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

ANDRÉ OLIVEIRA CASTELUCIO

UMA REDE SOBREPOSTA NO NÍVEL DE SISTEMAS AUTÔNOMOS PARA RASTREAMENTO DE TRÁFEGO EM REDES IP

Rio de Janeiro
2008

INSTITUTO MILITAR DE ENGENHARIA

ANDRÉ OLIVEIRA CASTELUCIO

UMA REDE SOBREPOSTA NO NÍVEL DE SISTEMAS AUTÔNOMOS PARA RASTREAMENTO DE TRÁFEGO EM REDES IP

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.

Orientadores: Prof. Ronaldo M. Salles - Ph.D.
Prof. Artur Ziviani - Dr.

Rio de Janeiro
2008

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

C349 Castelucio, A. O.

Uma rede sobreposta no nível de Sistemas Autônomos para rastreamento de tráfego em redes IP/ André Oliveira Castelucio. – Rio de Janeiro: Instituto Militar de Engenharia, 2008.

81 p.: il., graf., tab.

Dissertação (mestrado) – Instituto Militar de Engenharia – Rio de Janeiro, 2008.

1. Redes de computadores. 2. Gerenciamento em redes. 3. Segurança em redes. I. Uma rede sobreposta no nível de Sistemas Autônomos para rastreamento de tráfego em redes IP. II. Instituto Militar de Engenharia.

CDD 004.6

INSTITUTO MILITAR DE ENGENHARIA

ANDRÉ OLIVEIRA CASTELUCIO

UMA REDE SOBREPOSTA NO NÍVEL DE SISTEMAS AUTÔNOMOS PARA RASTREAMENTO DE TRÁFEGO EM REDES IP

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.

Orientadores: Prof. Ronaldo M. Salles - Ph.D.
Prof. Artur Ziviani - Dr.

Aprovada em 03 de Abril de 2008 pela seguinte Banca Examinadora:

Prof. Ronaldo M. Salles - Ph.D. do IME - Presidente

Prof. Artur Ziviani - Dr. do LNCC

Profa. Raquel Coelho Gomes Pinto - DSc., do IME

Prof. Nilton Alves Jr. - DSc., do CBPF

Prof. José Ferreira de Rezende - Dr., da UFRJ

Rio de Janeiro
2008

Dedico este trabalho à minha família e meus amigos.

AGRADECIMENTOS

Agradeço à minha família por todo o esforço que fizeram para eu me tornar a pessoa que sou. À Vilma, por estar sempre ao meu lado nos momentos difíceis da minha vida e pela compreensão nas horas de estudo.

Aos amigos Grácia e Raul, por sempre me apoiarem e me motivarem a buscar o melhor.

Aos meus orientadores Artur Ziviani e Ronaldo Salles, por toda a amizade, dedicação e ensinamentos durante o tempo de mestrado e na jornada para que este trabalho pudesse ser realizado.

Aos meus amigos Marcos, Bruno e Freire, amigos de longas horas de estudo e que contribuíram com o desenvolvimento desta dissertação, seja através de críticas, idéias ou incentivos.

Por fim, ao Instituto Militar de Engenharia (IME) e ao Laboratório Nacional de Computação Científica (LNCC) pelo suporte operacional e a CAPES pelo suporte financeiro.

André Oliveira Castelucio

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

ACC	*Aggregate-Based Congestion Control*
AS	*Autonomous System*
ASN	*Autonomous System Number*
AS-SPT	*AS-Level Single Packet Traceback*
ASTS	*Autonomous System Traceback Server*
BGP	*Border Gateway Protocol*
BHRS	*BlackHole Route Server*
DGA	*Data Generation Agent*
DNS	*Domain Name Service*
DoS	*Denial of Service*
DDoS	*Distributed Denial of Service*
DrDoS	*Distributed Reflector Denial of Service*
FBG	*Filtro de Bloom Generalizado*
FBO	*Filtro de Bloom Original*
ICMP	*Internet Control Message Protocol*
IDPS	*Intrusion Detection and Prevention Systems*
ISP	*Internet Service Provider*
IME	*Instituto Militar de Engenharia*
IP	*Internet Protocol*
LNCC	*Laboratório Nacional de Computação Científica*
NAT	*Network Address Translation*
NS-2	*Network Simulator 2*
NEM	*Network Manipulator*
OSPF	*Open Shortest Path First*
QoS	*Quality of Service*
RAT	*Rastreamento de Ataques*
RFC	*Request for Comments*

SA	*Sistema Autônomo*
SCAR	*SPIE Collection and Reduction Agent*
SIP	*Session Initiation Protocol*
SPIE	*Source Path Isolation Engine*
STM	*SPIE Traceback Manager*
TCP	*Transmission Control Protocol*
TTL	*Time to Live*

RESUMO

Ataques distribuídos de negação de serviço (DDoS) atualmente representam uma grande ameaça à operação adequada de serviços na Internet. Nesta dissertação é proposto um sistema que cria uma rede sobreposta para o rastreamento de tráfego em redes IP a ser implementada no nível de Sistemas Autônomos (SAs) para lidar com essa ameaça. Este sistema de rastreamento de tráfego IP no nível de SAs contrasta com os trabalhos anteriores, pois ele não requer conhecimento prévio da topologia da rede enquanto permite o rastreamento de um único pacote bem como uma instalação parcial e incremental. A implementação do sistema de rastreamento é avaliada através de simulações, mostrando que a possibilidade de instalação parcial ofertada pelo nosso sistema provê resultados relevantes de rastreamento IP, tornando-o viável para redes de larga escala como a Internet.

ABSTRACT

Distributed Denial of Service (DDoS) attacks currently represent a serious threat to the appropriate operation of Internet services. In this dissertation is proposed an overlay network that provides an IP traceback system to be deployed at the level of Autonomous Systems (ASes) to deal with this threat. Our proposed AS-level IP traceback system contrasts with previous work as it does not require a priori knowledge of the network topology while allowing single packet traceback and incremental deployment. The placement problem of the traceback system is investigated through simulations, showing that the partial deployment offered by our proposed system provides relevant results in IP traceback, rendering it feasible for large-scale networks such as the Internet.

