS-Attacks-CounterAttack-in-Progress-860335/> Acesso em 27 de Outubro de 2011.

[6] **ZDNET.** Disponível em <www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670> Acesso em 27 de Outubro de 2011.

[7] **CNET.** Disponível em <news.cnet.com/2100-1001-963005.html> Acesso em 27 de Outubro de 2011.

[8] WANG, Haining. ZHANG, Danlu. SHIN, Kang G. **Detecting SYN Flooding Attacks**

[9] OLIVER, Ross. **Countering SYN Flood Denial-of-Service Attacks**

[10] XIAOMING, Li. SEJDINI, Valon. CHOWDHURY, Hasan. **Denial of Service (DoS) Attack with UDP Flood**

[11] **INTERNET WORLD STATS.** Disponível em <http://www.internetworldstats.com/stats.htm> Acesso em 26 de Junho de 2012.

[12] KIM, Myung-Sup. KUNG, Hun-Jeong. HONG, Seong-Cheol. CHUNG, Seung-Hwa. HONG, James W. **A Flow-based Method for Abnormal Network Traffic**

Detection

[13] LAN, Kun-chan. HUSSAIN, Alefiya. DUTTA, Debojyoti. **Effect of Malicious Traffic on the Network**

[14] HU, Hao. **Poisson Distribution and Application**

[15] MONTGOMERY, Douglas C. RUNGER, George C. **Applied Statistics and Probability for Engineers**, 2003. John Wiley & Sons

[16] TANENBAUM, Andrew S. **Redes de Computadores**, 2003. Campus Editora

[17] VIRTAMO, J. **Queueing Theory / Poisson Process**

[18] SHAWKY, Ahmed. BERGHEIM, Hans. RAGNARSSON, Olafur. WRATNY, Andrzej. PEDERSEN, Jens. **Characterization and Modeling of Network Traffic**

[19] WANG, Jie. PHAN, Raphael C. W. WHITLEY, John N. PARISH, David J. **Advanced DDoS Attacks Traffic Simulation with a Test Center Plataform**

[20] FOROUZAN, Behrouz A. **Protocolo TCP/IP**, 2008. Mc Graw Hill

[21] CAMPOS-HERNÁNDEZ, Félix. **Generation and Validation of Empirically-Derived TCP Application Workloads**

[22] THING, Vrizlynn L. L. SLOMAN, Morris. DULAY, Naranker. **A Survey of Bots Used for Distributed Denial of Service Attacks**