MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPATARMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
CURSO DE MESTRADO EM SISTEMAS E COMPUTAÇÃO

WELLINGTON HETMANEK DOS SANTOS

MÉTODO DE DETECÇÃO DE ATAQUES DDOS COMPOSTOS BASEADO EM FILTRAGEM SEQUENCIAL

Rio de Janeiro
2012

INSTITUTO MILITAR DE ENGENHARIA

WELLINGTON HETMANEK DOS SANTOS

MÉTODO DE DETECÇÃO DE ATAQUES DDOS COMPOSTOS BASEADO EM FILTRAGEM SEQUENCIAL

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Sistemas e Computação.

Orientador: Prof. Anderson Fernandes P. dos Santos, D.Sc.

Rio de Janeiro
2012

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

005.1 Santos, Wellington Hetmanek dos
S231m Método de Detecção de Ataques DDoS Compostos baseado em Filtragem Sequencial/ Wellington Hetmanek dos Santos. - Rio de Janeiro: Instituto Militar de Engenharia, 2012.

80 p.:il, graf., tab.

Dissertação (mestrado) – Instituto Militar de Engenharia – Rio de Janeiro, 2012.

1. Engenharia de Sistemas e Computação - teses, dissertações. 2. Algoritmo 3. Detecção de Ataques DDoS. I. Santos, Anderson Fernandes P. dos II. Título. III. Instituto Militar de Engenharia.

CDD 005.1

INSTITUTO MILITAR DE ENGENHARIA

WELLINGTON HETMANEK DOS SANTOS

MÉTODO DE DETECÇÃO DE ATAQUES DDOS COMPOSTOS BASEADO EM FILTRAGEM SEQUENCIAL

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Sistemas e Computação.

Orientador: Prof. Anderson Fernandes P. dos Santos, D.Sc.

Aprovada em 22 de Agosto de 2012 pela seguinte Banca Examinadora:

Prof. Anderson Fernandes P. dos Santos, D.Sc. do IME - Presidente

---

Prof. Ronaldo Moreira Salles, Ph.D. do IME

Prof. Sidney Cunha de Lucena, D.Sc. da UNIRIO

Rio de Janeiro
2012

Dedico esta dissertação primeiramente a Deus. Dedico aos meus pais e irmãos.

AGRADECIMENTOS

Agradeço a todas as pessoas que contribuíram no desenvolvimento deste projeto, tenha sido por meio de críticas, idéias, apoio, incentivo ou qualquer outra forma de auxílio.

Agradeço a paciência dos meus pais e amigos, por me entenderem e aguentarem durante essa época desgastante e intensa na vida de um mestrando.

Agradeço a Natália, que revisou meu português, atendendo meus pedidos de última hora.

Agradeço ao Anderson, orientador que sempre acrescentou e nunca desmotivou.

Agradeço ao Luís, funcionário do laboratório de computação do IME por me ajudar nos experimentos realizados.

Agradeço aos meus sócios, Arilson, Marcelo, Maurício e Sandro, que mesmo durante esse período de mestrado, me passaram tranquilidade e confiança para conquistar meus objetivos e incentivo para juntos construirmos uma empresa, que por si só já valeu todo esforço.

Agradeço aos amigos de IME, Cláudio, Renato, Priscilla e Camila, que sempre se mostraram companheiros e dispostos a vencer os desafios do mestrado.

Agradeço aos professores do IME, Salles, Raquel e Vidal, pelo apoio, aulas e também pelas dicas ao longo dessa etapa.

Agradeço ao professor do LNCC, Jauvane, simplesmente por ministrar uma das aulas mais interessantes que eu já presenciei no IME e na vida.

Em especial a professora Carmona, de estatística, que teve paciência e cuidado em ensinar sua matéria de maneira praticamente particular, sempre conseguindo um tempo para me explicar.

Agradeço a Emília, da secratária do IME, pelas dicas e orientações.

Por fim, a todos os professores e funcionários do Seção de Engenharia de Computação (SE/8) do Instituto Militar de Engenharia.

Wellington Hetmanek dos Santos

Emancipate yourself from mental slavery.

Marcus Garvey

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ABREVIATURAS

AS	-	*Autonomous System*
DARPA	-	*Defense Advanced Research Projects Agency*
DoS	-	*Denial of Service*
DDoS	-	*Distributed Denial of Service*
DNS	-	*Domain Name System*
HTTP	-	*HyperText Tranfer Protocol*
ICMP	-	*Internet Control Message Protocol*
IDS	-	*Intrusion Detection System*
IME	-	*Instituto Militar de Engenharia*
IP	-	*Internet Protocol*
IPS	-	*Intrusion Prevention System*
LAMP	-	*Linux, Apache, MySQL, PHP/Python/Perl*
LOIC	-	*Low Orbit Ion Cannon*
MATLAB	-	*MATrix LABoratory*
PING	-	*Packet INternet Groper*
OSI	-	*Open Systems Interconnection*
RPF	-	*Router-based Packet Filtering*
SGSI	-	*Sistema de Gestão da Segurança da Informação*
SYN	-	*Synchronize*
TCP	-	*Transmission Control Protocol*
UDP	-	*User Datagram Protocol*
WWW	-	*World Wide Web*

RESUMO

Nos últimos anos, ataques distribuídos de negação de serviço (DDoS) têm evoluído em termos de complexidade de detecção, tamanho da *botnet* e volume de tráfego gerado. Dois ataques ocorridos na Coréia do Sul, o primeiro em 2009 (ataque 7.7) e o segundo em 2011 (ataque 3.4), acrescentaram mais características aos ataques DDoS. Esses dois ataques lançaram uma ofensiva contra seus alvos a partir de diferentes tipos de ataques DDoS conhecidos e ao mesmo tempo, formando um ataque DDoS composto. Este tipo inovador de ataque possui características particulares que podem ser usadas para serem identificadas, seja separando cada ataque ou analisando-os conjuntamente.
Neste estudo, é apresentado um método de detecção de ataques DDoS através do algoritmo desenvolvido, o Algoritmo de Detecção de Ataques DDoS Compostos, que utiliza uma sequência de filtros que objetivam identificar as origens, os destinos e o perfil de utilização de protocolos dessas origens de ataque que compõe uma *botnet*. Para comprovar a eficiência do algoritmo foram construídos ambientes de simulação, onde foi possível gerar tráfego malicioso com características de ataques DDoS compostos e coletar esses dados na saída da rede. O método proposto se mostrou eficaz em todas as simulações, identificando 100% dos ataques DDoS compostos existentes nesses ambientes.

ABSTRACT

In recent years, Distributed Denial of Service attacks (DDoS) have evolved in terms of complexity, botnet size and generated traffic flow. Two South Korea attacks, the first in 2009 (7.7 attack) and the other in 2011 (3.4 attack), increased features to DDoS attacks. Both attacks launched different kinds of known DDoS attacks in a compound way, in other words, diversified DDoS attacks being used at the same time, at the same targets. Those attacks, separately or jointly, have particular characteristics that can be used to identify them.

In this study, we present a method for DDoS attack detection by the developed algorithm, the Compound DDoS Attack Detection Algorithm, which uses a sequence of filters that aim to identify the attack traffic sources, the attack targets and the use of protocol profiles from these traffic sources originated from a network that has a part of the botnet involved. Simulation environments were created to prove the efficiency of the algorithm , where it was possible to generate malicious traffic like a compound DDoS attack and collect data traces from the outbound network. The proposed method was effective in all simulations, identifying 100 % of the compounds DDoS attacks in these environments.

1 INTRODUÇÃO

Através da Internet, é possível obter informações praticamente na medida em que acontecem. Uma importante ferramenta para o processo de globalização e difusão do conhecimento nos últimos vinte anos, a Internet, é considerada o principal meio de comunicação da atualidade e exerce um papel fundamental para o desenvolvimento economico-cultural da sociedade.

Dentro deste contexto, entretanto, da mesma forma como cada vez mais pessoas se tornam usuárias assíduas desse canal, cresce também o número de pessoas mal intencionadas, interessadas em obter algum tipo de vantagem ou simplesmente prejudicar terceiros, através de ataques na rede.

Dentre os inúmeros tipos de ataques, o ataque distribuído de negação de serviço (*Distributed Denial of Service* (DDoS)) é considerado um dos mais destrutivos (INFO, 2011), por visar, em geral, alvos importantes, como por exemplo, portais governamentais, servidores de conteúdo e servidores de DNS.

A perda de conexão ou a impossibilidade de acesso à alguns registros fundamentais pode significar desde pequenos prejuízos financeiros até a paralisação geral de serviços governamentais e corporativos associados à Internet.

Seguindo este raciocínio, sistemas e mecanismos de proteção contra ataques de qualquer espécie na Internet tornaram-se igualmente indispensáveis. Sem segurança, a experiência do usuário pode estar comprometida.

Vale salientar que a expressão "ataques DDoS compostos", embora não seja considerada oficial, será empregada frequentemente nesse projeto para indicar a combinação de vários ataques DDoS ocorrendo em conjunto na mesma ofensiva. A utilização de um novo termo para indicar especificamente esse tipo de ataque vem da carência de definições existentes e também para realçar as características inéditas dessa modalidade de ataques DDoS.

1.1 CONTEXTO

Inúmeros eventos acerca de ataques cibernéticos são diariamente relatados, e essa estatística é cada vez mais significativa tanto para o número

de ocorrências quanto para o número de novos ataques. Considerando ataques DDoS, essa realidade não é diferente.

A figura 1.1, representa o crescimento em largura de banda utilizada nos ataques DDoS reportados através dos anos por um dos provedores de serviços que participam do *World Wide Infrastruture Security Survey* (ARBOR, 2010).

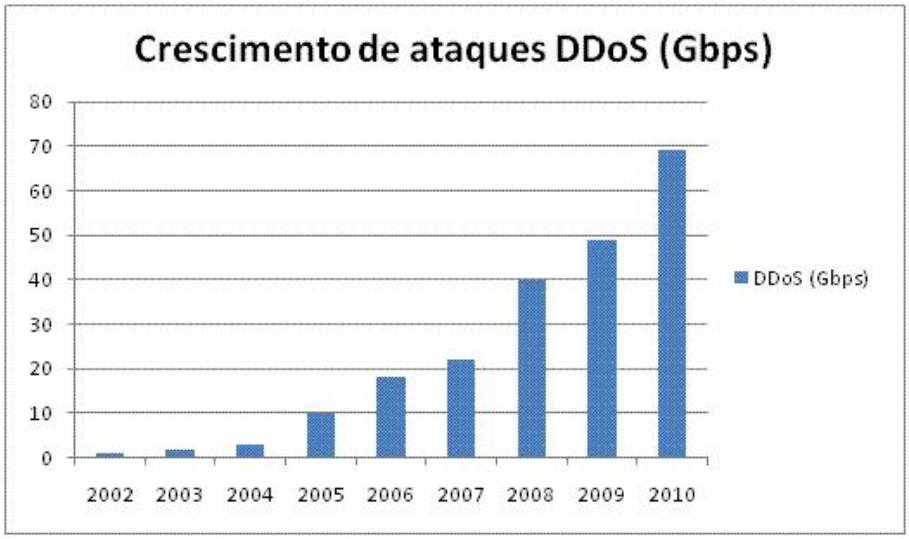

FIG. 1.1: Crescimento de ataques DDoS (Gbps) através dos anos.

Como exemplo, pode-se citar a onda de ataques direcionada à portais da Internet de ministérios, partidos políticos, bancos e jornais, entre outras entidades da Estônia, que segundo (TRAYNOR, 2007), quase conduziram aquela nação ao colapso.

Já no contexto militar, a exploração dos sistemas de informação estabelecidos pelas forças inimigas durante o transcurso de suas operações, pode levar a uma superioridade no campo de batalha (DUTRA, 2007). Para reforçar essa preocupação, o Exército Brasileiro criou o Centro de Defesa Cibernética do Exército e ativou o Núcleo do Centro de Defesa Cibernética do Exército (DCT, 2010).

Os principais ataques ocorridos relacionados ao tema são listados abaixo:

- O primeiro grande ataque envolvendo servidores DNS ocorreu em janeiro de 2001. O alvo foi o **register.com** (UNISOG, 2010). Este ataque forjava requisições para os registros MX da **aol.com**, e durou cerca de uma semana.

- Em duas ocasiões os atacantes realizaram ataques DDoS em servidores raiz de DNS. O primeiro ocorreu em outubro de 2002 e interrompeu o serviço em 9 dos

13 servidores raiz. O segundo ocorreu em fevereiro de 2007 e causou rupturas em dois dos servidores raiz (ICANN, 2007).

- Nas semanas que antecederam a guerra de cinco dias na Ossétia em 2008, ataques de DDoS foram direcionados aos portais governamentais da Geórgia que sobrecarregou e derrubou vários servidores georgianos, incluindo o portal do presidente e o portal do Banco Nacional da Geórgia. Na ocasião, apesar das acusações o governo russo negou envolvimento (MARKOFF, 2008).

- Durante os protestos nas eleições Iranianas em 2009, ativistas estrangeiros encontraram uma maneira de ajudar a oposição lançando ataques de DDoS contra o governo do Irã. (SHACHTMAN, 2009).

- Em 6 de agosto de 2009 diversos portais, incluindo o Twitter, Facebook, e páginas de blogs do Google foram alvo de ataques de DDoS (TWITTER, 2010) (WORTHAM, 2009).

- Uma ofensiva conhecida como 7.7 DDoS foi iniciada na manhã de 4 de Julho de 2009, e durou quatro dias. O ataque ocorreu contra uma série de portais comerciais e governamentais dos EUA e Coréia do Sul (LEE, 2010).

- A ofensiva 3.4, iniciada em 4 de março de 2011 contra alguns portais da Internet da Coréia do Sul, semelhante ao ataque 7.7 ocorrido dois anos antes no mesmo país, utilizou diferentes tipos de ataques DDoS conhecidos de maneira combinada, ou seja, diversos ataques DDoS diferentes atacando os mesmos alvos e ocorrendo ao mesmo tempo (AHNLAB, 2011).

- Ano passado, o caso Wikileaks repercutiu pelo mundo. O portal que publica notícias de fontes anônimas, e informações confidenciais vazadas de governos e empresas, entrou em guerra cibernética contra as instituições que foram consideradas contra o Wikileaks. Inicialmente, o portal teria sofrido um ataque e ficado indisponível após a divulgação de documentos secretos do exército norte-americano que relatavam a morte de milhares de civis na guerra do Afeganistão. Como resposta, um grupo de *crackers*[1] se mobilizou para contra-atacar empresas de cartão de crédito que teriam

[1]Como são conhecidos os usuários que se destinam a práticas que podem vir a prejudicar terceiros ou o comportamento normal das redes de computadores

bloqueado doações para o portal (G1, 2011). A figura 1.2 apresenta o terceiro dia de ataques contra o portal do Wikileaks, em 1 de dezembro de 2010. Na figura, o tráfego em vermelho representa DDoS.

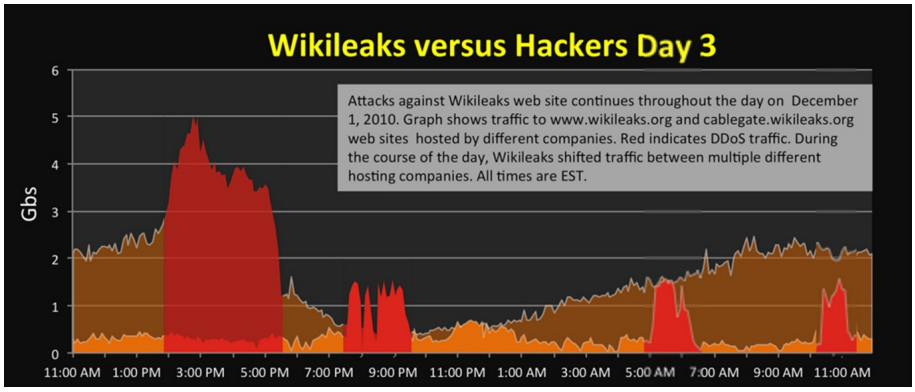

FIG. 1.2: Mapeamento do terceiro dia de dia ataques contra o Wikileaks (ARBOR, 2010).

1.2 MOTIVAÇÃO

Ataques DDoS não objetivam interceptar informações sigilosas de terceiros. A princípio, esse tipo de ataque tem o objetivo de interromper ou dificultar o acesso à serviços dos alvos. Essa natureza destrutiva faz com que o momento do ataque seja considerado um ponto difícil de se mapear, pois sua ação se dá através de comunicações muitas vezes consideradas normais pelos sistemas de segurança, já que utilizam protocolos comuns[2], sem nenhum tipo de assinatura de código malicioso, e por isso, a princípio, são consideradas comunicações legítimas.

A diferença de um ataque ocorrido há cinco anos para um ataque atual se dá pela força de trabalho[3] investida nesse ataque, uma vez que a capacidade dos servidores modernos de suportar milhares de comunicações paralelas também tenha aumentado significativamente. No entanto, ainda é possível encontrar ataques DDoS eficazes que utilizam a mesma técnica empregada há 10 anos.

Por essa característica peculiar (ataque disfarçado de tráfego legítimo[4]), os ataques DDoS vêm sendo estudados há anos. Com intuito de evitar ataques DDoS, corporações

[2]Protocolos comumente utilizados: TCP, UDP e ICMP.

[3]Por força de trabalho entende-se a quantidade de máquinas zumbis infectadas, e a quantidade de pacotes enviados por segundo.

[4]Tráfego de ataques que se assemelham a conexões de usuários legítimos, dificultando a sua identificação.

privadas e instituições acadêmicas estão pesquisando maneiras de detectar e mitigar essas ameaças, propondo e experimentando diversos mecanismos de defesa.

Sistemas de detecção de ataques cibernéticos são utilizados diariamente, e sua necessidade, assim como a da própria Internet, já não é mais colocada em dúvida. É de conhecimento irrestrito que equipamentos diretamente conectados à grande rede devem utilizar algum tipo de mecanismo de defesa aos ataques e vírus existentes.

Apesar da preocupação dos usuários indicar um importante passo para a erradicação dessas ameaças, os ataques se tornaram cada vez mais rebuscados e difíceis de tratar e ainda continuam sem uma solução definitiva. O assunto é tratado como um problema em aberto e dispõe de uma ampla literatura relacionada, além de ser alvo de estudo de diversos acadêmicos e empresas especializadas.