1 INTRODUÇÃO

Inicialmente, a Internet era destinada apenas às instituições acadêmicas e governamentais. Por este motivo, a preocupação com a segurança era menor do que nos dias atuais. Atualmente, devido a expansão da Internet, a evolução das redes e a sua utilização para fins comerciais, a segurança passou a ser tratada de outra forma e vem se tornando um problema cada vez mais crítico.

A Internet atual é vulnerável a ataques distribuídos de negação de serviço (DDoS- *Distributed Denial of Service*) (CERT, 2001; HUSSAIN, 2003; LAUFER, 2005a; MIRKOVIC, 2004; MOORE, 2006). Ataques desse tipo têm como objetivo fazer com que uma rede ou serviço oferecido por ela fiquem inacessíveis a usuários legítimos, o que geralmente é alcançado quando um atacante envia pacotes a uma taxa maior do que a vítima pode processar e tipicamente ocorre com múltiplas fontes enviando pacotes para a mesma vítima.

Para identificar a ocorrência de um ataque, geralmente são utilizados sistemas de detecção e prevenção de intrusão (IDPS- *Intrusion Detection and Prevention Systems*)(NIST, 2007). Após esta identificação, o próximo passo é encontrar a origem dos pacotes de ataque, para que em um terceiro passo, sejam tomadas providências para filtrá-los. É claro que a dimensão de um ataque pode ser enorme e com isso esta filtragem deve ser feita da forma mais distribuída possível, pois se for feita apenas localmente pode não diminuir o impacto do ataque.

1.1 MOTIVAÇÃO

Identificar a origem de ataques DDoS é uma tarefa desafiadora. Alguns motivos que contribuem para isto são: (i) o roteamento dos pacotes na rede é feito baseado apenas no endereço de destino do pacote IP; (ii) os pacotes IP não são autenticados no momento do seu encaminhamento, permitindo que pacotes com endereços forjados sejam utilizados em ataques DDoS (CERT, 1996; ISS, 2000); (iii) os pacotes também podem ser enviados

por máquinas chamadas zumbis, cujos proprietários não sabem que estão participando de um ataque; (iv) nenhuma informação sobre o encaminhamento dos pacotes é mantida nos roteadores intermediários devido a restrições de escalabilidade; (v) a identificação da origem de um ataque não significa necessariamente encontrar o atacante, pois ele pode estar protegido por um *firewall* ou por endereços privados e desta forma a identificação só será realizada até a borda da rede de onde os pacotes são provenientes.

Todos estes fatos são suficientes para que o atacante tenha uma garantia virtual de anonimato e indicam claramente a necessidade de criação de mecanismos para identificar, mesmo que parcialmente, a rota dos pacotes de ataque e o desenvolvimento de ferramentas para bloquear os ataques ao menos em alguns pontos estratégicos nesta rota.

1.2 SISTEMAS DE RASTREAMENTO DE TRÁFEGO

Os sistemas de rastreamento de tráfego IP tem como objetivo identificar a origem dos pacotes que estão trafegando na rede, encontrando sua verdadeira fonte. Eles são tipicamente propostos para identificar a origem de um ataque. Um exemplo da utilização de um sistema de rastreamento IP pode ser visto na FIG. 1.1, onde dois atacantes estão enviando pacotes para uma vítima, um servidor WEB, enquanto um usuário legítimo tenta acessá-lo. Neste caso, o administrador da rede do servidor WEB quer saber de onde estão vindo os pacotes de ataque, pois deseja bloqueá-los para que o servidor não fique inacessível para usuários legítimos e para que o ataque não cause danos. Neste cenário, a existência de um sistema de rastreamento IP permitiria que o administrador do servidor pudesse identificar de onde os ataques estão partindo e desta forma realizar algum tipo de bloqueio para os pacotes vindos desta origem.

Antes de escolher qual seria o tipo de sistema de rastreamento a ser desenvolvido, foram estudados diferentes cenários de ataques e os sistemas de rastreamentos existentes em cada cenário.

No primeiro cenário observado, foram considerados ataques sendo feitos de dentro do SA (Sistema Autônomo) da vítima, conforme ilustrado na FIG. 1.2, onde ataques realizados contra vítimas nos SAs 1 e 2 são provenientes de dentro dos próprios SAs. Neste caso, a instalação de um sistema de rastreamento dentro dos próprios SAs deve ser

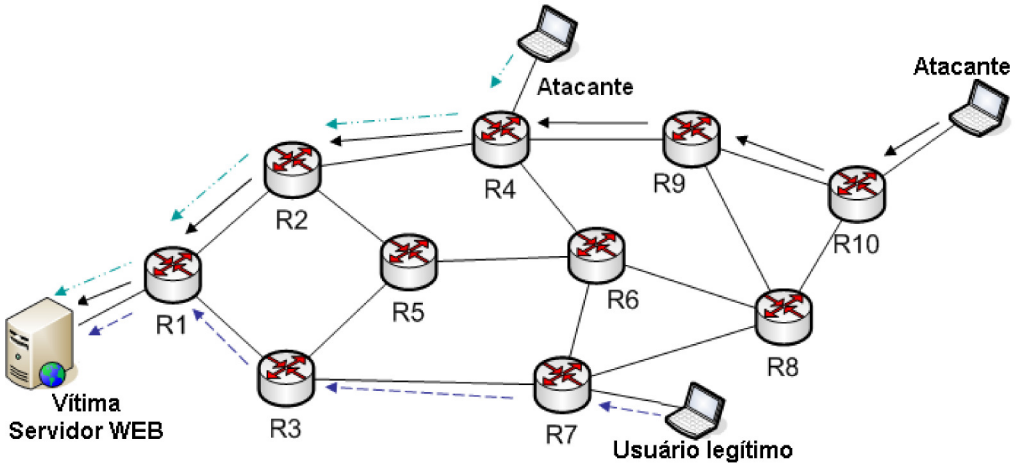

FIG. 1.1: Exemplo de utilidade do rastreamento de tráfego.

suficiente para rastrear o ataque. Note que os sistemas podem ser independentes.

Em um segundo cenário, exemplificado na FIG. 1.3, a vítima está recebendo pacotes de ataque tanto de dentro de seu próprio SA quanto de um SA externo. Neste cenário híbrido, a abordagem a ser utilizada seria a instalação de um sistema de rastreamento nos roteadores de borda dos SAs, que indicaria de qual SA está sendo enviado o tráfego de ataque, funcionando em conjunto com um sistema dentro do SA da vítima, que realizaria o rastreamento interno.

No terceiro cenário, analisado e ilustrado na FIG. 1.4, os pacotes são enviados por um atacante que está de fora do SA da vítima. Neste caso, a instalação do sistema nos roteadores de borda dos SAs é suficiente para descobrir de qual SA estão sendo enviados os pacotes de ataque.

Considerando o aumento dos ataques em larga escala (DDoS) nos últimos anos na Internet, nos quais pacotes são oriundos de diferentes redes, acredita-se que a instalação de sistemas de rastreamento apenas dentro das redes pode não ser suficiente para que o ataque seja rastreado e que os pacotes sejam bloqueados de forma eficiente, uma vez que o rastreamento será feito apenas até a borda da rede da vítima do ataque. Dependendo da escala do ataque, simplesmente bloquear o ataque no roteador de borda do SA da vítima pode fazer com que todo o SA fique inacessível para usuários legítimos. Da mesma forma, o desenvolvimento de um sistema híbrido, ou seja, que execute o rastreamento

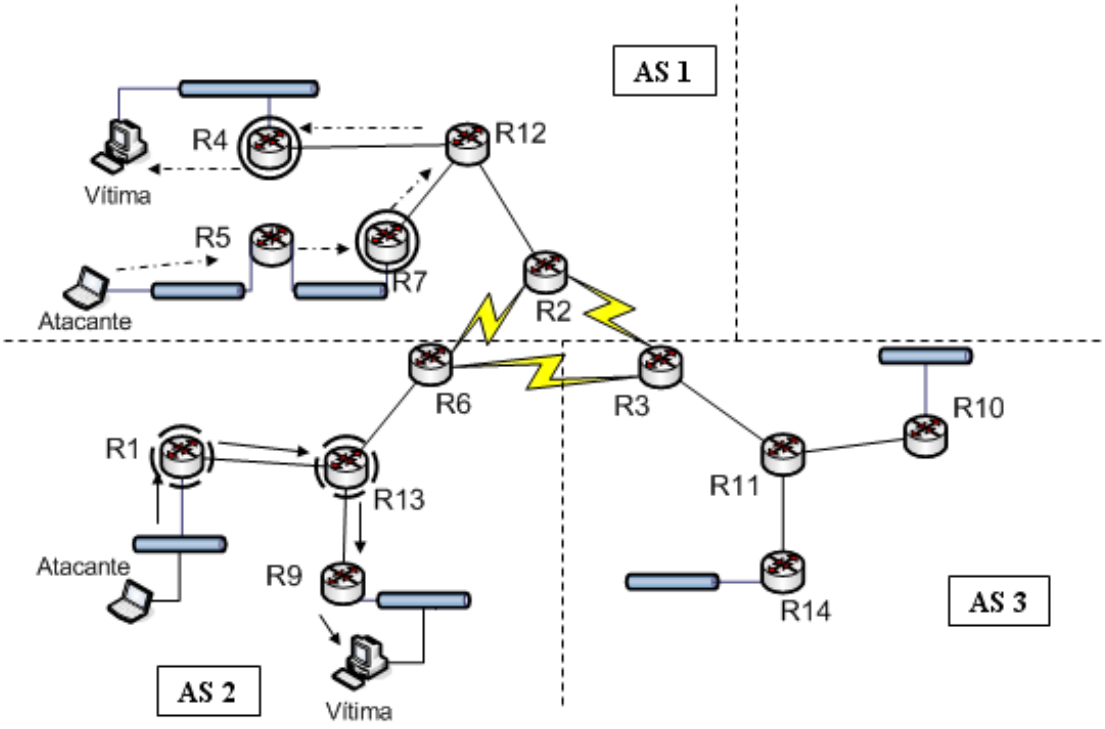

FIG. 1.2: Cenário de ataque 1.

tanto dentro da rede quanto nos roteadores de borda, pode ser inviável pois devem haver mecanismos para trocas de mensagem entre estes roteadores, o que poderia revelar, mesmo que parcialmente, a topologia interna de um SA – característica indesejável para a maioria dos operadores de SAs. Acredita-se que a instalação de um sistema de rastreamento apenas nas bordas dos SAs é suficiente para que medidas sejam tomadas contra os atacantes.

1.3 OBJETIVOS

Trabalhos relacionados na área de rastreamento de tráfego (discutidos mais profundamente no Capítulo 3) possuem como requisito típico a necessidade do sistema proposto por cada um deles ser instalado em todos os roteadores da rede monitorada. Isto ocorre devido a maneira como o rastreamento se realiza, onde o resultado esperado é o caminho *completo* por onde os pacotes passaram. Esse requisito claramente limita muito a possibilidade desses sistemas serem amplamente utilizados em uma rede de larga escala.