1.3 OBJETIVO

Neste estudo foi desenvolvido um método de detecção de ataques DDoS compostos. O método é implementado através do Algoritmo de Detecção de Ataques DDoS Compostos, que tem o objetivo de identificar a ocorrência desses ataques a partir da coleta de *traces* na saída de uma rede. Os *traces* então são submetidos à análise pelos filtros sequencias que compõe o algoritmo e procuram por características de ataques DDoS compostos.

O método ainda propõe a baixa utilização de memória por parte do equipamento processador dos *traces*, uma vez que se concentra em um passado recente da rede e não objetiva armazenar informações do perfil da rede ou assinaturas de tráfego malicioso.

Por fim, o algoritmo desenvolvido independe de sincronização com outras redes ou sistemas autonômos, o que permite a fácil utilização na saída de redes, possibilitando ao administrador encontrar usuários infectados que possivelmente estarão consumindo indevidamente os recursos da rede.

Ao longo do texto será possível compreender melhor a estrutura e natureza do ataque, como é executado, e a partir de quais premissas o método foi elaborado.

Os capítulos a seguir explicam o método elaborado, iniciando por uma apresentação do escopo teórico do projeto através do capítulo 2. O capítulo 3 explica a metodologia empregada na implementação do método de detecção e a elaboração dos filtros de pacotes. No capítulo 4 são apresentados os testes realizados e os resultados obtidos. Já no capítulo 5, será realizada uma análise qualitativa do método e apresentadas as considerações finais sobre o trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Na medida em que o ser humano evoluiu, desde épocas remotas até os dias de hoje, muitos objetos e artefatos ganharam notoriedade pelo seu valor material e, o simples fato de possuir determinados bens, principalmente a partir do contexto de sociedade econômica de hoje, fez com que muitos homens fossem invejados e admirados. No entanto, um bem, não material, mas sim abstrato, a informação, também ganhou notoriedade em nossa sociedade, e até hoje o detentor de determinada informação pode se destacar em meio à milhões de semelhantes da mesma maneira.

Historicamente, o possuidor de informações privilegiadas obteve vantagem sobre aqueles que não as possuía, sejam intelectuais, financeiras ou estratégicas.

Nas últimas décadas, o uso da Internet proporcionou o fenômeno da globalização das informações e da difusão do conhecimento entre as pessoas, uma verdadeira inundação de informações. Hoje em dia é possível encontrar informações sobre os mais diversos assuntos em variados níveis de aprofundamento.

Tal fenômeno não apenas alterou a maneira como a sociedade funciona, seja no mundo dos negócios, no ensino, nas comunicações, colocando em evidência detentor da informação, mas também alterou a maneira como o indivíduo está se adaptando ao meio, seja a partir de novas formas de relacionamento, lazer ou trabalho, mas principalmente, como cada um seleciona as informações ao seu redor.

Na medida em que as tarefas diárias migram para o mundo virtual, a dependência da infraestrutura da Internet aumenta. Porém, essa mudança significativa do comportamento da sociedade não foi capaz de impedir que hábitos antigos deixassem de existir no ambiente cibernético.

Hoje em dia milhares de pragas, vírus e ataques maliciosos infestam redes de computadores inteiras, inclusive a Internet. Motivados em obter vantagens sobre determinados alvos, os *crackers*, a partir de suas ações, ameaçam o bom funcionamento da rede e representam um grande perigo aos usuários regulares, pois em geral buscam roubar ou danificar informações privilegiadas.

O termo “ataque DDoS” está inserido dentro do contexto de ataques em redes de computadores, que por sua vez está inserido dentro do contexto mais amplo de segurança

da informação.

2.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação visa proteger contra ameaças à confidencialidade, integridade e disponibilidade das informações e dos recursos sob sua responsabilidade (BRINKLEY, 1995).

Por confidencialidade entende-se a não disponibilidade ou revelação da informação a indivíduos, entidades ou processos não autorizados. Integridade refere-se à propriedade de salvaguarda da exatidão e completeza dos ativos. E por fim, disponibilidade é a propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada (ABNT, 2006).

2.1.1 ÁREAS DE ESTUDO

A área da segurança da informação compreende o padrão para sistemas de gestão da segurança da informação que é normatizada pela ISO 27001 ABNT ISO/IEC 27001:2006 (ISO, 2006) e promove a adoção de uma abordagem de processo para estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI de uma organização (ABNT, 2006).

Através dos temas: Políticas de segurança; Organização da segurança da informação; Gestão de ativos; Segurança em recursos humanos; Segurança física e do ambiente; Gerenciamento das operações e comunicações; Controle de acesso; Aquisição, desenvolvimento e manutenção de sistemas de informação; Gestão de incidentes de segurança da informação; Gestão da continuidade do negócio; e Conformidade (ABNT, 2006), a norma lista as recomendações para apoiar os controles especificados.

Dentre os objetivos de controle referenciados pela norma, a seção de Gerenciamento da segurança em redes é umas das áreas tratadas, e objetiva garantir a proteção das informações em redes e a proteção da infraestrutura de suporte (ABNT, 2006).

2.2 SEGURANÇA DE REDES DE COMPUTADORES

Em redes de computadores, a atenção é focada na comunicação entre os equipamentos e protocolos. A segurança da informação pode ser realizada através de diversas técnicas e mecanismos a partir das camadas de redes de computadores.

Na camada física, as linhas de transmissão, quando não são bem isoladas fisicamente, representam possibilidade de interceptação na comunicação. Na camada de enlace, as informações transmitidas em texto claro podem ser lidas quando interceptadas. Já na camada de rede, IPs falsos e tráfegos não permitidos devem ser bloqueados para que não haja fluxo desnecessário ou malicioso. Na camada de transporte é possível criptografar conexões inteiras, fim a fim, no intuito de impedir a captura e a interpretação dos dados. Por fim, pode-se tratar questões como autenticação do usuário e não repúdio na camada de aplicação a fim de garantir conexões confiáveis.

2.2.1 ATAQUES EM REDES DE COMPUTADORES

De acordo com (KOTENKO, 2003), todas as noções a respeito da segurança são estruturadas a partir do conhecimento das intenções do atacante em relação às vítimas. Essas intenções são apresentadas em (GORODETSKI, 2002) e (KUHL, 2007) e representadas a seguir e em ordem:

- 1. Identificação dos *hosts*, Serviços e Sistema Operacional;
- 2. Mapeamento dos recursos compartilhados, usuários, grupos e aplicativos;
- 3. Ganhar acesso aos recursos do *host*;
- 4. Escalonar privilégios em relação aos recursos do *host*;
- 5. Realizar violação de Sigilo e de integridade; e
- 6. Criar *backdoors*.

Em (MIRKOVIC, 2002) é discutida uma taxonomia para os ataques de DDoS considerando os aspectos mais relevantes. Os ataques são divididos em quatro principais aspectos:

- Automação: O processo de preparação de um ataque DDoS envolve a localização de *botnets* e o envio do comando de início de ataque para as mesmas.
- Vulnerabilidade: Um ataque DDoS pode explorar falhas no sistema alvo para causar a negação de serviço.
- Dinâmica da Taxa de Ataque: A dinâmica da taxa de ataque especifica como a ofensiva se distribui ao longo do tempo.

- Impacto: Os ataques DDoS também são classificados quanto ao nível de impacto causado à vitima. (LEE, 2010)

2.2.2 ATAQUES

a. UDP *flood*

O UDP *flood* é amplamente utilizado em ataques DDoS e sua ação consiste em enviar, em larga escala, pacotes a portas aleatórias de um *host* atacado.

Uma vez que o pacote chega ao seu destino, o *host* remoto verifica para qual porta e aplicativo aquele pacote está destinado. Após checar que não existe serviço na porta indicada, o servidor atacado prepara um pacote ICMP *Destination Unreachable* como resposta para informar o suposto usuário que a solicitação de servido não poderá ser atendida.

Desta maneira, tendo que responder a uma grande quantidade de requisições, o servidor atacado se torna inacessível para usuários legítimos.

Geralmente os endereços de origem dos pacotes são gerados aleatoriamente, o que torna ainda mais difícil a identificação da origem do ataque.

b. ICMP *flood*

Os ataques através dos pacotes ICMP são semelhantes aos ataques UDP. Um método conhecidos de ataque ICMP é apresentado a seguir:

b.1. Smurf attack

O atacante envia um pacote ICMP *echo request* com endereço de origem da vítima para o endereço de *broadcast* de uma rede intermediária. Todos os *hosts* da rede intermediária enviam pacotes ICMP *echo reply* para a vítima.

c. TCP SYN *flood*

O TCP SYN *flood* atua com a intenção de sobrecarregar o alvo atacado através de solicitações sucessivas de conexão. O mecanismo consiste em explorar o processo de estabelecimento de conexão em três vias (*three-way handshake*) do protocolo TCP. Para cada requisição TCP SYN, o servidor aloca recursos para o restante do processo de conexão. Os agentes iniciam múltiplas conexões que nunca são concluídas, esgotando os recursos do servidor.

A figura 2.1 exemplifica este processo. Enquanto a primeira imagem representa o processo de uma conexão TCP regular, a segunda representa um atacante alocando os recursos do servidor através de solicitações sucessivas de conexão, enquanto o usuário

legítimo fica impossibilitado de usar o serviço. O ataque consiste em executar um grande número de solicitações (aparentemente regulares) de conexões TCP através de pacotes SYN, fazendo com que o servidor responda à solicitação com o pacote SYN-ACK, como parte do procedimento padrão, e aguarde pela confirmação através do pacote ACK, que, propositadamente, não é enviado em resposta pelo atacante, deixando o servidor ocupado, aguardando a resposta de conexão. Em determinado momento, o servidor fica impossibilitado de responder à conexões legítimas devido ao grande de número de solicitações em aberto que foram alocando recursos progressivamente.

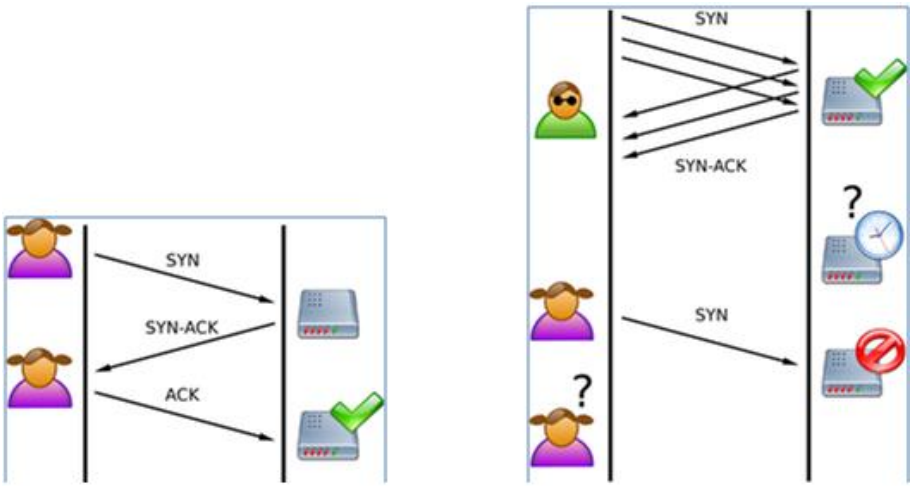

FIG. 2.1: Ataque TCP Flood

d. HTTP GET Request Flood

A partir do crescimento contínuo do uso da Internet, os serviços WWW tornaram-se um dos mais importantes aplicativos atualmente, geralmente utilizando o protocolo HTTP através da porta 80. Devido ao seu grande uso, a maioria dos mecanismos de segurança na Internet deixa liberada a porta TCP 80 com a finalidade de liberar o tráfego HTTP. Infelizmente, essa característica tornou o ataque HTTP como sendo um dos mais utilizados atualmente.

O mecanismo estabelece uma sessão TCP regularmente, realizando o *three-way-handshake* e respondendo à requisições de conexão, o que requer um IP genuíno. Sua ação ocorre na camada de apresentação, através de inúmeras solicitações de conteúdo ao servidor, preferencialmente de maneira diversificada, o que causa, em larga escala, a indisponibilidade do serviço e também atrapalha a detecção do ataque por se assemelhar ao comportamento de uma solicitação legítima.

2.3 DOS E DDOS

A figura 2.2 exemplifica o cenário de um ataque distribuído, onde o atacante lança mão de máquinas intermediárias - Mestres - para aumentar o grau de anonimato e diminuir o tráfego necessário para o envio de comandos aos escravos (LEE, 2010).

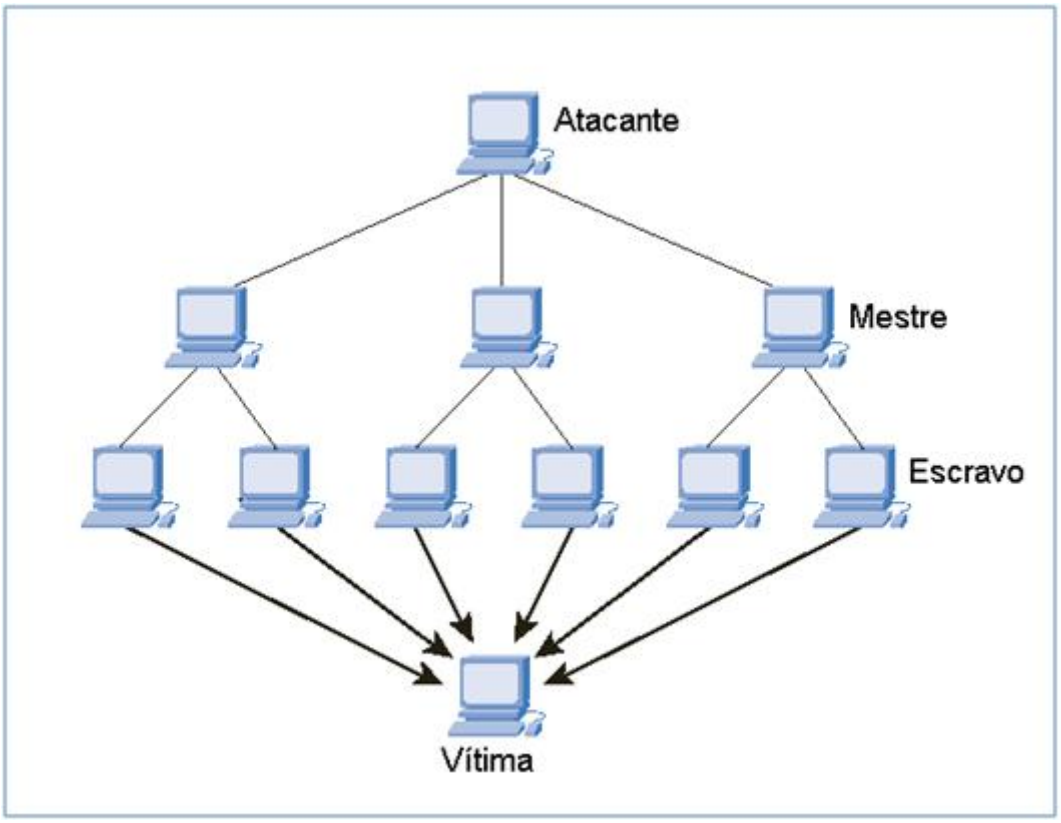

FIG. 2.2: Ataque Distribuído de negação de serviço.

Alguns prognósticos ajudam na percepção de um ataque DDoS em andamento e podem ser fundamentais para análise e mitigação desses mecanismos. Lentidão, impossibilidade de acesso a serviços na rede, portal e arquivos são consequências comuns em ataques DDoS.

2.3.1 ATAQUES DDOS COMPOSTOS

Uma forte tendência dentre alguns dos ataques DDoS mais recentes é a utilização combinada de diversos ataques DDoS distintos. Dois ataques específicos são objetivados nesse projeto: o ataque 7.7 e o ataque 3.4, ambos ocorridos na Coréia do Sul que utilizaram a ação de diversos ataques combinados.

A combinação entre essas ofensivas torna o ataque mais difícil de ser detectado, uma vez que sua assinatura passa a ser mais complexa. A tabela 2.1 apresenta os tipos de ataques utilizados em 7.7 e 3.4.

INVESTIDA	7.7 DDoS (2009)	3.4 DDoS(2011)
Tipos de Ataque	-HTTP Get Flooding -Non-Spoofed ICMP Floodind -Spoofed ICMP Floodind -Non-Spoofed UDP Floodind -Spoofed ICMP Floodind	-HTTP Get Flooding -Non-Spoofed ICMP Floodind -Non-Spoofed UDP Floodind

TAB. 2.1: Ataques DDoS compostos, retirada de (AHNLAB, 2011).

Já a figura 2.3 apresenta a proporção de ataques DDoS utilizada na ofensiva 3.4.

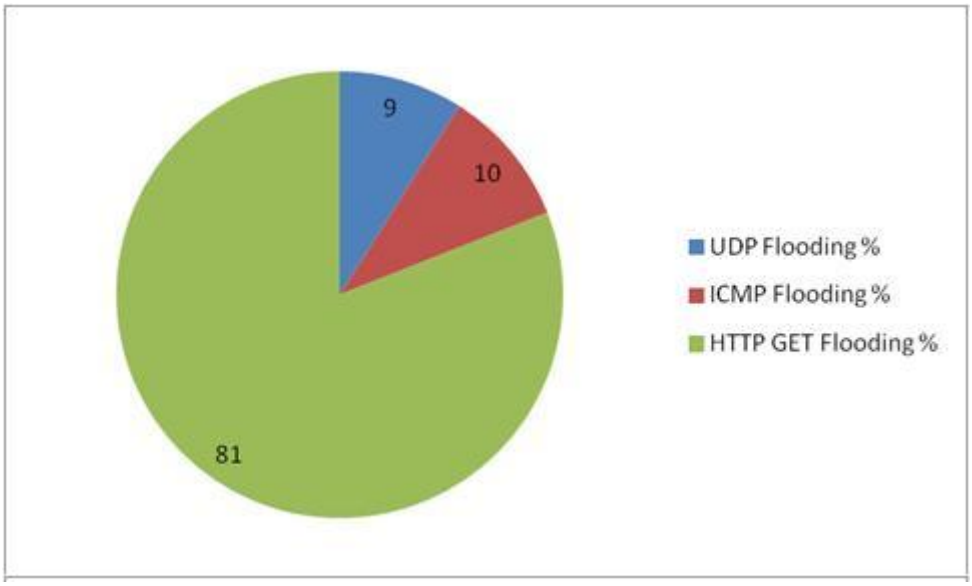

FIG. 2.3: Tipos de tráfego do 3.4, retirada de (AHNLAB, 2011).

2.4 DEFESA DDOS

Uma vez que a ameaça se torna clara e bem definida, os principais alvos desses ataques necessitam também de técnicas igualmente apuradas para realizar sua defesa. Sabendo que na maioria das vezes o ataque de DDoS se passa por tráfego legítimo, algumas técnicas e equipamentos são apresentados a seguir.

a. Equipamentos

Equipamentos e aplicativos de segurança são utilizados no intuito de combater e identificar não só os ataques de DDoS, mas também qualquer outro ataque conhecido que exista em redes de computadores.

Firewalls, IDS/IPS, antivírus, serviços de autenticação e treinamento dos usuários acerca das boas práticas de utilização e segurança, são mecanismos utilizados para impedir que qualquer tipo de ataque se forme ou se instale.

b. Técnicas

As técnicas de defesa objetivam separar o tráfego legítimo do malicioso. Além de identificar os ataques existentes, devem ser capazes de reconhecer comportamentos suspeitos não mapeados.

Segundo (MIRKOVIC, 2002), os mecanismos de defesas são divididos em dois principais aspectos:

- Nível de atividade: é classificado como sendo reativo quando tem o intuito de combater o ataque uma vez que ele já existe e é identificado, ou como sendo preventivo quando atua tanto no combate de ataques existentes, mas também na prevenção da ocorrência dos mesmos.

- Localização: que diz respeito à localização da implementação do mecanismo de defesa.

Além disso, é sempre importante realizar treinamentos com usuários acerca das boas práticas de utilização e segurança, uma vez que, na maioria das vezes, são os próprios usuários que autorizam a entrada e espalham os muitos tipos de vírus existentes no mundo cibernético.

A seguir são apresentados as quatro principais abordagens para executar a defesa contra ataques DDoS: prevenção; detecção; análise e identificação; e reação e mitigação.

2.4.1 PREVENÇÃO

Evita o acontecimento de ataques DDoS antes que possa causar danos ao alvo. Mecanismos de prevenção de DDoS não são relacionados à prevenção de formação de *botnets*, e prevê mecanismos de análise de pacotes diretamente de roteadores (PENG, 2007).Essa técnica consiste em detectar a ocorrência de pacotes spoofados[5] na rede.

[5]Termo técnico designado para especificar que um pacote possui seu endereço IP de origem modificado e não é legítimo na rede, o que dificulta a localização do verdadeiro verdadeiro *host* de origem desse pacote

2.4.2 DETECÇÃO

Após a prevenção dos ataques, o próximo passo para defesa de ataques DDoS é a detecção. A detecção de ataques pode significar mais tempo para se preparar para uma reação, protegendo assim os usuários, além de poder ajudar na identificação do atacante para que ações legais sejam tomadas (PENG, 2007).

Ataques DDoS simulam tráfego real, inclusive, podem ser gerados a partir de tráfegos genuínos, gerados de usuários que decidiram, em conjunto, organizar ataques contra determinados alvos utilizando ferramentas de ataques, como ocorrido no caso *wikileaks*[6].

O fenômeno de *flash crowds* é um exemplo de tráfego legítimo que pode ser confundido com um ataque DDoS. *Flash crowds* são grandes quantidades de tráfego legítimo direcionado a alguns portais específicos na Internet dentro de um tempo relativamente curto de tempo. Geralmente ocorrem em portais populares, quando milhares de requisições de acesso a esses servidores chegam simultâneamente. Flash Crowds são bem similares a ataques DDoS em termos de anomalia e fenômeno de tráfego; de fato, algumas vezes, podem causar lentidão no portal e até mesmo derrubar o servidor devido ao significante aumento no tráfego (ARI, 2003), (MAYUR, 2007), (RACHEV, 1991) e (ZHOU, 2008).

As técnicas de detecção DDoS mais populares se dão através da análise de informações contidas nos pacotes da rede, ou através da análise das informações extraídas dos fluxos de comunicações estabelecidos na rede, em outras palavras, segundo (PENG, 2007), existem dois tipos de técnicas de detecção de ataques DDoS. A primeira técnica é baseada em características específicas dos ataques DDoS, já a segunda técnica é baseada na modelagem do comportamento normal do tráfego.

Na análise de informações contidas nos pacotes da rede, rastreia-se por assinaturas de pacotes não legítimos. Na análise de informações extraídas dos fluxos de comunicações estabelecidos na rede, o rastreamento se dá por encontrar anomalias nas tendências de comportamento do tráfego.

É exatamente nessa segunda técnica de detecção de ataques DDoS, conhecida como Detecção baseada em anomalias *(anomaly-based detection)* em que o projeto está inserido.

[6]Um grupo formado por manifestantes auto-intitulado Annonimous contra-atacou ao boicote do weakleaks instalando um aplicativo de ataque em seus próprios computadores e gerando ataques DDoS em horas agendadas

2.4.3 ANÁLISE E IDENTIFICAÇÃO

Uma vez que o ataque foi detectado, idealmente, o próximo passo seria o bloqueio do tráfego gerado em sua origem. Infelizmente, devido a características de eficiência e escalabilidade provenientes da Internet e do protocolo IP, os roteadores tomam decisões de roteamento baseados no próximo salto e não retêm informações sobre o caminho ou origens dos pacotes, o que dificulta bastante o rastreamento dos ataques (PENG, 2007). De maneira a resolver essa limitação várias técnicas e mecanismos baseados na mudança do funcionamento de equipamentos e protocolos foram propostos.

2.4.4 REAÇÃO E MITIGAÇÃO

Uma vez que o ataque é detectado e identificado existe pouco tempo de reação contra este ataque, e a primeira ação a ser tomada deve ser a proteção do local que se caracteriza como o gargalo da rede[7]. No entanto, se o ataque for robusto o suficiente, outros gargalos irão aparecer ao decorrer do tempo (PENG, 2007).

2.4.5 ESTADO DA ARTE

Imediatamente após o primeiro ataque de larga escala, muitos pesquisadores se dedicaram ao novo problema de parar, mitigar, e filtrar ataques DDoS nas máquinas alvo (MIRKOVIC, 2002).

A partir das quatro abordagens de defesa de ataques DDoS apresentadas anteriormente, são discutidas a seguir algumas importantes técnicas e métodos desenvolvidos de defesa DDoS.

a. Prevenção de ataques

- Em (FRANÇOIS, 2012) é criado um sistema de prevenção de intrusão (IPS) como parte do algoritmo nomeado como *FireCol* e, que fica localizado nos provedores de serviços de Internet (ISPs). O IPS atua trocando informações específicas com os *hosts* no intuito de defender a rede

- A **filtragem do tráfego de entrada e saída da rede** foi originalmente proposto por (FERGUSON, 2000) e tem o propósito de apenas liberar o tráfego para entrar

[7]Ponto onde o fluxo de chegada do tráfego é maior do que a capacidade de encaminhamento por parte de um equipamento ou limitação de banda.

ou sair de uma determinada rede se o seu endereço de origem for reconhecido a partir de uma tabela previamente determinada de endereços.

b. Detecção de ataques

- Em (WANG, 2011) é apresentado um método de detecção de ataques DDoS baseado na análise da distriuição do tráfego da rede a partir da correçação dos endereços IP. Em caso de ataques, a disperção de endereços IP torna o tráfego da rede assimétrico em comparação ao aumento de tráfego normal naquela rede, que apresenta um tráfego de rede simétrico.

- Em (OSHIMA, 2012) é proposto um método nomeado de **CSDM (Chi-Square-based Space Division Method)**. Os experimentos levaram em consideração o endereço IP de origem, ó número da porta de destino e o intervalo de tempo de chegada dos pacotes com o propósito de melhorar a precisão da detecção de ataques DDoS.

- Em (JUN, 2011) é apresentado um mecanismo de detecção de ataques DDoS baseado no cálculo da entropia de informações dos pacotes por um determinado período de tempo.

c. Identificação de ataques

- Em (CASTELUCIO, 2008) é apresentado um sistema que cria uma rede sobreposta de rastreamento de trafego IP a ser implementada no nivel de Sistemas Autonomos, proposto para atuar em redes de grande porte. O sistema porpõe a criação de um novo Community Attribute para o protocolo BGP, que é responsável por identificar qual Sistema Autônomo possui o sistema de rastreamento IP proposto instalado. É proposto também um mecanismo de marcação de sequência dos roteadores, a ser usado antes do pacote ser marcado por um roteador de borda de um Sistema Autônomo.

d. Reação de ataques

- Em (JING, 2006), o método de *rate limit*[8], o qual consiste em, uma vez que detectado o ataque, estabelecer taxas limites de tráfego para serem implementadas próximas às origens do ataque.

[8]limitação da taxa

3 METODOLOGIA

Nesse capítulo será apresentado o método no qual o algoritmo proposto foi elaborado, o processo no qual ele foi idealizado e os porquês e mecanismos das funcionalidades dos filtros.

3.1 TRABALHOS RELACIONADOS

- O **D-WARD** (MIRKOVIC, 2003b) é um mecanismo de segurança que analisa dados estatísticos da rede de origem no intuito de encontrar anomalias. O mecanismo monitora o comportamento de cada fluxo de comunicação de cada rede de orgiem. D-WARD procura sinais de dificuldades de comunicação, tais como uma redução no número de pacotes de resposta ou longos tempos de resposta. Periodicamente, compara os valores observados das estatísticas geradas pela comunicação dos pares com as estatísticas de um modelo de tráfego normal previamente estabelecido. Se a comparação revela a possibilidade de um ataque DDoS, D-WARD responde pela imposição de uma restrição no fluxo suspeito de saída para este ponto.

- Em (MUKHOPADHYAY, 2007), o autor apresenta o estudo feito a partir de métodos distintos para lidar com ataques DDoS. No estudo são discutidas, entre outras, três recentes técnicas de *active filtering* (filtragem ativa):

  Em (XUAN, 2001) é proposto um sistema de defesa para detectar ataques e controlar o tráfego através da implementação de diversos *gateways* analisadores de tráfego espalhados na rede;

  Em (YAAR, 2004) é proposto um esquema de marcação de pacotes, o qual modifica cada pacote da rede e de acordo com essa marcação controla o acesso do tráfego;

  Em (PENG, 2003) é construída uma base de dados baseado no histórico de todos os pacotes IP originados de uma rede e, através da checagem dos pacotes, é determinado se o endereço IP do pacote pertence ou não ao banco de dados.

- Em (FEINSTEIN, 2003) é introduzida pela primeira vez o conceito de entropia e

distribuições de frequência de um atributo do pacote IP no auxílio à identificação de ataques DDoS;

- Em (WANG, 2010) é utilizado um método para detecção de anomalias no tráfego IP analisando o número de conexões distintas entre os IPs de origem e de destino, onde a mudança do comportamento normal dessa relação, calculada a partir da entropia, significa uma anomalia.

3.2 ABORDAGEM DO PROBLEMA

Junto com os mecanismos apresentados acima, inúmeras outras publicações sobre o tema atacam o problema.

Idealmente, ataques DDoS devem ser interrompidos o mais próximos da origem, quanto possível (MIRKOVIC, 2003a).

De acordo com (MIRKOVIC, 2003a) o sistema de defesa pode ser desenvolvido através de um sistema autônomo (*single-point ou ponto único de controle*) e também através de um sistema distribuído, que consiste em múltiplos pontos de defesa.

Um requesito para habilitar um mecanismo de segurança através de um sistema distribuído é dispor de uma infraestrutura que atravessa múltiplas redes e domínios administrativos.

Já, a implementação de defesa através de um único ponto de controle requer um mecanismo de coleta de *traces* que intercepte os dados em algum lugar estratégico entre a origem e o destino do ataque. A escolha do local de coleta varia de três maneiras distintas: próxima à vítima, nas redes intermediárias ou próximas à origem.

Embora a maior parte dos sistemas de defesa seja criada próximo aos destinos do ataque, onde é possível coletar todo o tráfego gerado pelo ataque, essa abordagem apresenta alguns fatores negativos como o tempo de resposta pequeno e um grande volume de tráfego para ser analisado (MIRKOVIC, 2003a). Ao detectar um ataque DDoS já próximo ao alvo, o tempo de ação para mitigar esse ataque será menor em relação a abordagens mais próximas à origem, uma vez que o ataque já está acontecendo e o ataque já está estabelecido. Além disso, o volume de tráfego coletado incluindo todos os tipos de fluxos já próximos ao destino é consideravelmente maior quando comparado ao volume de tráfego de redes locais, o que pode sobrecarregar o mecanismo de defesa implementado.

A partir de redes intermediárias, embora haja maior tempo de resposta comparado

aos mecanismos próximos às vítimas, o volume de tráfego gerado pode ser ainda maior (MIRKOVIC, 2003a).

Por fim, com a coleta de dados realizada próxima à origem, os problemas de volume de tráfego e tempo de resposta são minimizados. Porém, por análise próxima à origem, se entende sistemas administrativos que podem ou não fazer parte de um ataque, e que, em caso de *botnets*, iria representar apenas uma pequena parte do tráfego gerado, o que, de fato, prejudicaria em perceber o tamanho real do ataque, dificultando a percepção e detecção do ataque. Além disso, erradicar uma *botnet* em apenas uma rede não mitiga todo o ataque.

A defesa baseada na interceptação do tráfego na origem do ataque foi escolhida para ser usada nesse método, pois assim, acredita-se lidar com dilemas associados à dificuldade de detecção, o que requer um método bem elaborado, porém menos suscetível à problemas de infraestrutura e complexas topologias para testes.

A figura 3.1 apresenta uma visão geral de um ataque DDoS em andamento, incluindo os sistemas autônomos infectados, que fazem parte de uma determinada *botnet*. Na imagem, um vilão, que planeja interromper os serviços de uma determinada vítima, contrata um botmaster[9], que é reponsável por montar a *botnet*. Durante o ataque, os usuários infectados enviam requisições ao alvo continuamente. Considerando que milhares de usuários atacam ao mesmo tempo, o fluxo final já próximo ao alvo torna-se elevado, interrompendo o serviço para usuários legítimos.

3.2.1 ANÁLISE BASEADA NA COLETA DE DADOS PRÓXIMO À ORIGEM

Determinar o local de análise do tráfego pode representar um aumento considerável na complexidade do problema em termos de custo, tempo, organização, *hardware* e processamento. Algumas razões para analisar o tráfego IP próximo a origem do ataque, no limite limite das redes locais, são apresentas a seguir:

- Possibilidade de medidas de prevenção de ataques antes da negação do serviço (SECUZILLA, 2006);
- Facilidade de utilização de mecanismos *anti-spoofing*, uma vez que controlar a en-

[9]Especialista em ataques na Internet. O botmaster é a pessoa responsável por implementar um plano de ação para executar um ataque, o que envolve desde formar a botnet até determinar um momento para que as máquinas infectadas ataquem.

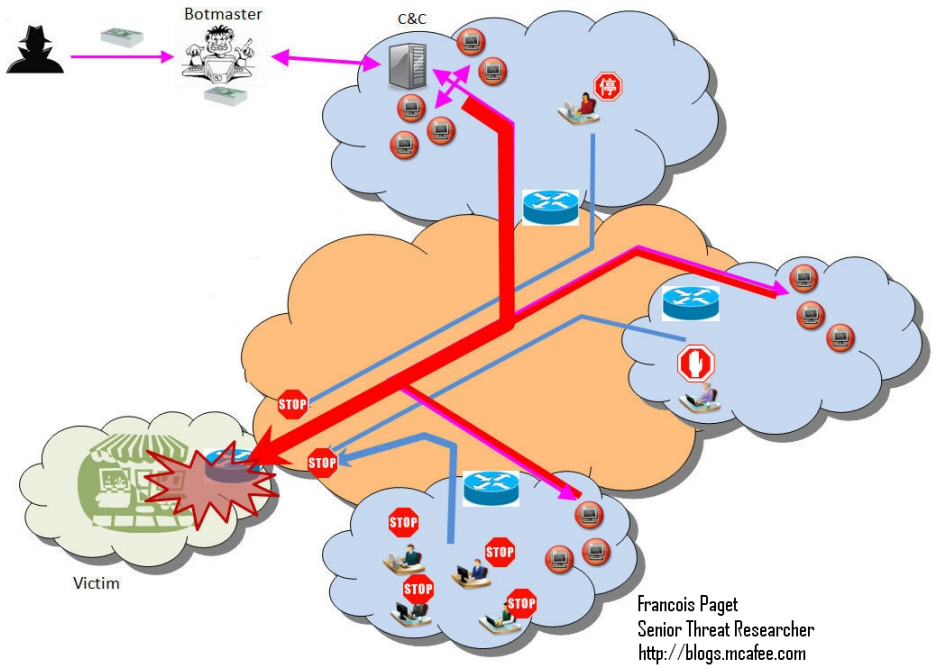

FIG. 3.1: Ataque DDoS em ação (PAGET, 2009)

trada de pacotes IP forjados ou não próximos ao destino dos ataques pode se tornar uma tarefa dispendiosa de tempo e processamento. Dentro dos limites de uma rede local uma lista de controle de acesso nos roteadores de borda seria o suficiente;

- Possibilidade de análise dos fluxos individuais de comunicação baseada em cada IP de origem, uma vez que próximo ao destino, a quantidade de IPs de origem, de um site popular, por exemplo, torna a solução custosa e complexa computacionalmente;

- Foco na gerência pró-ativa da rede, identificando máquinas infectadas que podem fazer parte de *botnets*, consumindo recursos da rede.

A figura 3.2 ilustra, a partir do cenário estabelecido na figura 3.1, a coleta do tráfego na saída de uma rede que faz parte de uma *botnet*. Um equipamento coletor de tráfego (sniffer) é incluído na saída da rede. Com isso, todo tráfego gerado dentro desse sistema autônomo, obrigatoriamente, passa pelo coletor, filtrando cada fluxo de pacotes o mais próximo possível da origem, incluindo possíveis ataques.