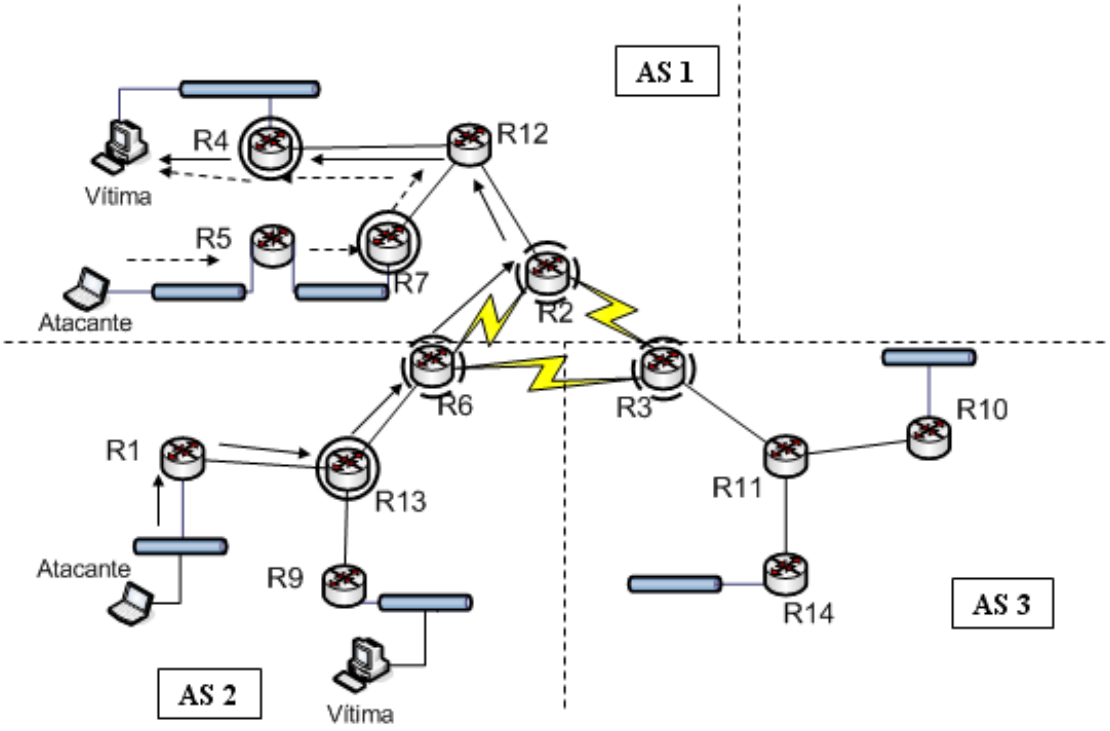

FIG. 1.3: Cenário de ataque 2.

Neste trabalho é proposto e avaliado um sistema para rastreamento de tráfego IP que trabalha no nível de Sistemas Autônomos e que pode ser instalado *parcialmente* em redes de larga escala como a Internet. A instalação desse sistema de rastreamento é feita nos roteadores de borda de alguns SAs, que após a troca de algumas informações transportadas pelo protocolo BGP (*Border Gateway Protocol*) (REKHTER, 1995), constroem uma rede sobreposta para rastreamento de tráfego IP.

Através de simulações é mostrado que o sistema aqui proposto pode ser instalado *apenas em alguns SAs* da rede e de forma *incremental*, permitindo que os SAs que queiram se juntar a qualquer momento à tarefa de rastreamento possam fazê-lo, aumentando assim a eficiência na identificação do caminho reverso do ataque. Além disso, os resultados indicam que mesmo com um número pequeno de SAs com o sistema instalado, desde que escolhidos estrategicamente, o rastreamento pode ser realizado de forma eficiente em redes de larga escala.

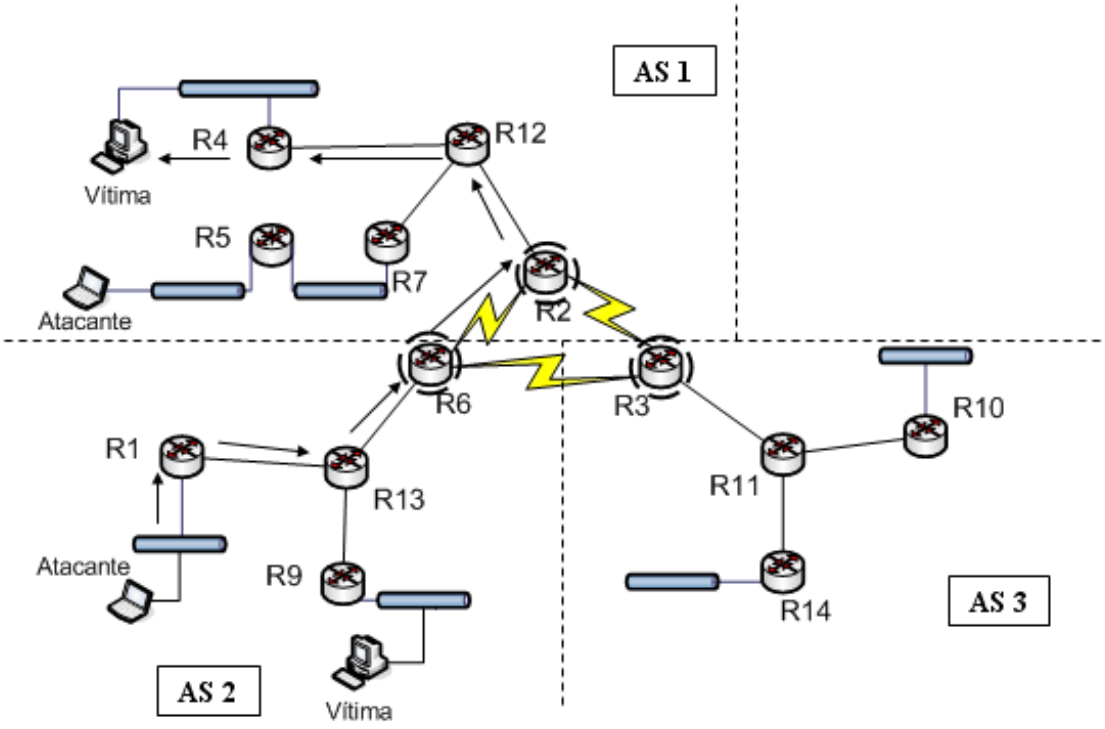

FIG. 1.4: Cenário de ataque 3.

1.4 ORGANIZAÇÃO DA DISSERTAÇÃO

Esta dissertação está organizada da seguinte forma:

No Capítulo 2 são abordados os principais ataques de negação de serviço e algumas técnicas que podem ser utilizadas para bloqueá-los e filtrá-los.

No Capítulo 3 são discutidos os principais sistemas de rastreamento de tráfego estudados.

No Capítulo 4 são detalhadas todas as características e o funcionamento do sistema proposto.

No Capítulo 5 são apresentadas as características das simulações realizadas e seus resultados.

Finalmente, no Capitulo 6 são realizadas as considerações finais sobre a dissertação juntamente com os trabalhos futuros.

2 ATAQUES DE NEGAÇÃO DE SERVIÇOS

Segundo um relatório anual da CSI/FBI (CSI/FBI, 2006), os ataques (D)DoS estão entre os incidentes de segurança que mais trazem prejuízos às empresas americanas, o que mostra uma necessidade de criar mecanismos para identificar de onde são originados e desenvolver ferramentas para bloquear seu andamento.

O principal objetivo de ataques (D)DoS é fazer com que uma rede ou serviço oferecido por ela fiquem inacessíveis a usuários legítimos. Isto geralmente ocorre quando os atacantes enviam uma grande quantidade de pacotes para a vítima, que quando não tem a capacidade de processar todos eles, começa a descartá-los de forma a avisar a origem destes pacotes, que neste momento são usuários legítimos e os próprios atacantes, que devem diminuir a quantidade de pacotes enviados. Neste momento, os usuários legítimos diminuem a taxa de envio de pacotes enquanto os atacantes mantêm ou aumentam sua taxa de envio. Em um dado momento, os recursos da vítima, tais como CPU e memória são esgotados, tornando a vítima incapaz de responder às novas requisições.

Neste capítulo serão mostrados como alguns tipos de ataques (D)DoS funcionam e afetam suas vítimas e o que pode ser feito após a identificação da origem dos ataques.

2.1 TCP SYN FLOOD

Neste tipo de ataque, conhecido como inundação de mensagens TCP SYN (CERT, 1996), os atacantes se aproveitam do procedimento de abertura do protocolo TCP conhecido como *three-way handshake*. O funcionamento detalhado do *three-way handshake* pode ser encontrado na RFC 793 (DARPA, 1981). Porém, o funcionamento básico será apresentado neste trabalho para que o ataque TCP SYN Flood possa ser entendido.

Durante a abertura de uma conexão TCP (FIG. 2.1), o *host* que deseja iniciar a conexão (A) envia uma mensagem TCP SYN para o *host* destino (B). Esta mensagem indica que uma abertura de conexão está sendo requisitada e possui um número de sequência inicial, que ajuda o receptor da mensagem reconhecer os dados perdidos, fora de ordem ou

até mesmo repetidos. Em um segundo momento, após um determinado tempo de processamento, o *host* B responde ao *host* A com uma mensagem TCP SYN+ACK, informando que o pedido de conexão requisitado foi aceito. Esta mensagem contém o reconhecimento do número de sequência enviado pelo *host* A e o número de sequência inicial do *host* B. Finalmente, o *host* A responde com uma mensagem TCP ACK, como reconhecimento ao número de sequência do *host* B, completando o processo de abertura de conexão entre os dois *hosts*, que a partir deste momento, podem começar a trocar dados entre si.

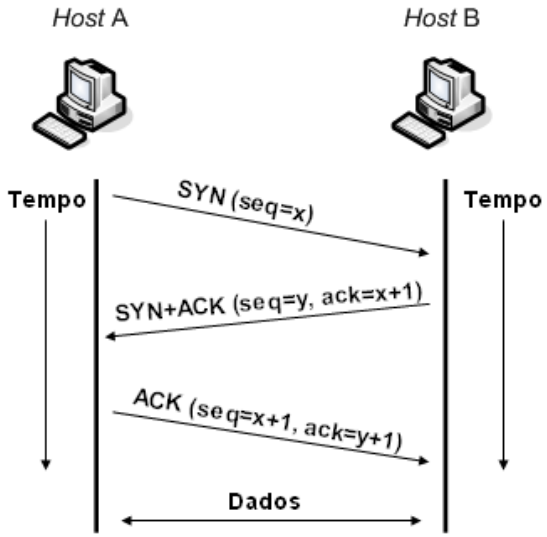

FIG. 2.1: Processo de abertura de uma conexão TCP.

Em um primeiro cenário de ataque TCP SYN Flood, o atacante envia diversas mensagens TCP SYN seguidamente para a vítima que não tem tempo de responder a todas as requisições, tendo seu processamento aumentado e esgotado para requisições de outros usuários, que neste momento são descartadas devido às inúmeras mensagens de abertura de conexão enviadas pelo atacante.

Em um outro cenário, o atacante usa endereços de IP de origem forjados, de forma que quando a vítima responde às mensagens TCP SYN, o faça para endereços inválidos, permitindo que as conexões TCP permaneçam em um estado conhecido como semi-aberto, ou seja, aguardando por um uma mensagem ACK da origem, neste caso o atacante, que como tem endereços IP de origem forjados, não vai enviar as mensagens ACK. Como

consequência, os recursos de memória da vítima são esgotados devido a grande quantidade de conexões no estado semi-aberto.

2.2 ICMP FLOOD

Este tipo de ataque também conhecido como *smurf* (CERT, 2000) é constituido de três personagens: o atacante, o nó intermediário e a vítima (note que o intermediário também pode ser a vítima). Em seu funcionamento, o atacante envia pacotes ICMP Echo Request para o endereço de *broadcast* da rede do nó intermediário usando o endereço de IP de origem da vítima. Como resposta a estes pacotes, todos os *hosts* que pertencem a mesma rede onde está localizado o nó intermediário enviam um pacote ICMP Echo Reply de volta para a vítima, uma vez que o atacante enviou os pacotes iniciais utilizando o endereço da vítima. Neste caso, a vítima tem seus recursos esgotados e se torna incapaz de responder a novas requisições.