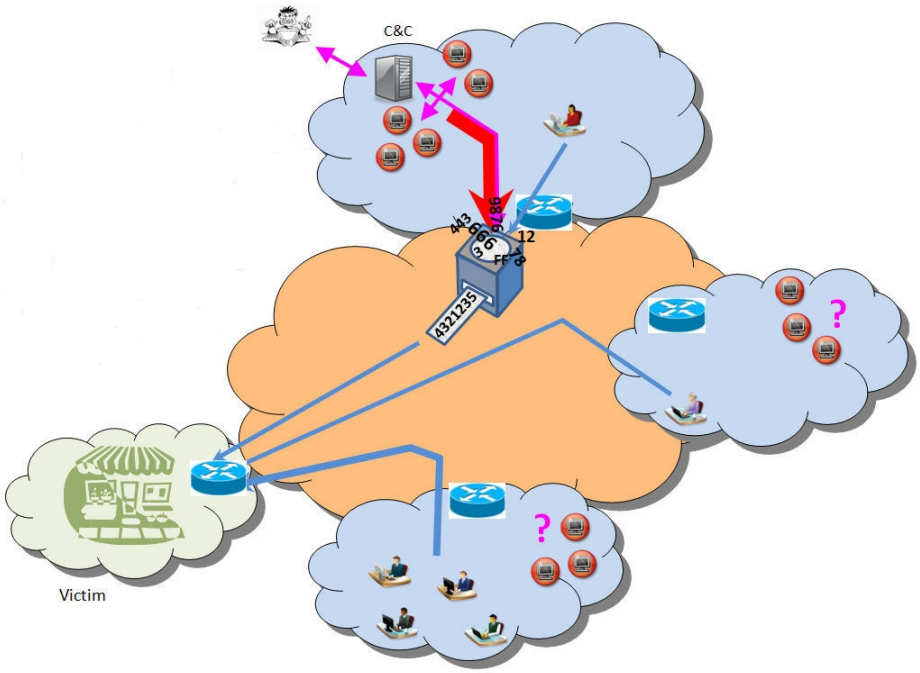

FIG. 3.2: Análise do fluxo IP baseado na origem do ataque (PAGET, 2009).

3.2.2 ANÁLISE BASEADA NA CAMADA DE REDE DO TRÁFEGO

Determinar os dados a serem analisados, dependendo do detalhamento das informações, pode representar um aumento considerável no processamento. A seguir são levantados alguns pontos que influenciaram na escolha da análise dos dados baseada na camada de rede do modelo OSI:

- Representa uma simplificação em relação à análise das camadas superiores dos pacotes, uma vez que a leitura das informações contidas nos cabeçalhos dos pacotes acima da camada de rede requer dispositivos mais caros e mais complexos, e que apresentam também um consumo de recurso maior (processamento e memória);
- Diminui o tempo de análise comparado à análise de cabeçalhos de pacotes de camadas superiores;
- Não baseado nas conexões dos usuários, o que requer uma capacidade computacional de armazenamento de dados menor;
- A abordagem do problema é baseada em quatro informações contidas no cabeçalho IP, e uma informação adicional calculada automaticamente:

- IP origem;
- IP destino;
- Protocolo;
- Tamanho em bytes;
- Registro do intervalo de envio entre os pacotes (intervalo TEMPO).

3.2.3 ANÁLISE BASEADA EM ATAQUES COMPOSTOS QUE PODEM TAMBÉM APRESENTAR CARACTERÍSTICAS DE AUMENTO DISCRETO DO FLUXO DE PACOTES

A combinação de diferentes tipos de ataques DDoS simultaneamente, somada a estratégia baseada no aumento discreto do fluxo de pacotes de ataque - crescimento e formação do ataque DDoS lento e contínuo -, representam uma evolução na maneira como os ataques estão sendo executados. Estas novas tendências em ataques DDoS têm a pretensão de superar os métodos de detecção existentes partindo de uma premissa básica: misturar o tráfego malicioso ao tráfego normal. Quanto mais semelhante a fluxos de pacotes legítimos, mais os fluxos de pacotes maliciosos de ataques DDoS se tornam difíceis de se detectar e trafegam imperceptíveis aos mecanismos de deefsa existentes na rede. A seguir, são apresentadas razões para a escolha de um método que abordasse esse tipo de ataque:

- Dificuldade de detecção pelos equipamentos da rede (KUZMANOVIC, 2003);
- Simulam tráfego legítimo, o que reforça a ideia de que métodos complexos de detecção baseados apenas no histórico do comportamento normal da rede podem não ser suficientes;
- Implementação de diversos mecanismos e métodos baseados em diferentes parâmetros. Para realizar a detecção de ataques compostos foi elaborado um mecanismo que progressivamente identifica as características dos ataques, e que pode ser reorganizado ou adaptado através de mudanças simples no algoritmo.

3.3 PROPOSTA

Objetivando elaborar um método com capacidade de lidar com ataques DDoS com as características apresentadas acima, as seguintes etapas foram alcançadas:

- Conhecer diversos tipos de ataques DDoS, preferencialmente os mais utilizados hoje em dia; Conhecer métodos de detecção de ataques DDoS e seus mecanismos, identificar seus pontos fortes e fracos;
- Elencar as melhores maneiras de lidar com o problema com as características previamente descritas.
- A partir do conhecimento adquirido, identificar um método de detecção baseado na filtragem de pacotes de uma rede.

3.3.1 ALGORITMO PROPOSTO

O método desenvolvido compreende algumas definições, conforme descritas a seguir:

- requer mecanismo *anti-spoofing*;
- captura de *traces* próximo à origem do tráfego;
- baseado na análise dos parâmetros (tempo : IP origem : IP destino : Protocolo : Tamanho do pacote) dos cabeçalhos da camada de rede dos pacotes, não nas conexões;
- coleta de dados na saída da rede local;
- Métodos estatísticos e quantitativos de análise de dados. As mudanças de comportamento são identificadas a partir da criação de um histórico recente das comunicações com origem na rede local, baseadas basicamente em contagens estátiscas (computacionalmente fácil de ser implementado em relação a processamento e armazenamento);
- Determinação de limites (*thresholds*) adaptativos (não rígidos).

Através da figura 3.3 é possível visualizar os processos pelo qual o *trace* capturado na rede percorrerá até a captação dos dados para análise e seu posterior alarme para casos de detecção de anomalia. A ilustração se desenvolve da esquerda para direita, onde, a partir do *sniffer* implementado na rede se obtém o *trace* da rede.

O *trace* é submetido ao algoritmo de detecção de ataques DDoS compostos, que por sua vez, realiza uma filtragem sequencial baseada na captação das informações contidas na camada de rede dos pacotes IP. Os filtros, explicados a seguir, processam os dados,

utilizam métodos estatísticos e quantitativos de análise, calculam os padrões de comportamento da rede e podem gerar gráficos e alarmes.

Na sequência de análise dos filtros, caso o último filtro seja alarmado, o algoritmo apresenta quais endereços IPs de origem apresentam um comportamento suspeito, o provável alvo e o perfil do tráfego gerado.

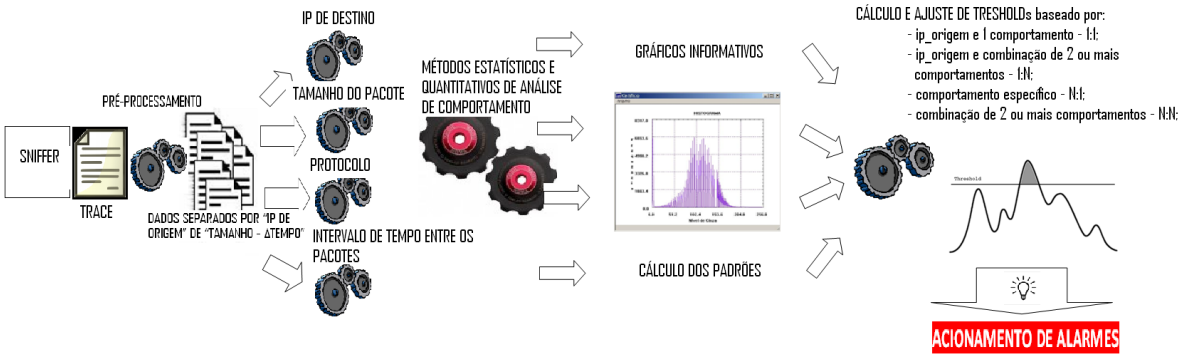

FIG. 3.3: Processo do método proposto.

A figura 3.4 situa o processo ocorrendo em relação à rede analisada. A imagem representa um sistema autônomo, parte da botnet criada na figura 3.1. De acordo com a figura 3.2, o equipamento coletor de pacotes inserido na saída dessa rede é, nessa figura, configurado para processar os dados através do algoritmo implementado. O fluxo de dados coletados se dá de dentro da rede local para fora. Conforme os dados são analisados, o algortimo pode gerar alarmes para casos de ataques DDoS combinados.

Por fim, o algoritmo de detecção desenvolvido, através de seus filtros sequenciais, que analisam as características pontuais dos ataques, inicialmente apenas geram alertas para fluxos de dados que apresentem características de ataques em conjunto, quando todos os filtros do algoritmo são acionados. Porém, é possível identificar também outras características de ataques, como aumento repentino no fluxo de pacotes e a incidência de pacotes direcionados a poucos alvos comparado ao restante da rede.

3.4 FILTROS SEQUENCIAIS DE ANÁLISE

O método proposto não utiliza a análise de assinaturas, como os equipamentos IDS o fazem, na verdade, não existe registro de atividades suspeitas que seja utilizado para futuras comparações pelo método proposto, mas sim, é realizada a análise do fluxo presente, através de um histórico recente do comportamento tráfego.

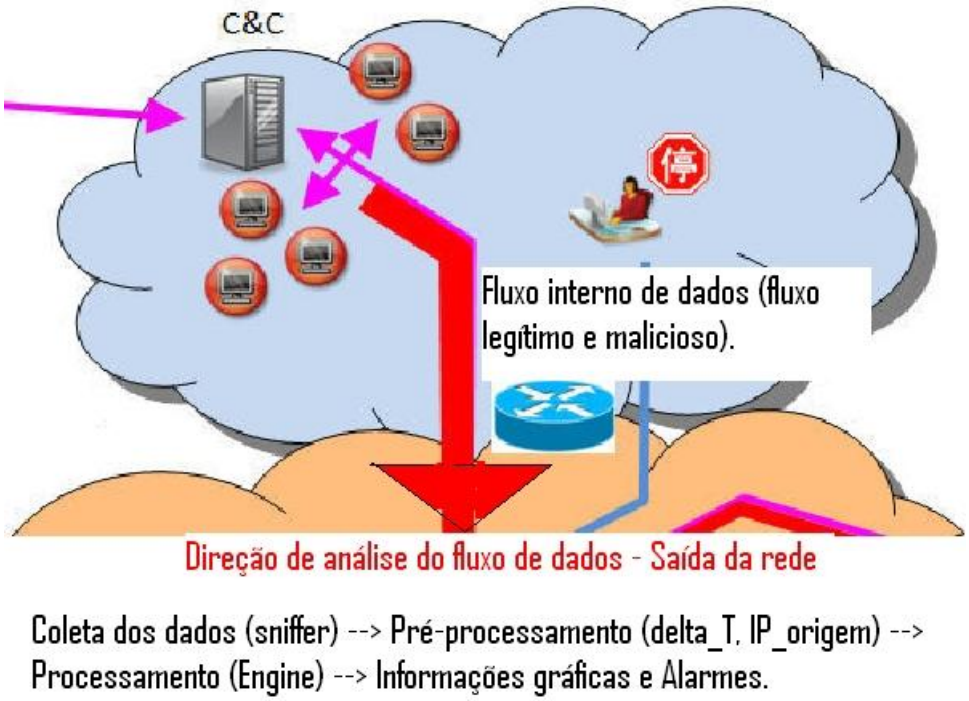

FIG. 3.4: Processo proposto em relação à rede.

É importante salientar que um dos principais efeitos desse tipo de ataque é gerar fluxos que se misturem com o tráfego legítimo, sendo utilizadas assim, diversas técnicas que, individualmente, se apresentam como parte normal do tráfego de uma rede.

Os filtros sequencias têm a função de analisar pontualmente comportamentos anômalos no tráfego de saída da rede interna, como: o aumento no volume de tráfego de maneira repentina, mesmo em pequenas escalas; a ocorrência excessiva da comunicação de usuários da origem com determinados endereços de destino comparado à comunicação de toda rede quando o volume de tráfego aumenta repentinamente; o perfil dos protocolos utilizados pelas máquinas de origem quando estão se comunicando em excesso com determinados destinos.

O método criado consiste em aplicar os filtros de análise a partir das características dos ataques mais abrangentes (pertinente à maior parte dos ataques DDoS existentes), como aumento do fluxo de pacotes na rede, seguidas por características mais específicas desses ataques, como o perfil do tráfego contido nos ataques.

O primeiro filtro é utilizado para identificar uma característica intríseca em qualquer tipo de ataque DDoS: aumento no fluxo de pacotes da rede. A motivação para alocá-lo como primeiro critério para detectar um ataque DDoS se justifica pela sua simples

implementação e baixo consumo de memória e processamento, além de ser uma característica predominante em ataques DDoS.

O filtro 2, por sua vez, além de trabalhar com um escopo mais reduzido (o filtro 1 elima o tráfego que não apresenta aumento de fluxo), trata de outra característica intríseca a qualquer ataque DDoS: procura por possíveis alvos de um possível ataque. Essa característica, caso analisada antes do filtro 1, aumentaria consideravelmente a quantidade de pacotes analisados, consequentemente, requereria uma maior capacidade de processamento. No filtro 2, os pacotes que são enviados a destinos não identificados como alvos, são descartados, assim como os pacotes provenientes de protocolos não utilizados nos ataques. Assim, ao final dos filtros 1 e 2, o escopo de análise de pacotes fica reduzido consideravelmente comparado a tráfego original e contém apenas características comuns a ataques DDoS comuns.

Por fim, o filtro 3, a partir da saída do filtro 2, processa todo o tráfego extraído de modo a analisar os pacotes agrupados pelo seu endereço IP de origem. Nesse momento então, é montado um perfil de utilização percentual de cada protocolo presente em cada origem, que por fim, gerará um perfil de utilização percentual dos protocolos mais comum entre os endereços analisados, um perfil padrão daquele fluxo. Esse perfil padrão é utilizado então para detectar cada endereço de origem com perfil semelhantel ao padrão, que esta se comunicando com alvos específicos e ainda fazem parte de um fluxo de pacotes anômalo, tal qual um Ataque DDoS Composto. O filtro 3 é o filtro com maior consumo de memória e processamento, pois realiza a edição dos *traces* de entrada e também intensivas operações de comparação de dados.

Portanto, a sequência dos filtros estabelecida no método proposto visa antes de tudo a detecção de ataques DDoS compostos a partir das características mais abrangentes para as mais específicas, mas também um baixo consumo de recursos computacionais, facilitanto sua implementação e escalabilidade para a análise de *traces*.

A seguir são apresentados os filtros sequenciais estabelecidos para o algoritmo desenvolvidos.

3.4.1 FILTRO 1 - CONTAGEM DE PACOTES

A primeira abordagem ao problema foi a detecção de uma característica peculiar aos ataques DDOS: aumento do tráfego na rede.

O filtro tem o objetivo de detectar aumentos repentinos no fluxo regular da rede.

Para isso foi preciso estabelecer um parâmetro de comparação para determinar o que é considerado fluxo normal e o que é fluxo suspeito de pacotes.

O algoritmo desenvolvido trabalha a partir de *traces* coletados de redes reais, porém, para este projeto, a análise dos *traces* ocorre de maneira *offline*, e não em tempo real, o que quer dizer que os *traces* são avaliados com seus tamanhos já determinados, são finitos. A partir deste contexto, a primeira informação que o algoritmo de Detecção de Ataques DDoS Compostos extraí é a quantidade de pacotes existentes no *trace*.

Para determinar se uma rede esta apresentando características de crescimento no fluxo de pacotes em relação ao comportamento normal dessa rede, foi preciso estabelecer um parâmetro de comparação, uma tabela dinâmica que armazenasse a quantidade média de pacotes saindo dessa rede, baseada num histórico recente do fluxo da rede. Considerando que redes de computadores não são determinísticas e, que mesmo mapeando todo o passado de comunicações de determinada rede não será possível prever o seu comportamento futuro e todas as variações de crescimento de tráfego, sejam essas variações decorrentes de momentos de pico de utilização da rede pelos usuários, seja derivado de flash crowds ou ataques.

O método propõe identificar aumentos no volume de tráfego mesmo que esse aumento não represente um ataque, ou seja, qualquer tipo de aumento deve ser identificado, pois, para manter o algoritmo simples computacionalmente, optou-se por realizar a análise do fluxo de pacotes de baseada no passado recente do fluxo dessa rede, mesmo que essa abordagem identificasse qualquer tipo de variação de crescimento no tráfego, seja qual for o motivo desse crescimento.

O passado recente da quantidade média de pacotes de uma rede é um parâmetro relativo, pois recente pode significar dias, horas, minutos e até segundos, como o algoritmo desenvolvido trabalha *offline* e com *traces* finitos, foi preciso estabelecer uma análise do tráfego por partes, ou seja, procurando por catacterísticas de ataques DDoS divindindo o trace em módulos menores e de tamanhos iguais (é usada a terminologia janelas de pacotes para designar os módulos do *trace* de tamanhos iguais), para que os próprios módulos pudessem ser usados como parâmetro de comparação do funcionamento normal da rede.

Para a análise do *trace offline* finito, a quantidade de janelas criadas a partir desse *trace* é baseada no tamanho total do *trace*, pois assim, é possível assegurar que cada *trace* analisado terá um número suficiente de janelas para que fosse possível criar uma

tabela dinâmica de comparação, capaz de armazenar informações contendo a média da quantidade de pacotes existentes nessa rede, baseada no próprio histórico do *trace*.

O tamanho da janela então é decorrente da quantidade total de pacotes do trace, e segue a seguinte abordagem, onde um número inteiro é extraído da operação abaixo:

(Tamanho_Janela = (1000*log10(numero_de_pacotes_do_trace))

Nesse ponto, é importante levantar uma discussão referente ao número de falsos negativos que podem ser criados a partir do descarte dos fluxos de pacotes que não apresentam crescimento na quantidade de pacotes a partir da abordagem acima. De fato as janelas de pacotes que não apresentam crescimento são descartadas pelo algoritmo, e é razoável entender que, possivelmente, parte do tráfego oriundo de ataques DDoS sejam descartados. No entanto, uma das características predominantes de ataques DDoS é a presença de um fluxo contínuo, intermitente de pacotes direcionado aos seus alvos e, tal fluxo malicioso, sendo identificado uma, duas, três ou inúmeras vezes no decorrer da análise, irá significar a detecção do ataque DDoS. Um falso negativo, para o caso de ataques DDoS, só é considerado caso o método deixe de detectar completamente um ataque ao longo de todo o *trace*, ou seja, a exclusão de partes do *trace* por parte do algoritmo proposto, não é determinante neste método para o aumento no número de falsos negativos.

Por fim, a partir do armazenamento das informações de quantidade de pacotes em cada janela e o conhecimento da média de pacotes, assim como o desvio padrão, poderá ser utilizado como parâmetro de comparação para cada nova janela analisada. A quantidade de janelas que compõe a tabela dinâmica de comparação foi determinada em dez, o que quer dizer que, as dez últimas janelas são levadas em consideração para determinar se a janela atual apresenta ou não crescimento relativo do volume de pacotes. O valor de dez janelas é relacionado a quantidade de janelas criadas no total, sendo que antes do algoritmo armazenar as dez primeiras janelas, a tabela vai acumulando as informações e pode ser usada como parâmetro de referência mesmo que ainda não existam dez janelas anteriores, nesses casos, são usadas as médias e desvio padrão das janelas existentes, sejam uma, duas ou nove janelas. O limite de dez janelas como base de comparação do passado recente da rede é determinado pela quantidade de janelas criadas, que esta na ordem de dezenas e centenas. As dez últimas janelas refletem um passado recente do

funcionamento da rede e mantém o histórico sempre recente, facilitando a percepção de mudanças pequenas de comportamento, uma vez que o histórico alongado tornaria mais provável disfarçar mudanças sutis de comportamento.

O parâmetro de controle do filtro 1 é baseado no desvio padrão das janelas, como apresentado a seguir:

Alarme_Contagem = Media + (v1*Desvio_padrao)

onde v1=1; é o grau de rigidez do controle, valor default = 1.

Portanto, resumidamente, o algoritmo tem a função de identificar qualquer aumento do fluxo de pacotes através da contagem do número de pacotes enviados em determinado tempo. A determinação se houve ou não um aumento no fluxo de pacotes se dá através da divisão do tráfego em janelas de tamanhos pré-definidos e da comparação direta dessas janelas de pacotes com o histórico das dez últimas janelas de pacotes. Todas as janelas de pacotes suspeitas são enviadas para o próximo filtro, as janelas que apresentarem normalidade comparada ao histórico das dez janelas anteriores, serão desconsideradas.

Através da figura 3.5, é apresentado um resumo da funcionalidade do filtro. O *trace* coletado da rede é analisado de acordo com as informações extraídas do *trace*: TEMPO de chegada; IP DE ORIGEM; IP DE DESTINO; PROTOCOLO; e TAMANHO do pacote. A contagem de pacotes do *trace* determina o tamanho da janela a ser utilizada e divide os *traces* nessas janelas, após, essas janelas são analisadas uma a uma e então, é tomada a decisão conforme a indicação de aumento de tráfego, a seguir:

É importante salientar nesse ponto que, em todos os filtros criados, o fator de decisão é determinado por um parâmetro de controle de rigidez que, combinado com fator de comparação, vai ou não alertar cada filtro.

3.4.2 FILTRO 2 - FREQUÊNCIA DA OCORRÊNCIA DE IP DE DESTINO

Uma segunda característica, proveniente dos ataques DDoS, é o fato de possuírem destinos alvos, ou seja, o aumento do tráfego causado por um ataque DDoS é direcionado para destinos específicos. Através da análise dos IPs de destino dos cabeçalhos dos pacotes IP gerados na rede, é possível verificar se existe uma incidência de pacotes muito frequente que é direcionada a poucos destinos.

O segundo filtro analisa a ocorrência excessiva dos IPs de destino do fluxo de pacotes

FIG. 3.5: Filtro 1: Contagem de Pacotes

alarmados no filtro 1. A análise é realizada através da contagem dos IPs de destino contidos em uma janela, através do limite estabelecido, e define se cada destino existente tem a frequência excessiva ou não.

Um resumo da funcionalidade do filtro 2 é apresentado através da figura 3.6.

Inicialmente, as janelas alertadas pelo filtro 1 são analisadas para contabilizar o número total de IPs de destino destintos e após, calcula a média de ocorrência de cada IP, frequência de ocorrência de cada IP proporcional ao total. A análise é realizada através dessa média multiplicada por uma variável de controle, como apresentado a seguir (ex.: média = 0,05; variável de controle = 2, portanto, *threshold* = 0,10, ou 10% de ocorrência):

Probabilidade_IP_destino = (Quant_IP_destino(j) / Total_de_pacotes_Janela);

if probabilidade_IP_destino > v2*(1/Quant_IPs_destino_unicos)

onde v2 é o grau de rigidez do controle, valor default = 2.

Ao final do filtro 2 é criado também um outro vetor, o vetor de protocolos, nesse vetor são inseridos os nomes dos protocolos específicos que se deseja investigar. Como apresentados no capítulo 2, os ataques DDoS 7.7 e 3.4 lançam mão de três modalidades de ataques através dos protocolos HTTP, UDP e ICMP para realizar suas ofensivas. Nesse momento o filtro é definido para analisar exatamente esses três protocolos listados, porém qualquer outro tipo de combinação é possível. A seguir a figura 3.6:

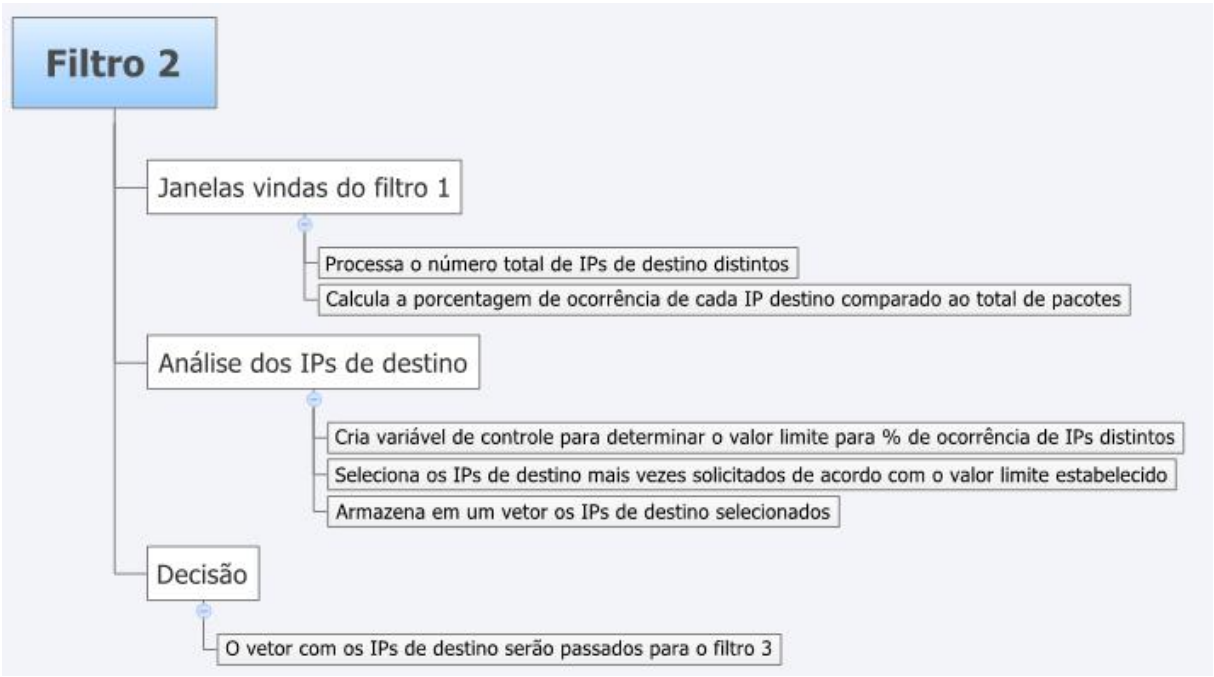

FIG. 3.6: Filtro 2: Ocorrência de IPs de destino

3.4.3 FILTRO 3 - PERFIL DOS PROTOCOLOS DOS IP DE ORIGEM

Outra característica percebida nos ataques DDoS é direcionada aos ataques DDoS compostos, que é a combinação de ofensivas diversas, camuflando os ataques por detrás de uma estratégia que é a de tornar o fluxo malicioso de pacotes similar ao fluxo normal. Como listados anteriormente, os protocolos HTTP, UDP e ICMP são comumente utilizados nos dias de hoje, nas diversas aplicações existentes.

O terceiro filtro objetiva realizar a análise do perfil de protocolos de cada IP de origem da rede que está sendo analisada. Para isso as informações selecionadas nos filtros

anteriores são processadas antes de entrarem no filtro 3.

O processamento consiste em criar arquivos para cada endereço IP de origem proveniente da janela alertada pelo filtro 1 e que se comunicam com o(s) endereço(s) IPs de destino alertados pelo filtro 2 através dos protocolos HTTP, UDP e ICMP. Resumidamente, o filtro final irá analisar os pacotes originados na rede interna que possuam os mesmos destinos predominantes e que utilizam os mesmos protocolos.

Então, a partir de cada arquivo gerado pelo processamento do filtro, a análise será focada em encontrar um perfil de utilização de protocolos, referente à proporção de pacotes que cada protocolo específico analisado possui em relação ao total de pacotes analisados de cada um desses endereços IP de origem.

A partir da análise de cada perfil de utilização de protocolos individual é determinado qual é o perfil mais recorrente, um perfil padrão.

O perfil padrão corresponde ao perfil individual mais recorrente, no entanto, o filtro não procura por um perfil de utilização de protocolos exato, pois os tráfegos legítimos podem influenciar na composição desses perfis individuais, mas sim por um perfil de utilização aproximado, determinado pela variável de controle do filtro 3, ajustado para encontrar valores de utilização entre +10% e -10% da proporção mais recorrente de cada protocolo. As fórmulas a seguir representam como é determinado o perfil mais recorrente, e como os perfis existentes são rotulados por possuírem um perfil padrão, respectivamente:

VPAP(k) - Vetor de Proporção arredondada do protocolo (k) =(ROUND()PAC)

onde PAC = pacotes desse protocolo na janela / pacotes totais na janela.

if VPAPa(k) > (modeVPAP - v3) and VPAP (k) > (modeVPAP - v3)
if VPAPb(k) > (modeVPAP - v3) and VPAP(k) > (modeVPAP - v3)
if VPAPc(k) > (modeVPAP - v3) and VPAP(k) > (modeVPAP - v3)
then IP_de_Origem possui perfil padrão.

onde v3 é grau de rigidez do filtro 3, valor default = 1.

Os IPs de origem relacionados ao final de toda filtragem sequencial são alarmados como resultado final, conforme figura 3.7 a seguir:

É importante apontar para o fato de que, a partir do filtro 3, não será possível encontrar uma única máquina *zoombie*, ou uma minoria de máquinas infectadas com comportamento

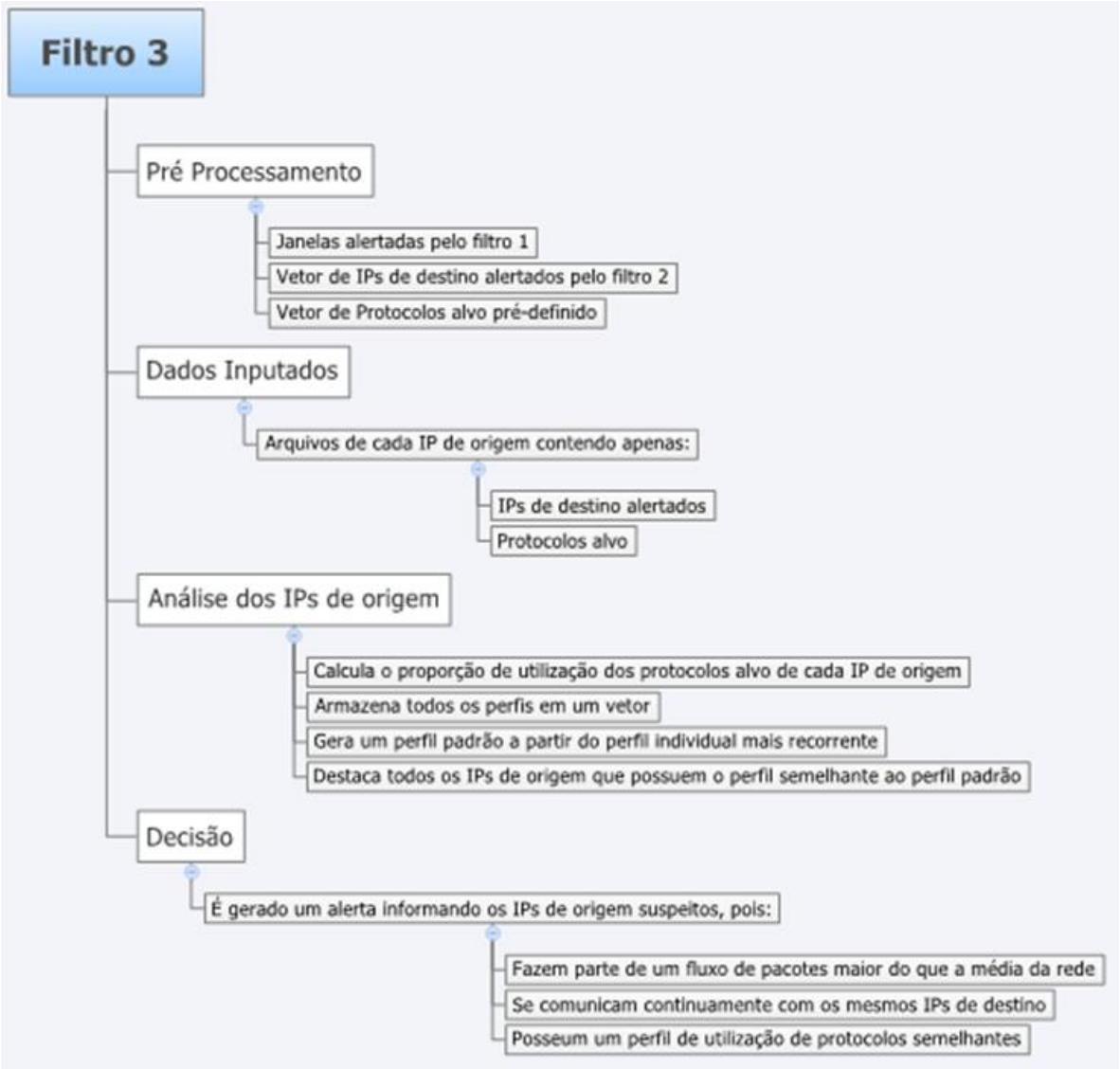

FIG. 3.7: Filtro 3: Perfil dos Protocolos dos IPs de origem

suspeito, uma vez que o método se destina a encontrar grupos de usuários com um perfil de utilização de protocolos mais frequentes da rede local.

4 RESULTADOS

Uma das maiores dificuldades para a abordagem do problema é a escassez de *traces* confiáveis para testes e que possuam as características necessárias de um ataque DDoS combinado.

Em (LI, 2008) discute-se que, apesar das avaliações em ambientes simulados serem "artificiais" quando comparadas ao ambiente imprevisível da Internet, um ambiente de simulação ainda oferece vantagens em relação a avaliação em ambientes reais, devido a questões de custo e infraestrutura. Nesse sentido, pode ser observado que, em muitos trabalhos, diferentes tipos e estilos de abordagem foram implementados em ambientes simulados, como em (CHEN, 2009), (MURASE, 2008), (NICOL, 2004) e (CHAN, 2006).

No intuito de se realizar uma análise detalhada, foram criadas situações de simulação de diversos comportamentos de uma rede. Essas situações são encontradas dentro dos ambientes simulados e foram, inicialmente, retiradas de traces existentes no projeto DARPA, projeto apresentado na próxima seção.

As situações foram separadas em 4:

- tráfego normal;
- ataque DDoS simples;
- outros tipos de ataques;
- ataques DDoS compostos.

4.1 DARPA - 1999

Uma boa fonte de consulta para *traces* de ataques e análise de métodos de detecção de ataques disponíveis é proveniente de um estudo realizado nos anos de 1998 e 1999 pelo grupo de tecnologia e sistemas cibernéticos do laboratório Lincon do Instituto de Tecnologia de Massachusetts (MIT) (LIPPMANN, 1999) e (MASSACHUSSETS, 1999), onde foi criando um grande ambiente de testes e simulação junto com a Agência de

Projetos de Pesquisa Avançada em Defesa (DARPA) baseado na rede de computadores do Laboratório de Pesquisa da Força Área (Eyrie AFB).

Apesar dessa base de dados, hoje, ser considerada ultrapassada considerando o perfil de utilização de aplicativos dos usários da Internet, ela permite realizar alguns testes atuais, conforme descrito pelas situações listadas acima.

Esse primeiro conjunto de testes, baseados em diversas situações, permitiu o aperfeiçoamento do primeiro e segundo filtros, considerando que o terceiro filtro é específico para encontrar as características de ataques DDoS compostos, ainda não disponíveis na época dos testes em 1999.

4.1.1 ANÁLISE DE SENSIBILIDADE DOS FILTROS

A partir dos *traces* disponibilizados do projeto DARPA foi possível realizar uma análise de sensibilidade de cada filtro do algoritmo, assim como a análise dos parâmetro envolvidos no algoritmo. Optou-se por utilizar os *traces* do DARPA devido a variedade de situações criadas no experimento, pela documentação organizada e clara e, principalmente, por ser uma fonte de dados amplamente conhecida e testada.

4.1.1.1 FILTRO 1 - TAMANHO DA JANELA

O tamanho da janela é baseado no tamanho total do *trace*. As janelas devem conter um conjunto de informções do tráfego suficientemente grande para identificar as características dos ataques DDoS que possivelmente existam na rede, mas também devem ser criadas em uma quantidade suficiente a ponto de representarem um histórico da rede, e assim poderem ser referências de análise das próximas janelas.

Como é impossível prever um tamanho padrão dos *traces* que serão analisados, o tamanho das janelas de cada *trace* é baseado no próprio tamanho desse *trace*, explicitado pela equação 3.1 (1).

O ponto de equilíbrio para a escolha do multiplicador que determinará o tamanho final da janela foi estabelecido através da análise de dois *traces*, o primeiro, foi o de maior quantidade de pacotes utilizados nesse projeto, com 462201 pacotes, e o segundo o de menor quantidade de pacotes, com 9113 pacotes.

4.1.1.2 FILTRO 1 - PARÂMETRO DE CONTROLE

O filtro 1 tem o objetivo identificar variações na quantidade de tráfego que extrapolam o histórico recente desse tráfego baseado na média de pacotes das dez últimas janelas e o seu desvio padrão, como apresentado na equação 3.2 (2). O parâmetro de controle pode ser modificado para ser mais ou menos tolerante às variações do tráfego.