2.3 ATAQUE POR REFLETOR

No ataque por refletor, também chamado DrDoS (Distributed Reflector Denial of Service) (PAXSON, 2001), o atacante utiliza máquinas zumbis para encaminhar o tráfego de ataque para a vítima. Essas máquinas zumbis, conhecidas como refletores, recebem os pacotes do atacante com o endereço IP de origem forjado como se fossem originados pela vítima. Devido a esta característica, as respostas enviadas pelos refletores são enviadas diretamente para a vítima.

No ataque por refletor é comum a utilização do protocolo TCP justamente por causa do *three-way handshake*, onde os refletores recebem as mensagens TCP SYN do atacante e respondem com as mensagens TCP SYN+ACK para a vítima. Devido a utilização de endereços IP de origem verdadeiros neste tipo de ataque a identificação do atacante é muito difícil.

2.4 SIP FLOOD

O protocolo SIP (*Session Initiation Protocol*) (ROSENBERG, 2002) é um protocolo do nível de aplicação utilizado para se estabelecer, modificar ou terminar uma sessão multimídia e é comumente utilizado em aplicações de voz sobre IP. A FIG. 2.2 ilustra o processo básico de abertura de uma conexão SIP, onde o *host* A deseja se comunicar com o *host* B. Inicialmente o *host* A envia um pacote do tipo *Invite* para o computador B que tipicamente é encaminhado para o servidor *proxy* SIP do *host* A (passo(1)). Este por sua vez, faz uma busca no servidor DNS (*Domain Name Service*)[1] procurando pelo endereço do servidor *proxy* SIP do *host* B (passo (2)). De posse do endereço (passo(3)), o servidor *proxy* SIP do *host* A envia o pacote *Invite* para o servidor *proxy* SIP do *host* B (passo(4)). Finalmente, o servidor proxy SIP do *host* B repassa o pacote *Invite* para o *host* B (passo(5)). A partir deste momento, a comunicação pode ser estabelecida.

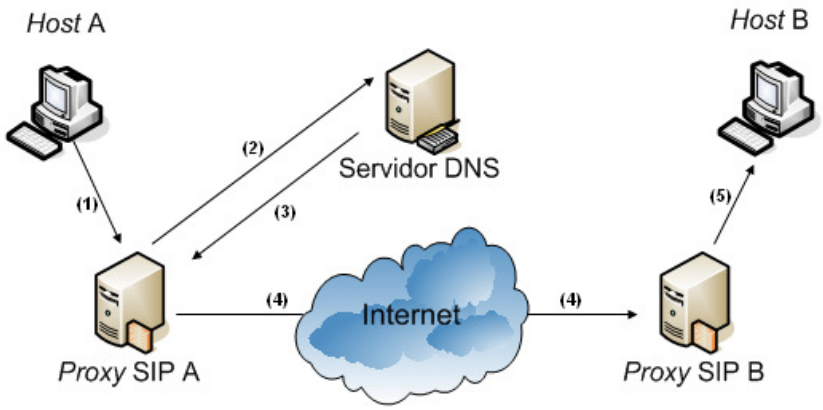

FIG. 2.2: Processo de abertura de uma conexão SIP.

O ataque do tipo SIP Flood pode ocorrer quando atacante inunda o *proxy* SIP com uma grande quantidade de mensagens *Invite* com endereços de IP forjados (CHEN, 2006) ou em uma segunda abordagem, se o atacante utiliza endereços IP válidos de máquinas zumbis para realizar a inundação. Neste caso, não só os *proxies* SIP ficam sobrecarregados demais para prover o serviço necessário para o estabelecimento da conexão, como os *hosts*

[1]É um servidor que faz a tradução de nomes de domínios para endereços IP.

que estão recebendo as mensagens *Invite* originadas do atacante ficam impossibilitados de responder a requisições de usuários legítimos.

2.5 ATAQUES À INFRA-ESTRUTURA DA REDE

Nesta modalidade de ataque, o atacante tipicamente tenta consumir todos os recursos da rede da vítima com o tráfego gerado pelos pacotes de ataque. Desta forma, a vítima não é atacada diretamente, mas fica incapacitada de responder às requisições provenientes de usuários legítimos, uma vez que em algum ponto da rede entre eles e a vítima, existe algum tipo de estrangulamento dos recursos da rede.

Um exemplo de ataque deste tipo pode ser efetuado em servidores DNS (MOCKAPETRIS, 1987) de forma que um *site* fique inacessível. Para que um determinado *site* seja acessado, geralmente as pessoas utilizam o nome do *site*, por exemplo www.ime.eb.br e o servidor DNS faz a conversão deste nome em endereço IP. Para que um ataque seja realizado, os atacantes enviam inúmeras consultas aos servidores DNS da entidade atacada, que podem deixar de responder às consultas e fica inacessível. Um ataque deste tipo foi efetuado em Outubro de 2002 nos 13 principais servidores DNS da Internet (CAIDA, 2002; VIXIE, 2002), que ficaram sobrecarregados e não conseguiram responder às consultas feitas pelos usuários.

2.6 FORMAS DE BLOQUEIO DE ATAQUES

Nesta seção serão abordadas técnicas que podem ser utilizadas para tentar minimizar os danos causados pelo tráfego de ataque, seja através de filtro ou bloqueio destes pacotes. Tais técnicas podem ser utilizadas após a conclusão da etapa de identificação da origem dos atacantes, ou seja, do rastreamento do tráfego.

2.6.1 FILTRAGEM DE PACOTES E CONTROLE DE ACESSO

Nesta técnica, proposta na RFC 2827 (FERGUSON, 2002), os roteadores de ingresso de um SA descartam pacotes que tenham endereço IP de origem dentro de uma faixa de endereços que não são anunciados por eles, isto é, se o endereço de origem de um pacote

está dentro da faixa de endereços 200.40.x.x à 200.60.x.x e os roteadores de ingresso de um SA não anunciam esta faixa de endereços, todos os pacotes com o endereço IP de origem que pertencem a esta faixa são descartados.

A filtragem pode ser configurada através de regras nos sistemas *firewalls* para que somente tráfego autorizado entre na rede. Porém, essas regras trazem uma série de problemas pois devem ser configuradas manualmente e aumentam consideravelmente o processamento dos sistemas, uma vez que o processamento é realizado por pacote. Um outro problema é que é inviável que sejam configuradas em servidores WEB e redes de trânsito, já que elas necessitam receber tráfego de diversas origens.

2.6.2 CONTROLE DE TRÁFEGO

No sistema proposto por Mahajan et al. (MAHAJAN, 2002), o mecanismo ACC (*Aggregate-Based Congestion Control*) habilita um roteador congestionado identificar o fluxo responsável pelo tráfego e controlar o *throughput*[2], ajudando a prevenir a degradação da largura de banda. O ACC deve ser capaz de detectar o congestionamento, identificar os fluxos responsáveis, determinar uma largura de banda limite para os fluxos, e se preciso usar *pushback*[3] e rever a largura de banda quando o congestionamento diminuir.

Com os resultados das simulações apresentadas no artigo, seus autores consideram que a utilização do mecanismo ACC é indicada para controle de congestionamento de fluxos agregados. Porém, segundo os autores, muitos fatores ainda devem ser estudados para sua implementação, como por exemplo se o *pushback* pode prejudicar tráfegos legítimos que estão muito perto do atacante se não for feita uma diferenciação entre os tipos de tráfego.

2.6.3 ALTERAÇÕES NO ROTEAMENTO

Na técnica conhecida como *Enhanced BGP-Triggered Black Holing*, proposta na RFC 3882 (TURK, 2004), é utilizado o `Community Attribute` (CHANDRA, 1996) do proto-

[2]É a velocidade de transmissão dos dados de um lugar para outro ou o número de pacotes que foram gerados e recebidos sem perda de pacotes.

[3]É o mecanismo pelo qual roteadores congestionados são capazes de requisitar a seus roteadores adjacentes que estão gerando um alto tráfego agregado que limitem sua taxa de *upstream*, diminuindo assim o congestionamento.

colo BGP (REKHTER, 1995) (detalhes sobre esta característica do BGP serão abordadas na Seção 4.3) para redirecionar o tráfego de ataque para uma interface nula dos roteadores de borda do SA. Em outras palavras, quando um tráfego de ataque é detectado em alguma interface do roteador de borda do SA, algumas novas rotas são configuradas neste roteador de borda para que o tráfego que está sendo enviado para a vítima seja classificado e os pacotes de ataque sejam desviados para um "buraco negro", configurado com endereços de rede inválidos para a Internet (REKHTER, 1996). Neste caso, o tráfego que é classificado como tráfego de ataque é descartado, enquanto o tráfego legítimo continua sendo encaminhado normalmente pela rede. Usando esta mesma técnica, o tráfego de ataque pode ainda ser encaminhado para um túnel ao invés de ser descartado, para que tenha suas características analisadas.

Nas versões iniciais desta técnica, todos os pacotes que chegavam na interface do roteador de borda por onde o ataque foi detectado, cujo destino era a vítima, eram redirecionados para endereços de rede inválidos através da reconfiguração de roteamento do BGP. Porém, como não existia uma diferenciação nos pacotes, todo o tráfego era descartado e sendo assim a vítima e a rede da vítima se tornavam inacessíveis não só para o atacante como também para usuários legítimos.

3 TRABALHOS RELACIONADOS

Vários sistemas de rastreamento de tráfego IP foram propostos nos últimos anos. Pode-se destacar dois artigos (ALJIFRI, 2003; BELENKY, 2003) como pontos chave para se fazer uma comparação entre os sistemas existentes. Mais adiante, vamos fazer referência ao artigo (BELENKY, 2003) por acreditarmos ser o mais completo.

Podemos dividir os sistemas de rastreamento IP em duas classes de operação: os que trabalham no nível de roteadores (*router-level*), que são os sistemas mais tradicionais e os que trabalham no nível de Sistemas Autônomos (*AS-level*), que são os sistemas mais atuais incluindo o proposto neste trabalho. Um resumo dos principais sistemas de rastreamento IP pode ser encontrado neste capítulo.

3.1 SISTEMAS DE RASTREAMENTO QUE OPERAM NO NÍVEL DE ROTEADORES

Tipicamente, os sistemas *router-level* foram propostos para funcionar dentro de um SA, rastreando ataques internos. Conforme já foi dito anteriormente, estes sistemas tem o propósito de encontrar o caminho completo por onde os pacotes de ataque passaram. Porém, isto não garante que os atacantes serão encontrados com mais precisão, uma vez que a precisão implica em encontrar o primeiro roteador que encaminha os pacotes de ataque e não todos os roteadores do caminho.

3.1.1 AMOSTRAGEM DE TRAJETÓRIA

Duffield e Grossglauser (DUFFIELD, 2001) propuseram um método de amostragem de trajetória de pacotes que trafegam por uma rede. A grande motivação do trabalho é a necessidade de se fazer engenharia de tráfego na rede e a colocação de QoS. Porém, apesar do sistema proposto no trabalho não ter foco em rastreamento de tráfego, ele também pode ser utilizado com este propósito.