O valor zero para esse parâmetro de controle significa que qualquer variação do tráfego de uma janela que esteja acima da média analisada representará um alerma, o valor de um, significa que apenas as janelas que contiverem uma quantidade de tráfego maior que a média somada ao desvio padrão das últimas 10 janelas serão alertadas.

4.1.1.3 FILTRO 2 - PARÂMETRO DE CONTROLE

O filtro 2 tem o objetivo de identificar os endereços IPs de destino que são mais frequentemente requisitados e, portanto, podem representar possíveis alvos de ataques DDoS. O critério de seleção para determinar se um endereço de destino esta sendo muito utilizado é determinado pela utilização dos outros endereços de destino, o algoritmo contabiliza a quantidade total cada endereço de destino, e calcula a respectiva proporção de ocorrência relativa a todos o pacotes.

O parâmetro de controle do filtro 2 irá determinar até quantas vezes um determinado destino pode ser requisitado propocionalmente a todos os outros destinos, conforme apresentado na equação 3.3 (3). O valor padrão desse parâmetro foi determinado através de testes, e é dois, o que quer dizer que um endereço de destino para ser alertado precisa ter um número de ocorrências maior que duas vezes a ocorrência proporcional de todos os outros destinos.

4.1.1.4 FILTRO 3 - PARÂMETRO DE CONTROLE

O último filtro tem a finalidade de averiguar se os perfis de utilização de protocolos dos endereços de origem que se comunicam com endereços de destino alertados pelo filtro 2 são semelhantes, tais quais em um ataque DDoS composto. Após a determinação do perfil padrão, equação 3.4 (4), cada um dos endereços de origem analisados terá seu perfil de utilização de protocolos comparado ao perfil padrão.

O parâmetro de controle do filtro 3, caso considerado como zero, indicaria que o perfil de uma origem necessitaria ser identica ao padrão, no entanto essa é uma situação

improvável, uma vez que apenas um pacote a mais ou menos de um determinado protocolo já seria suficiente para deixar os perfis não semelhantes. O valor padrão desse parâmetro foi testado e determinado em um, o que quer dizer uma variação para mais ou para menos de 10% comparado aos valores do perfil padrão, como apresentado na equação 3.5 (5).

4.1.2 RESULTADOS OBTIDOS

As situações criadas comentadas anteriormente foram retiradas desse experimento realizado pelo laboratório Lincon da MIT e serão examinadas a seguir.

Situação de tráfego normal;
Foi utilizado o primeiro dia da primeira semana de treinamento de 1999, abrangendo 1.007.235 pacotes, durante o período de aproximadamente 10:00 horas até 16:23 horas, coletados na saída da rede criada no experimento.

A figura 4.1 é resultado do output do código referente ao primeiro filtro. Nela, é possível visualizar as variações das quantidades de pacotes por cada janela analisada, como cada janela possui uma quantidade fixa de pacotes a partir de um *trace*, a variação de tráfego é medido pelo tempo entre o primeiro e último pacotes de cada janela. As depressões apresentadas no gráfico representam íntervalos de tempo menores entre o primeiro e último pacote comparado aos picos do gráfico, que são intervalos maiores, essa variação de tempo é verificada no eixo vertical da figura. Utilizando o primeiro filtro, 14,92% do tráfego foi selecionado por apresentar contagem excessiva de pacotes.

Já o segundo filtro, analisou todas as 10 janelas selecionadas pelo filtro 1. Os alertas de suspeita de ocorrência excessiva de IPs de destino foram analisados a partir de dois fatores diferentes: a média de ocorrência e, a variável de rigidez do filtro, conforme explicado na seção 3.4.2.

Se o filtro 3 fosse utilizado conforme os moldes originais, no intuito de analisar somente os protocolos específicos, para esse *trace*, não resultaria nenhuma informação, pois esse *trace* não apresenta as características de ataques DDoS como os ataques 7.7 e 3.4. No entanto, para fins de teste, foi utilizado o seguinte vetor de protocolos: 'TCP' 'SMTP' 'TELNET', que foram os protocolos mais recorrentes analisados manualmente nesse *trace*.

Como resultado três dos cinco IPs de origem possuiam perfil semelhante. São os IPs ilustrados nas figuras 4.2, 4.3 e 4.4 marcado no eixo horizontal com os índices 1, 2 e 5. Ao final da execução o algoritmo gera o alarme apontando os suspeitos detectados:

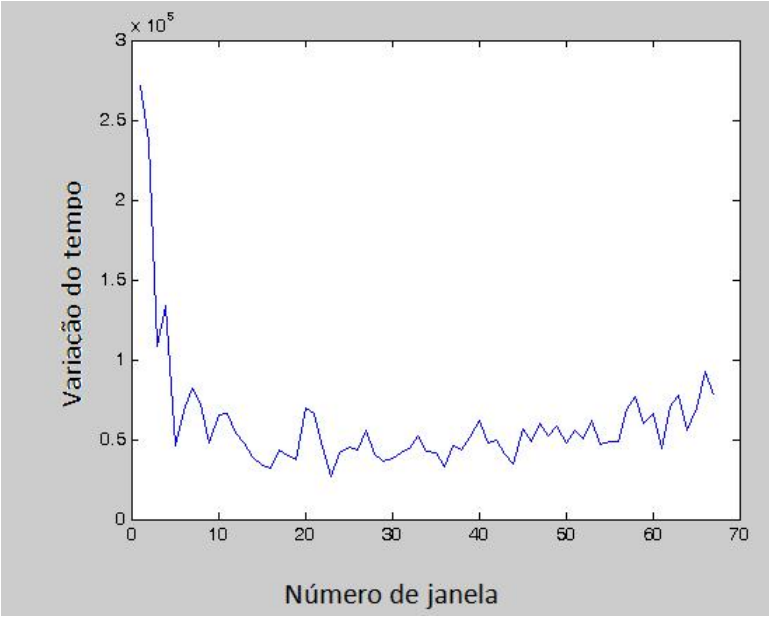

FIG. 4.1: Plotagem dos resultados do Filtro 1 na situação de tráfego normal.

Alarme!!!! 172.16.112.207 IP ORIGEM suspeito
Alarme!!!! 172.16.113.105 IP ORIGEM suspeito
Alarme!!!! 172.16.114.169 IP ORIGEM suspeito

Portanto, através dos filtros sequenciais, foi possível estabelecer a implementação da análise do *trace* buscando reconhecer características dos ataques DDoS compostos. Passo a passo os filtros descartam o tráfego que não é reconhecido como suspeito e ao final do algoritmo, é retornado uma lista de IPs de origem suspeitos, IPs de destino de prováveis alvos, o perfil de comportamento dos protocolos analisados e o momento em que estão ocorrendo os prováveis ataques.

Situação de Ataque DDoS simples

Foi utilizado o primeiro dia da quinta semana de treinamento de 1999, durante o período o qual ocorre um ataque DDoS do tipo *udpstorm*. O *trace* abrange aproximadamente 1 hora e meia de tráfego (de 20:00 horas até as 21:30) e o ataque dura 15 minutos (de 21:00 as 21:15).

O ataque começa aproximadamente na janela 6 do algoritmo, ilustrada pela figura 4.5. É possível observar que a duração do ataque é de 15 minutos dentro de um *trace* de um

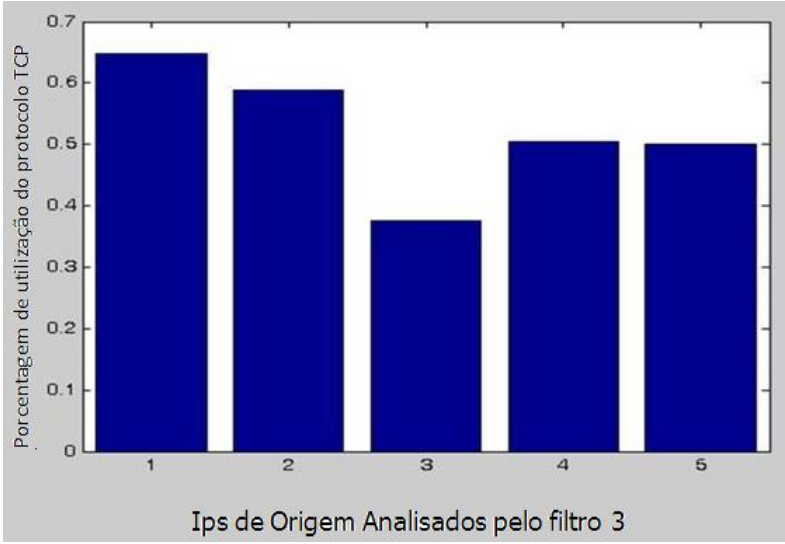

FIG. 4.2: Plotagem dos resultados do Filtro 3 na situação de tráfego normal relacionados ao protocolo TCP dos 5 IPs de origem (Y = 0.6471 — 0.5882 — 0.3750 — 0.5052 — 0.5000.)

total de uma hora e meia. A figura 4.5, representa toda a duração do ataque. Quando se inicia o ataque ,janela 6 aproximadamente, até seu fim, janela 58 aproximadamente, a quantidade de janelas crescem rapidamente, apesar de representarem apenas 15 minutos dos 90 minutos totais do *trace*. A quantidade de janelas durante o ataque é proporcionalmente muito maior do que a quantidade de janelas quando não há ataques, pois o gráfico é plotado em relação à tangente da variação do tempo para facilitar a visualização. Como muitas janelas, que possuiem uma quantidade fixa de pacotes, são geradas em um curto espaço de tempo, os 15 min de ataques representam a maior parte do pacotes do *trace* analisado.

No filtro 1, 32,20% do tráfego foi selecionado por apresentar contagem excessiva de pacotes. O ataque DDoS contido nesse trace pode ser detectado pelo algoritmo no filtro 1 através dessa análise de contagem excessiva de pacotes no momento em que o ataque ocorre. Após o término do último filtro, nenhum ataque DDoS composto foi alarmado, como deveria acontecer.

Situação com outros tipos de ataques

Foi utilizado o primeiro dia da quarta semana de treinamento de 1999, abrangendo um período de aproximadamente 8 horas e meia incluindo os diversos ataques listados em

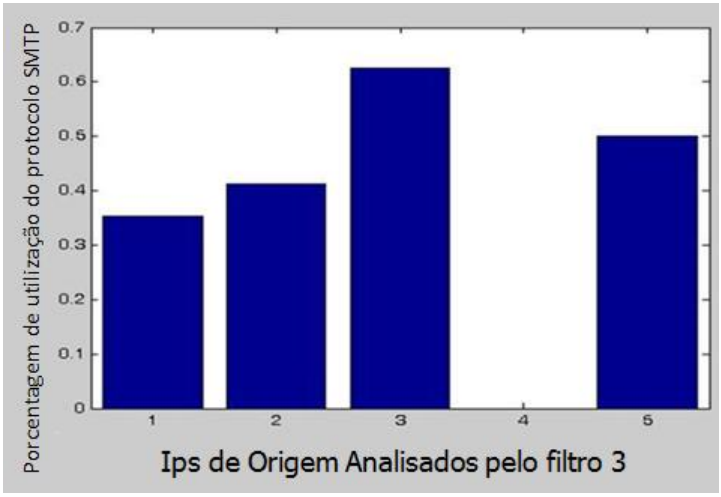

FIG. 4.3: Plotagem dos resultados do Filtro 3 na situação de tráfego normal relacionados ao protocolo SMTP dos 5 IPs de origem (Y = 0.3529 — 0.4118 — 0.6250 — 0.0 — 0.5000.)

(MIT) realizados nessa data. No entanto, o algoritmo não alarmou ataques DDoS, como era esperado, pois os *traces* dessa época não possuem as características de ataques DDoS compostos.

Situação DD - Ataques DDoS compostos

Infelizmente, à época desse experimento, 1999, não havia dados compatíveis com o perfil de ataques DDoS compostos.

Foi verificado que, através dos filtros sequenciais, foi possível estabelecer a implementação da análise do *trace* buscando reconhecer características comportamentais dos ataques DDoS combinados. Passo a passo os filtros descartam o tráfego que não é reconhecido como suspeito e, ao final do algoritmo, é retornado uma lista de IPs de origem suspeitos, IPs de destino de prováveis alvos, o perfil de comportamento dos protocolos analisados e o momento em que estão ocorrendo os prováveis ataques.

4.2 LABORATÓRIO DE REDES IME - 12 DE JANEIRO DE 2012

No intuito de superar a carência de *trace*s que contivessem as características de ataques DDoS compostos, foi necessário montar uma estrutura de simulação. Inicialmente, utilizou-se a estrutura do Laboratório de redes do IME, num total de 10 máquinas de usuários atacando uma máquina servidora. Os detalhes de como o ambiente foi executado são

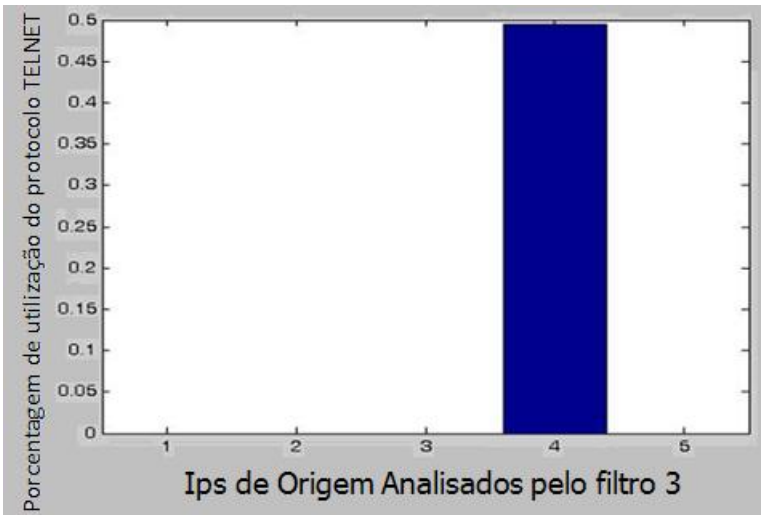

FIG. 4.4: Plotagem dos resultados do Filtro 3 na situação de tráfegfo normal relacionados ao protocolo TELNET dos 5 IPs de origem (Y = 0.0 — 0.0 — 0.0 — 0.4948 — 0.0.)

listados a seguir:

- Características das máquinas atacantes

  Sistema Operacional Ubuntu e Windows XP;

  Placa de rede de 100Mb;

  Utilização do *web browser* Mozilla Firefox, mecanismo para utilização de tráfego HTTP;

  Utilização da ferramenta PING, capaz de gerar tráfego ICMP.

- Características da máquina coletora (sniffer)

  Sistema Operacional Ubuntu;

  2 placas de rede de 100Mb;

  Foi usado o aplicativo wireshark para coleta de tráfego;

  Foi configurada a função de roteamento;

  Foi instalado um aplicativo com função limitadora de tráfego;

  Foi instalado um aplicativo com função de monitoração de tráfego.

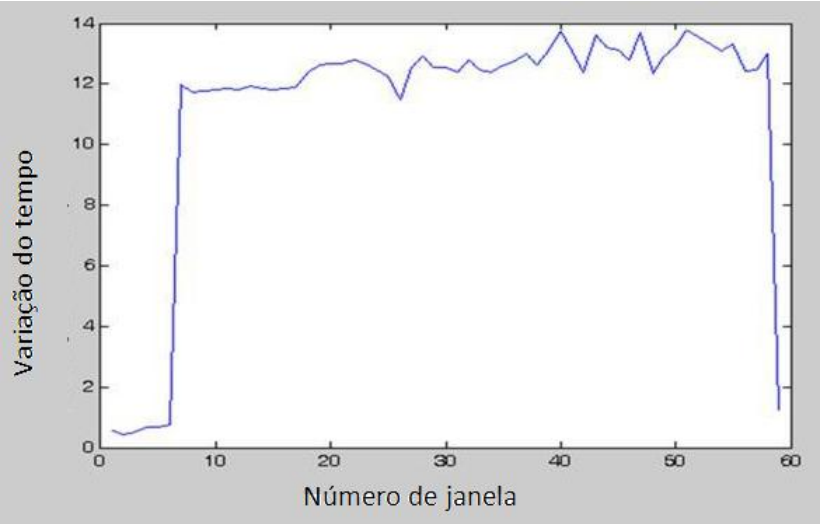

FIG. 4.5: Plotagem dos resultados do Filtro 1 na situação de ataque DDoS simples.

- Características da máquina alvo

  Sistema Operacional Ubuntu;

  Placa de rede de 100Mb;

  Foi instalado o aplicativo servidor web Apache.

A figura 4.6 ilustra o ambiente simulado, onde existe uma rede local com usuários, sendo que alguns desses usuários fazem parte de una *botnet* e estão representados por um pacote etiquetado (DETECTED). Os usuários estão conectados ao *switch* central da rede, que possui o último segmento para o roteador[10] localizado na saída da rede local. O alvo é um servidor de conteúdo e oferece um portal de conteúdo, no caso dessa simulação foi usado um portal cópia do portal www.comp.ime.eb.br, do IME, e também configurado para ser um servidor de vídeos para *download*. Os usuários também terão acesso real à Internet a partir da segunda simulação, em 28 de março de 2012.

Essa primeira etapa de simulação foi realizada em um ambiente controlado, sem acesso à Internet e sem que as máquinas atacantes tivessem tráfego de fundo. As redes foram implementadas de tal maneira que as máquinas atacantes ficassem em uma rede e a máquina alvo em outra, separadas pela máquina coletora, que atua como *gateway* das

[10]Também pode ser um *firewall* ou servidor que fazem a função de último equipamento que conecta essa rede local à Internet

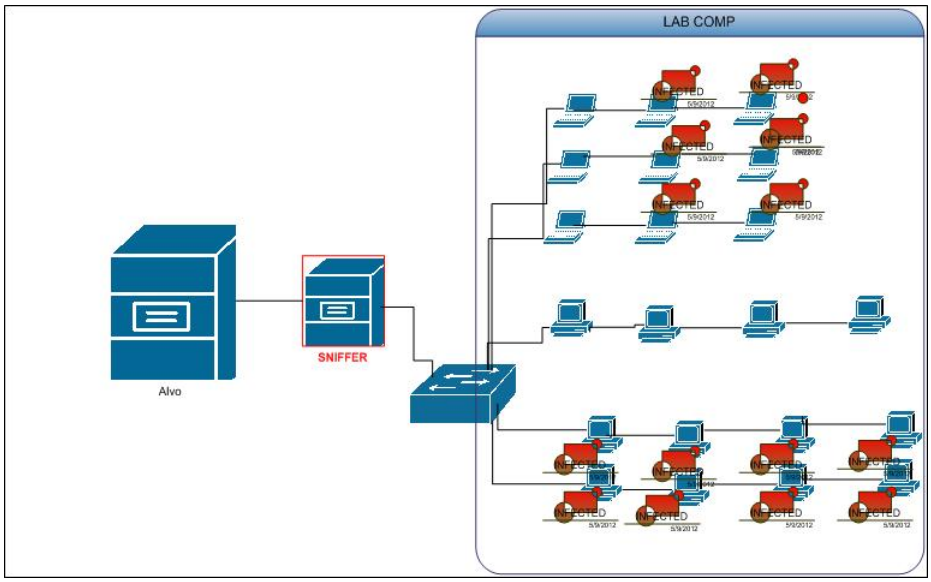

FIG. 4.6: Ambiente de simulação criado

duas redes.

O ataque consistiu na solicitação contínua pelas máquinas atacantes de um vídeo armazenado no servidor web da máquina alvo, no intuito de gerar tráfego HTTP. Também foram utilizados fluxos contínuos do protocolo ICMP através da ferramenta PING. A tabela 4.1 ilustra as etapas executadas nessa simulação:

Etapa	Duração (min)	Descrição do Tráfego	Usuários Infectados / Total
1	5	48 Solicitações HTTP legítimas	0/8
2	5	80 Solicitações HTTP legítimas	0/10
3	5	80 Solicitações HTTP legítimas	0/10
4	5	80 Solicitações HTTP legítimas / 6 ataques ICMP	6/10
5	5	80 Solicitações HTTP legítimas / 6 ataques ICMP	6/10
6	5	80 Solicitações HTTP legítimas	0/10
7	2	80 Solicitações HTTP legítimas	0/10
8	2	80 Solicitações HTTP legítimas	0/10
9	2	80 Solicitações HTTP legítimas	0/10
10	2	32 Solicitações HTTP legítimas	0/8

TAB. 4.1: Etapas da simulação realizada em 12 de janeiro de 2012.

4.2.1 RESULTADOS OBTIDOS

Seguindo a tabela de etapas da simulação, o algoritmo deverá ser capaz de detectar:

- aumento do volume do tráfego;
- os endereços IP de destino que sejam predominantes, em quantidade de pacotes, entre as comunicações das máquinas de origem da rede em direção à saída da rede.
- o perfil de utilização de protocolos predominante entre as máquinas de origem
- os endereços IP de origem que se enquadrem como tendo comunicações abertas com os endereços IP de destino identificados e com o perfil de protocolos semelhante ao perfil predominante na rede.

Como resultado da saída da etapa 5 dessa simulação, de acordo com a figura 4.7, eram esperados que 6 máquinas atacantes tivessem o perfil predominantemente formado por protocolos HTTP e ICMP atacando a máquina alvo, de endereço IP 192.168.77.68. A saída do algoritmo é apresentada a seguir:

Alarme!!!! 192.168.7.61 IP ORIGEM suspeito.
Alarme!!!! 192.168.7.62 IP ORIGEM suspeito.
Alarme!!!! 192.168.7.63 IP ORIGEM suspeito.
Alarme!!!! 192.168.7.64 IP ORIGEM suspeito.
Alarme!!!! 192.168.7.65 IP ORIGEM suspeito.
Alarme!!!! 192.168.7.67 IP ORIGEM suspeito.

Como demonstração do resultado da utilização do algoritmo sob os traces dessa simulação, foi selecionado um trecho de cerca de 10 minutos de comunicação, o qual era sabido que havia ataque. Eram esperados que seis máquinas atacantes tivessem o perfil predominantemente formado por protocolos HTTP e ICMP atacando a máquina alvo. E o algoritmo foi capaz de identificar perfeitamente as seis máquinas atacantes, o perfil desses ataques e o alvo, em diversos momentos do trace.

Importante salientar que o algoritmo detectou precisamente as 6 máquinas de origem atacantes, o endereço alvo e também o perfil de protocolos do ataque simulado.

4.3 LABORATÓRIO DE PROGRAMAÇÃO IME - 28 DE MARÇO DE 2012

Apesar de essa primeira simulação ter sido importante para testar o funcionamento do algoritmo com fluxos compostos de protocolos, ficou constatado que esse primeiro ambiente simulado apresentou diversas restrições, principalmente por não executar ataques

reais, mas sim acesso real web, além de não englobar todas os tipos de tráfego característicos de ataques DDoS compostos, HTTP, UDP e ICMP juntos.

O segundo ambiente utilizado, criado através de uma topologia semelhante ao ambiente inicial, conforme a figura 4.6, foi construído no dia 28 de março de 2012, na sala de programação do IME. Para esse caso, foram utilizadas 14 máquinas que representavam uma rede, onde a maioria foi configurada com aplicativo de ataque e outras não. Algumas características foram adicionadas a esse experimento em comparação à primeira simulação, conforme listadas a seguir:

- Características das máquinas atacantes:

  Sistema Operacional Ubuntu e Windows XP;

  Placa de rede de 100Mb;

  Utilização do web browser Mozilla Firefox.

  Utilização da ferramenta de ataque LOIC, capaz de gerar ataques HTTP.

  Utilização da ferramenta de ataque LOIC, capaz de gerar ataques UDP.

  Utilização da ferramenta PING, capaz de gerar tráfego ICMP.

- Características da máquina coletora (sniffer):

  Sistema Operacional Ubuntu;

  2 placas de rede de 100Mb;

  Foi usado o aplicativo wireshark para coleta de tráfego;

  Foi configurada a função de roteamento;

  Foi instalado um aplicativo com função limitadora de tráfego.

  Foi instalado um aplicativo com função de monitoração de tráfego.

- Características da máquina alvo:

  Sistema Operacional Ubuntu;

  Placa de rede de 100Mb;

  Foi instalado o aplicativo servidor web LAMP (Linux+Apache+ MySQL+PHP);

  Foi criada uma replica de *site* através da ferramenta wget

As etapas de simulação foram realizadas em um ambiente controlado, porém, dessa vez, com a possibilidade de acesso à Internet por parte algumas máquinas da rede. Também foram usadas máquinas não infectadas no ambiente, com o único intuito de gerar tráfego de fundo, considerado inofensivo. As redes foram implementadas de tal maneira que as máquinas da rede atacante ficassem em uma rede e a máquina alvo em outra, separadas pela máquina coletora, que atua como *gateway* das duas redes.

O ataque consistiu na utilização massiva da ferramenta de ataque LOIC pelas máquinas atacantes direcionadas ao servidor LAMP da máquina alvo, criando ataques HTTP e UDP contínuos. Também foram utilizados fluxos contínuos do protocolo ICMP através da ferramenta PING. A tabela 4.2 a seguir ilustra as etapas de coleta de *trace* realizadas durante essa simulação:

Etapa	Duração (min)	Descrição do Tráfego	Usuários Infectados / Total
1	5	Tráfego não malicioso	0/14
2	6	Ataques HTTP, ICMP e UDP	4/14
3	4	Ataques HTTP, ICMP e UDP	6/14
4	6	Ataques HTTP, ICMP e UDP	8/14
5	4	Ataques HTTP, ICMP e UDP	11/14
6	10	Ataques HTTP, ICMP e UDP	11/14
7	5	Ataques HTTP, ICMP e UDP	11/14
8	5	Ataques HTTP e UDP	11/14
9	4	Ataques HTTP e UDP	11/14
10	4	Ataques HTTP, ICMP e UDP	11/14

TAB. 4.2: Etapas da simulação realizada em 12 de janeiro de 2012.

4.3.1 RESULTADOS OBTIDOS

Como demonstração da utilização desse algoritmo sob essa simulação, foi selecionado um trecho do trace mapeado com o ataque. O algoritmo detectou precisamente as 4 máquinas de origem atacantes, o endereço alvo e também o perfil de protocolos do ataque simulado da etapa 2 conforme a tabela 4.2.

Para a etapa 3 da mesma tabela os resultados foram semelhantes, porém, dessa vez, detectando os 6 endereços de origem atacantes, como apresentado a seguir:

Alarme!!!! 192.168.91.123 IP ORIGEM suspeito.

Alarme!!!! 192.168.91.144 IP ORIGEM suspeito.

Alarme!!!! 192.168.91.21 IP ORIGEM suspeito.

Alarme!!!! 192.168.91.38 IP ORIGEM suspeito.

Alarme!!!! 192.168.91.63 IP ORIGEM suspeito.

Alarme!!!! 192.168.91.68 IP ORIGEM suspeito.

4.4 LABORATÓRIO DE PROGRAMAÇÃO DO IME - SIMULAÇÃO DE 19 DE JUNHO DE 2012

Para dar continuidade ao processo de análise do algoritmo, inclusive com intuito de aperfeiçoar a exatidão dos filtros, no dia 19 de junho de 2012, uma terceira simulação de ataque foi executada. No intuito de verificar a assertividade do método mesmo sob ambientes de difícil análise, a terceira bateria de simulação de ataques DDoS compostos se valia de ambiente e composição semelhantes à ultima simulação, figura 4.6.

As principais contribuições dessa simulação estão em contar com um tráfego de fundo muito maior por parte de todos os hosts, inclusive os infectados; realizar uma variação de acessos a sites não alvos (tráfego normal) mais aproximados ao perfil de utilização real e; diminuir a quantidade de ataques provenientes das máquinas infectadas, de tal maneira que o tráfego malicioso estivesse mais bem disfarçado entre o tráfego total da rede.

Foram usadas 12 computadores na rede interna, neles foram configurados um script para gerar tráfego, através do aplicativo crontab. Todas os usuários executavam acessos à Internet simulando ser um usuário padrão. No decorrer da simulação os ataques foram ativados em até 7 usuários da rede estabelecida. Uma parte da simulação contou com apenas 4 dos 12 usuários gerando ataques, no intuito de diminuir ainda mais a concentração do ataque.

No total foram gerados seis coletas de tráfego, três antes do ataque, sendo compostos apenas por tráfego não malicioso. São os *trace*s F1, F2 e F3 da tabela 4.1. O momento de transição do tráfego normal para tráfego malicioso esta contido no *trace* T1, onde os sete usuários vão sendo inseridos um a um no cenário. Os *traces* A1 e A2 representam a coleta durante os ataques, sendo que A1 contém seis usuários atacando e A2 apenas quatro. A tabela 4.3 apresenta as características dos *traces* coletados:

Os resultados do cenário criado ratificam toda a sequência de tráfego estabelecida. A tabela 4.4 apresenta detalhes do processamento dos *traces* analisados, indicando quantas vezes os filtros foram acionados e quantas vezes os alarmes foram gerados.

Mais uma vez o algoritmo foi preciso em identificar o alvo, as origens e perfil dos

TRACE	TEMPO (min)	DESCRIÇÃO	Usuários (infectados/total)
F1	4	Trágego normal	0/12
F2	1	Trágego normal	0/12
F3	4	Trágego normal	0/12
T1	5	Transição do tráfego para ataque	7/12
A1	1	ataque DDoS composto	6/12
A2	1	ataque DDoS composto	4/12

TAB. 4.3: *Traces* coletados em 19 de junho de 2012

TRACE	Quant. de Pacotes	N. de Janelas	N. de Utilizações do Filtro1/ Filtro2/ Filtro3	Quant. de vezes que o alerta foi usado	Usuários Infectados encontrados
F1	57002	24	1/1/0	0	0
F2	9113	4	0/0/0	0	0
F3	54287	23	4/4/0	0	0
T1	141184	55	1/1/1	1	7
A1	54415	23	2/2/2	2	6
A2	124814	50	8/8/8	8	4

TAB. 4.4: Resultado da análise do *traces* de 19 de junho de 2012

protocolos do ataque. Todos os usuários infectados durante as várias fases do ataque foram corretamente identificados.

5 CONSIDERAÇÕES FINAIS

Através do método estabelecido para detecção de ataques DDoS compostos foi possível desenvolver o algoritmo de detecção de ataques DDoS compostos apresentado nesse trabalho. A partir da simulação de ambientes com as características do ataque foi possível submeter o algoritmo a diversos tipos de análise, desde a análise em ambientes com tráfego normal, ataques DoS até ataques DDoS compostos camuflados ao meio de uma rede com alto índice de fluxo de dados considerados normais.

Em todos os testes o algoritmo conseguiu identificar o alvo, os endereços IP de origem envolvidos no ataque e o perfil de utilização dos protocolos utilizados nos ataques. Ainda que não tenha sido implementado em um ambiente de análise de tempo real, as características de baixo processamento, armazenamento de dados e pouca complexidade do algoritmo fez com que os resultados de análise de milhares de pacotes se dessem na ordem de poucos segundos.

O principal beneficiado desse modelo de mecanismo não é a vítima, mas sim os administradores de redes que poderiam identificar que a utilização da largura de banda de sua rede está sendo consumida por ataques. Uma vez que a opção pelo gerenciamento próativo de ameaças à rede for amplamente utilizado, a tendência é que os alvos e sistemas intermediários também venham a se beneficiar mais.

Com o maior controle dos pacotes na saída da rede, uma realidade já estabelecida entre as corporações nos dias de hoje, essa aboradagem torna-se uma opção de segurança viável. Uma vez que, pelas características de descentralização do controle dos dados na Internet, ainda não é possível ,na prática, implementar uma solução integrada através dos milhares de sistemas autônomos que compõe a Internet e, também, porque a detecção de ataques junto ao seu destino ainda não permite a localização em larga escala da origem de todos os IPs que compõe uma *botnet*, de acordo com os métodos existentes analisados até a presente data.

Por fim, o método proposto neste trabalho possui algumas vantagens quando comparado aos trabalhos anteriores, vantagens estas que caracterizam as contribuições da proposta. Foram realizadas simulações para avaliar a implementação e análise do algoritmo a partir de traces públicos, como o do projeto DARPA e traces criados especificamente com as

características exatas do comportamento descrito nos ataque 7.7 e 3.4, ataques DDoS compostos, e em todos os testes, o algoritmo identificou os ataques procurados. A ausência de uma análise de falsos positivos ou falsos negativos do método apresentado não representa uma omissão, mas sim, uma adaptação ao problema em questão, uma vez que ataques DDoS compostos são realizados durante horas e dias, nesse caso, o objetivo do método é a detecção ou não do ataque, não importando quantas vezes essa detecção é feita. O método é bem sucedido em caso de detecção e mal sucedido caso não detecte. O método é bem sucedido caso não detecte erradamente um ataque e mal sucedido caso detecte ataques onde não haja ataques, no trabalho em questões, e em todas as etapas de análise, o método sempre foi bem sucedido.

5.1 TRABALHOS FUTUROS

A principal contribuição futura para esse projeto será implementar o algoritmo para análise em tempo real, o que traria um enorme benefício para administradores de redes que, hoje em dia, dificilmente conseguiriam identificar que parte de sua banda esta sendo consumida por ataques DDoS. Ainda, pela abrangência das simulações realizadas, seria de extrema relevância a utilização do algoritmo sobre *traces* de ambientes de redes em produção submetidos a ataques DDoS combinados e, também, a utilização do método em redes de tamanhos mais abrangentes, comuns às grandes coporações.

6 REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. **NORMA BRASILEIRA ABNT NBR ISO/IEC 27001.** 2006.

AHNLAB, I. **Analytical Report on 3.4 DDoS Attacks**. Em *Ahnlab Institute, Seoul, 150-869, Korea.*, 2011.

ARBOR. **If you weren't paying attention last week, the Internet has gone to war.**, 2010. URL `http://asert.arbornetworks.com/2010/12/the-Internet-goes-to-war/`. `Portal oficial ARBOR Networks.` acessado em 18/01/2011.

ARI, E. A. **Managing flash crowds on the Internet.** *Modeling Analysis and Simulation of Computer Telecommunications Systems.*, 2003.

BRINKLEY, D. L.; SCHELL, R. R. **Concepts and terminology for computer security.** Em *In: ABRAMS, M. D.; JAJODIA, S.; PODELL, H. J. (Ed.). Information security: an integrated collection of essays. Los Alamitos, CA: IEEE Computer Society Press, p. 40-97.*, 1995.

CASTELUCIO, A., S. R. Z. A. **Evaluating the Partial Deployment of an AS-level IP Traceback System**. Em *UC'08 March 16-20,2008, Fortaleza, Ceará, Brazil*, 2008.

CHAN, E. A. **Intrusion Detection Routers: Design, Implementation and Evaluation Using an Experimental Testbed**. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, 24, 2006.

CHEN, L., L. J. **A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks**. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, 4, 2009.

DCT, 2010. URL `http://www.dct.eb.mil.br/`. `Portal oficial do Departamento de Ciência e Tecnologia do Exército Brasileiro`. acessado em: 27/11/2010.

DUTRA, A. **Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto.** 2007. Instituto Tecnológico da Aeronáutica - Praça Marechal Eduardo Gomes, 50 - Vila das Acácias. CEP 12228-900 - São José dos Campos - SP.

FEINSTEIN, L., S. D. B. R. K. D. **Statical Approaches to DDoS Attack Detection and Response.** . Em *Proceedings of the DARPA Information Survivability Conference and Exposition*, 2003.

FERGUSON, P. e SENIE, D. **Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC 2827**. Em *Internet Engineering Task Force (IETF). Website: www.ietf.org.*, 2000.

FRANÇOIS, J., A. I. B. R. **FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks.** Em *Natural Science and Engineering Council of Canada under its discovery program and the World Class University program through the Korea Science and Engineering Foundation funded by the Ministry of Education, Science, and Technology under Project R31-2008-000-10100-0. IEEE/ACM TRANSACTIONS ON NETWORKING*, 2012.

G1, 2011. URL `http://g1.globo.com/tecnologia/noticia/2010/12/. Portal de notícias da Rede Globo de Televisão.` acessado em 10/01/2011.

GORODETSKI, V. e KOTENKO, I. **Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool**. *Lecture Notes in Computer Science*, 2516, 2002.

ICANN. **Factsheet - Root server attack on 6 February 2007**, Março 2007. Internet Corporation for Assigned Names and Numbers.

INFO. **Ataques a computadores podem criar catástrofes**, 2011. URL `http://info.abril.com.br/noticias/seguranca/ataques-a-computadores-podem-criar-catastrofes-17012011-16.shl. Portal de notícias da revista INFO, editora Abril.` acessado em 18/01/2011.

ISO. **The ISO 27001 Information Security Management System Specification.** Em *Website do portal W3J, destinado a Governança de TI: http://www.w3j.com/5/s3.koman.html,*, 2006. acesso em 20/08/2011.

JING, Y., X. Z. W. X. Z. G. **O2-DN: An Overlay-based Distributed Rate Limit Framework to Defeat DDoS Attacks**. Em *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006; 23-29, pp. 79*, 2006.

JUN, J., O. J. K. S. **DDoS flooding attack detection through a step-by-step investigation**. Em *Kyungpook National University Daegu, South Korea.*, 2011.

KOTENKO, I. **Active Vulnerability Assessment of Computer Networks by Simulation of Complex Remote Attacks**. Em *Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing*, 2003.

KUHL, E. A. **Cyber Attack Modeling And Simulation For Network Security Analysis**. *Proceedings of the 2007 Winter Simulation Conference*, 2007.

KUZMANOVIC, A., K. E. W. **Low-Rate TCP-Targeted Denial of Service Attacks.** Em *SIGCOMM 03, August 25 to 29,2003, Karlsruhe, Germany.*, 2003.

LEE, H. S. **Counteracting DDoS Attack in KR**. Em *Korea Internet and Security Agency*, 2010.

LI, X., Z. K. Y. Y. **A Simulation Platform of DDoS Attack Based on Network Processor**. Em *International Conference on Computational Intelligence and Security*, 2008.

LIPPMANN, E. A. **The 1999 DARPA Off-Line Intrusion Detection Evaluation**. *Lincoln Laboratory MIT, 244 Wood Street, Lexington, MA 02173-9108.*, 1999.

MARKOFF, J. **Before the Gunfire, Cyberattacks**, Agosto 2008. The New York Times, acessado em: 26 de novembro de 2010.

MASSACHUSSETS, 1999. URL `Website do Laboratório Lincon da MIT que descreve o quarto dia de treinamento de 1999 e os ataques contidos: http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/1999/testing/week4/index.html e http://www.ll.mit.edu/mission/communications/ist/files/master-listfile-condensed.txt, respectivamente.` Última vez acessado em 29/12/2011.

MAYUR, E. A. **Flashback: A Peer-to-PeerWeb Server for Flash Crowds**. *Distributed Computing Systems*, 2007.

MIRKOVIC, J. **D-WARD: "Source-End Defense Against Distributed Denial-of-Service Attacks.** Em *PhD Dissertation, University of California, Los Angeles.*, 2003a.

MIRKOVIC, J., M. J. e P., R. **A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms**. 2002.

MIRKOVIC, J., P. G. P. e REIHER, P. **Source-End DDoS Defense.** Em *Second IEEE International Symposium on Network Computing and Applications (NCA'03). 2003: IEEE Computer Society.*, 2003b.

MUKHOPADHYAY, E. A. **A Study on Recent Approaches in Handling DDoS Attacks**. 2007.

MURASE, T. **Performance Evaluation of a Multi-Stage Network Event Detection Scheme against DDoS Attacks**. 2008.

NICOL, D. M., S. W. H. T. K. S. **Model-Based Evaluation: From Dependability to Security**. *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, 1, 2004.

OSHIMA, S., N. T. S. T. **The Evaluation of an Anomaly Detection System based on Chi-square Method** . Em *2012 26th International Conference on Advanced Information Networking and Applications Workshops.*, 2012.

PAGET, F. **DDoS Response**. Em *MACFEE, acessado em 19 de agosto de 2011.*, 2009. acessado em 19 de agosto de 2011.

PENG, T., L. C. R. K. **Protection from distributed denial of service attacks using history-based IP filtering**. Em *IEEE International Conference on Communications, 11-15 May 2003; pp.482 - 486.*, 2003.

PENG, T., L. C. R. K. **Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems.** Em *Department of Computer Science and Software Engineering, The University of Melbourne, Australia. ACM Computing Surveys, Vol. 39, No. 1, Article 3*, 2007.

RACHEV, S. ***Probability metrics and the stability of stochastic models.*** 1991.

SECUZILLA. **Source-Side Defenses Against DDoS Atacks**. 2006.

SHACHTMAN, N. **Activists Launch Hack Attacks on Tehran Regime**, Junho 2009. WIRED, acessado em: 26 de novembro de 2010.

TRAYNOR, I. **Russia accused of unleashing cyberwar to disable Estonia.**, 2007. URL `Guardian Unlimited. Bruxelas, 17 maio 2007, http://www.guardian.co.uk/russia/article/`. acessado em: 25/11/2010.

TWITTER. **Ongoing denial-of-service attack**, 2010. Twitter Status Blog acessado em: 26 de novembro de 2010.

UNISOG. **January 2001 thread on the UNISOG mailing list**, 2010. UNIversity Security Operations Group. Acessado em: 26 de novembro de 2010.

WANG, W., W. W. **Online Detection of Network Traffic Anomalies Using Degree Distributions.** Em *Department of Computer Science, Wuhan University of Science and Technology, Wuhan, China.*, 2010.

WANG, Z. e WANG, X. **DDoS Attack Detection Algorithm Based on the Correlation of IP Address Analysis** . Em *Department of Computing, YanShan University Qin Huang Dao China*, 2011.

WORTHAM, J.; KRAMER, A. E. **Professor Main Target of Assault on Twitter**, Agosto 2009. New York Times, acessado em: 26 de novembro de 2010.

XUAN, D., B. R. e W., Z. **A Gateway-based Defense System for Distributed DoS Attacks in High-Speed Networks**. Em *2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY; pp. 212-219.*, 2001.

YAAR, A., P. A. S. D. **SIFF: A stateless Internet flow filter to mitigate DDoS flooding attacks, Security and Privacy**. Em *Proceedings. 2004 IEEE Symposium on 9-12 May 2004; pp.130-143.*, 2004.

ZHOU, W. **Keynote III: Detection and traceback of DDoS attacks.** *Computer and Information Technology*, 2008.

7 APÊNDICE

Filtro 1

```
function [Alarme] = contagem ()

%1. ler txt que  contem uma coluna de informação, nos
seguintes moldes:
    %tempo_do_pacote_1
    %tempo_do_pacote_2
    % sucessetivamente, o tempo de cada pacote por cada
    linha, sem a  necessidade de preocupação com o tempo
    de inicio do primeiro pacote.
%2. Realizar a contagem das linhas, contabilizando, assim,
 o número de IPs.
%3. Receber o tamanho da Janela de análise. Inicialmente
através  de um input, posteriormente através de parametro.
%4. Separar o \textit{trace} analisado em blocos de informações do
tamanho da janela determinada na etapa (3).
%5. Realizar cálculos diretamente de cada bloco.
  %Utilzando o a primeira e última céluca de cada bloco,
  calcular o arco da tangente formado por: x=tempo do
  pacote; y=contagem do pacote.
    %Esse resultado terá 2 funções:
%5a. Servir de banco de dados para o calculo da média e do
desvio padrão dos arcos tangente do \textit{trace} analisado,
formando assim, uma variável_índice de comparação;
%6. Será comparado diretamente com a variável_índice de
comparação, para determinar, através desse índice, se existe
um comportamento anomalo de determinado conjunto de pacotes.
Sendo que esse passo é realizado primeiro do que o passo 5a.
%7. Acionamento ou não de alarme de contagem de pacotes.


fprintf('\n****\n\n Análise de detecção de Ataques DDoS
compostos: FILTRO ***1***: CONTAGEM DE PACOTES\n');
```

```
fid=fopen('darpa.txt','r');
%fid=fopen('5colunas completo.txt','r');

%1. leitura do arquivo que contem os tempos dos pacotes;
InputText = textscan(fid, '%10n %s %s %s %n');
%Criando o vetor com os tempos dos pacotes;



count=0;
fid=fopen('darpa.txt','r');
%fid=fopen('5colunas completo.txt','r');

while ~feof(fid)
    line = fgetl(fid);
    if isempty(line) | strncmp(line, '%', 1)
        continue

    end
    count=count+1;
end
number_of_line=count;
%2. Contagem dos pacotes

TamJanela = round(1000*log10(number_of_line));
%3. Tamanho da Janela de controle
indice_block=1;
Bloco =  InputText{1};
Alar = 0;
janela = 0;
v1=1;
%v1 é o grau de rigidez do controle, valor default = 1.
```

```
for block =1:TamJanela:(number_of_line - TamJanela)
    janela = janela+1;
    %marcador da janela analisada.
    block_ini=block;
    block= block + TamJanela-1;
    block_fim= block;
Delta(indice_block)=(Bloco(block_fim)-Bloco(block_ini))/10^6;
   %acertando a casa decimal do tempo(ex: 0001062 = 0,001062)
    %4. Cada Delta (indice) representa um bloco de dados;
 Tangente(indice_block)=atand(TamJanela/Delta(indice_block));
 %5. Cada Tangente (indice) representa a tangente do bloco de
  dados
  Media = mean(Tangente);
  %Media dos valores das tangentes ao longo do tempo
  Desvio_padrao = std (Tangente);
  %Desvio Padrão dos valores das tangentes ao longo do tempo

   Alarme_Contagem = Media + (v1*Desvio_padrao) ;
     %v1 é o grau de rigidez do controle, valor default = 1.
   if Tangente(indice_block)> (Alarme_Contagem)
     Alar = Alar+1; %Contagem de alarmes de contagem em todo
     o \textit{trace}. %Tangente(indice_block)
        Media + Desvio_padrao;
        fprintf('\n ---> ALARME DE CONTAGEM entre os pacotes:
        %d %d , equivalente a janela de pacotes: %d',
        block_ini,block_fim, janela);
        fprintf('\n Contagem de PACOTES no intervalo indicado
       acima da média das últimas 10 janelas anteriores.\n');
         Alarme = destino(janela,block_ini, block_fim);
    else
                 fprintf('\n NORMALIDADE \n');
           end
```

```
    indice_block=indice_block+1;
    if indice_block == 11  %buffer da media
        indice_block=1;
    end
%controle para que a media não seja calculada a partir do
historico de todos os valores, mas sim em relação aos ultimos
x valores.
end
number_of_block=indice_block-1;
Alarme_1 = Alar / janela;
fprintf('O filtro 1, apresentou aproveitamento de %3f em
referencia a todo o tráfego analisado\n', Alarme_1 );
%Resultado entrega a porcentagem do \textit{trace} que esta Alarmado

fclose(fid);

%\end{lstlisting}
```

Filtro 2

```
function  [Alarme] = destino (janela, ind1, indn)



fprintf('\n Análise de detecção de Ataques DDoS compostos:
 FILTRO ***2***:
 Ocorrência de IPs de Destino\n');

fid=fopen('darpa.txt','r');
%fid=fopen('5colunas completo.txt','r');

%1. leitura do arquivo que contem os tempos dos pacotes;
InputText3 = textscan(fid, '%n %s %s %s %n');
%Criando o vetor com os tempos dos pacotes;

Tam_Janela = indn - ind1 +1;
%quantidade de pacotes sendo analizado (intervalo de pacotes
selecionado)

Bloco3 = InputText3{3};
%a terceira coluna do arquivo é correspondente a coluna dos
IPs de destino

Intervalo3 = Bloco3 (ind1:indn);
%Array com os IPs de destino, apenas dentro do Intervalo
indicado

IPs_unicos3 = unique(Intervalo3);
%Array contendo todos os IPs de destinos (únicos) contidos
no Intervalo

Q_IPs_unicos3 = size(IPs_unicos3);
Q_IPs_unicos3 = Q_IPs_unicos3(1);
```

```
%valor do número de IPs unicos dentro do Intervalo


Tam_Vetor_IP_DEST = 0;
v2=2;
%v2 é o grau de rigidez do controle, valor default = 2.
for j=1:Q_IPs_unicos3
    IP = find(ismember(Intervalo3, IPs_unicos3(j)));
    aIP = size(IP);
    Q_IP(j)= aIP(1);

    probabilidade = (Q_IP(j)/ Tam_Janela);
    if probabilidade > v2*(1/Q_IPs_unicos3 )
      %v2 é o grau de rigidez do controle, valor default= 2.
        Tam_Vetor_IP_DEST = Tam_Vetor_IP_DEST+1;
        Vetor_IP_DEST (Tam_Vetor_IP_DEST)= IPs_unicos3(j);
        fprintf(' ---> ALERTA DE OCORRÊNCIA EXCESSIVA para o
        IP destino: %s \n', IPs_unicos3{j});
        fprintf(' Apresenta ocorrência elevada equivalente a
        probabilidade de %3f dentro da janela %d \n',
        probabilidade, janela);
    end
end

Vetor_IP_DEST;
Tam_Vetor_IP_DEST;

%PROTO = {'TCP', 'UDP', 'ICMP', 'HTTP'};
PROTO = {'TCP', 'DNS', 'TELNET'};
%vetor que contem os tipos de protocolos que serão analisados.

Alarme = protocolo ( janela,ind1,indn,Vetor_IP_DEST,PROTO);
```

```
Alarme_2 = Tam_Vetor_IP_DEST / Q_IPs_unicos3;
fprintf('O filtro 2, apresentou aproveitamento de %3f em
referencia a todos os IPs de destino analisados\n',Alarme_2);

fclose(fid);
```

Filtro 3

```
function [Alarme]=protocolo(janela,ind1,indn,IP_DEST,PROTO);


fprintf('\n Análise de detecção de Ataques DDoS compostos:
FILTRO ***3***:
 Combinação de Protocolos\n');

% Nesse momento entra em ação o código dos alunos de PIBITI,
onde deverá executar a determinada ação: a partir do arquivo
completo com todos os pacotes (de uma janela), filtras os
pacotes que estão nos vetores IP_DEST e PROTO, eliminando
todos os pacotes que não estiverem nessas condições.
% Depois separar em arquivos individuais organizados IPs de
 origem (arquivo % nome: X_IP_ORIG.txt).
%X é a janela

%Resumindo serão gerados para cada IP de origem um
% arquivo texto, porém os pacotes devem conter tanto os
 IP_DEST, quanto os PROTO definidos nos vetores.

fid=fopen('darpa.txt','r');
%fid=fopen('5colunas completo.txt','r');

%1. leitura do arquivo que contem os tempos dos pacotes;
InputText2 = textscan(fid, '%n %s %s %s %n');
%Criando o vetor com os tempos dos pacotes;
Tam_Janela = indn - ind1 +1;
%quantidade de pacotes sendo analizado (intervalo de pacotes
selecionado)
%Contagem de IPs de origem únicos:
Bloco2 = InputText2{2};
```

```
%a terceira coluna do arquivo é correspondente a coluna dos
IPs de destino
Intervalo2 = Bloco2 (ind1:indn);

%Array com os IPs de destino, apenas dentro do Intervalo
indicado
IPs_unicos2 = unique(Intervalo2)

%Array contendo todos os IPs de destinos (únicos) contidos
no Intervalo
Q_IPs_unicos2 = size(IPs_unicos2);
Q_IPs_unicos2 = Q_IPs_unicos2(1);

%valor do número de IPs unicos dentro do Intervalo
%deverão ser criados Q_IP_unicos2 arquivos .txt para essa
função



PROTO;
Q_PROTO = size(PROTO);
Q_PROTO = Q_PROTO(2);



 for j=1:Q_IPs_unicos2
%j marca os arquivos , k marca dentro do arquivo
    %ler os arquivos separados

arquivo=([num2str(janela),'_',num2str(IPs_unicos2{j}),'.txt']);
    fid = fopen (arquivo,'r');
  %  fid=fopen('IPzin.txt','r');
    InputText4 = textscan(fid, '%n %s %s %s %n');
    Bloco4 = InputText4{4};
  %  Intervalo4 = Bloco4 (ind1:indn);
```

```
  %  IPs_unicos4 = unique(Bloco4);
  %  Q_IPs_unicos4 = size(IPs_unicos4);
  %  Q_IPs_unicos4 = Q_IPs_unicos4(1);

  count=0;
 % fid = fopen([j,'_',IPs_unicos2{j},'.txt', 'r']);
   fid = fopen (arquivo,'r');
  %fid=fopen('IPzin.txt','r');
while ~feof(fid)
    line = fgetl(fid);
    if isempty(line) | strncmp(line, '%', 1)
        continue

    end
    count=count+1;
end
number_of_line(j) = count;
%contagem de linhas do arquivos, armazenadas no vetor


  for k=1:Q_PROTO
    PROTOCOLO = find(ismember(Bloco4, PROTO(k)));
    aPROTOCOLO = size(PROTOCOLO);
    Q_PROTOCOLO(k)= aPROTOCOLO(1);
    %quantidade de ocorrencias de um protocolo no arquivo

     probabilidade(k) =(Q_PROTOCOLO(k)/number_of_line(j));


  end

  Perfil_probabilidadeA(j)= probabilidade(1) ;
  Perfil_probabilidadeB(j)= probabilidade(2);
```

```
  Perfil_probabilidadeC(j)= probabilidade(3) ;
  %Perfil_probabilidadeD(j)= probabilidade(4) ;


 end

 Perfil_probabilidadeA;
 Perfil_probabilidadeB;
 Perfil_probabilidadeC;
% Perfil_probabilidadeD

     PPA = round(Perfil_probabilidadeA*10);
     PPB = round(Perfil_probabilidadeB*10);
     PPC = round(Perfil_probabilidadeC*10);
    % PPD = round(Perfil_probabilidadeD*10)

  MA =  mode(PPA);
    MB =  mode(PPB);
      MC =  mode(PPC);


 k1 = size(Perfil_probabilidadeA)   ;
 k1 = k1(2);


v3=1;
%v3 é o grau de rigidez do controle, valor default = 1

cont=0;
 for k=1:k1
     if PPA(k)>(MA - v3) && PPA(k)<(MA+v3)
           if PPB(k)>(MB - v3) && PPB(k)<(MB+v3)
                if PPC(k)>(MC - v3) && PPC(k)<(MC+v3)
```

```
                    cont= cont +1;
                    fprintf('Alarme!!!! %s IP ORIGEM suspeito
                    \n',IPs_unicos2{k});
                end
            end
        end
    end


Alarme_3 = cont / Q_IPs_unicos2;
fprintf('O filtro 3, apresentou aproveitamento de %3f em
referencia a todos os IPs de origem analisados\n',Alarme_3);

    Alarme = Perfil_probabilidadeA;
fclose(fid);
```