Através do sistema proposto, é feita uma amostragem de um mesmo subconjunto de pacotes em todos os roteadores por onde passam. Esta amostragem é garantida por uma mesma função *hash* utilizada por todos os roteadores, que opera sobre partes invariantes do pacote, isto é, nos bits do pacote que não mudam durante o seu encaminhamento pela rede. Devido a essa característica, alguns pacotes nunca serão amostrados enquanto outros sempre serão amostrados. Para se identificar a trajetória, é utilizada uma segunda função de *hash*, responsável pela geração de uma etiqueta, que é unica por pacote. Através dela, pode-se conhecer o caminho por onde o pacote passou, uma vez que os roteadores terão observado a passagem da mesma etiqueta.

3.1.2 INSERÇÃO DE TRÁFEGO CONTROLADO

Burch e Cheswich (BURCH, 2000) propuseram um sistema de rastreamento IP onde a origem do ataque é detectado através da inserção de tráfego (de forma controlada) nos enlaces entre os roteadores. Neste sistema (FIG. 3.1), quando o ataque é detectado, o administrador da rede mais próxima da vítima se conecta ao roteador da rede por onde os pacotes de ataque chegam à vitima (passo (1)) e injeta tráfego nos enlaces com os roteadores adjacentes (passo (2)), esperando pela diminuição do tráfego de ataque. Esta diminuição ocorre porque os pacotes inseridos de forma controlada se misturam aos pacotes de ataque, fazendo com que estes diminuam sua frequência. Desta forma, o administrador da rede consegue identificar o próximo roteador no caminho reverso do ataque (passo (3)), que em um próximo passo é acessado pelo administrador, que recomeça o processo até que o primeiro roteador responsável por encaminhar os pacotes de ataque seja encontrado.

Alguns problemas deste sistema são: a necessidade do conhecimento prévio da topologia da rede, a ineficiência contra ataques distribuídos, a disponibilidade dos nós para sofrerem curtas inundações de tráfego, já que durante o ataque seus recursos já estarão sendo consumidos e a inundação por si só pode gerar um cenário de negação de serviços e a configuração padrão nos roteadores que mantêm desabilitado o serviço necessário para a utilização do sistema.

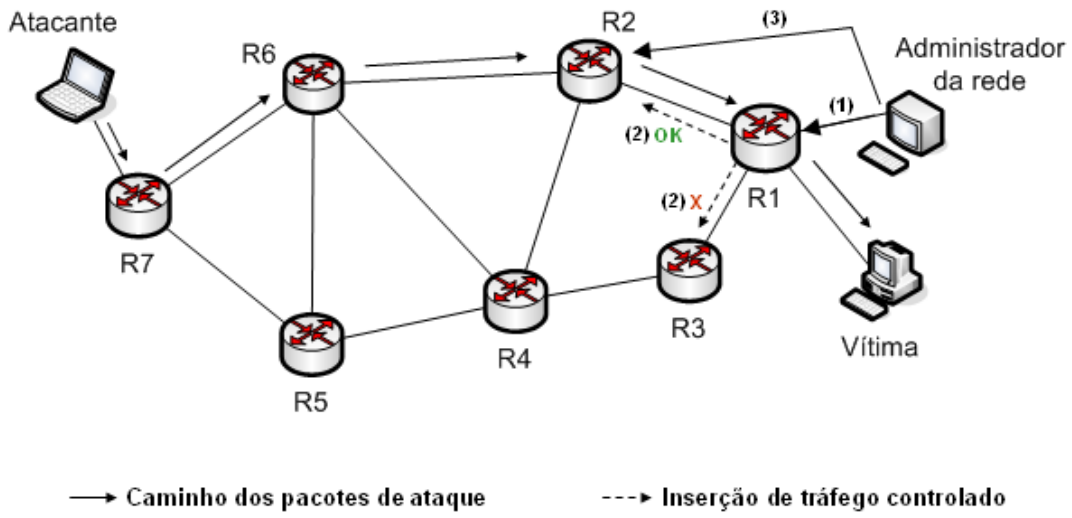

FIG. 3.1: Sistema de Burch e Cheswick (BURCH, 2000).

3.1.3 CENTERTRACK

Stone (STONE, 2000) propôs a idéia de se criar uma rede sobreposta para detectar a origem dos ataques. No funcionamento do sistema, todo o tráfego da rede é monitorado por um roteador chamado TR (*Tracking Router*). Quando uma assinatura de ataque é detectada, túneis são montados com o protocolo GRE (*Generic Route Encapsulation*)[4], entre os roteadores de borda da rede e o TR. Assim, o TR é capaz de descobrir por qual túnel o tráfego está sendo encaminhado e por consequência a origem do ataque.

Dentre os problemas deste sistema podemos considerar: a limitação de funcionar bem apenas dentro de um SA, pois para os túneis serem formados entre SAs, deve haver um protocolo que conecte os diversos TRs dos SAs que participam do sistema de rastreamento, fazendo com que os TRs se comportem como se estivessem em um único sistema; a existência de um ponto único de falha, neste caso o TR; e o envolvimento do ISP (*Internet Service Provider*) que é muito alto no momento do rastreamento.

[4]Protocolo de tunelamento utilizado em VPNs (*Virtual Private Networks*).

3.1.4 MARCAÇÃO PROBABILÍSTICA DE PACOTES

Savage et al. (SAVAGE, 2000) propuseram um sistema baseado em marcação probabilística de pacotes. Em sistemas com esta característica, os pacotes são submetidos a algum tipo de marcação a medida que passam pelos roteadores. Neste sistema em questão, os pacotes tem uma probabilidade p de 0,04 de serem marcados. Esta marcação contém informações sobre a rota atravessada pelo pacote e é feita no campo de fragmentação do pacote IP. Depois de uma quantidade expressiva de pacotes ser recebida pela vítima, esta executa um procedimento sendo capaz de reconstruir o caminho de ataque.

Dentre os principais problemas deste sistema estão: o aumento de processamento na vítima no momento do rastreamento (SONG, 2001), uma vez que ela é responsável pela reconstrução da rota, e a necessidade de uma grande quantidade de pacotes recebidos por parte da vítima para que ela possa realizar o rastreamento.

Em 2003, Bellovin et al. (BELLOVIN, 2003) introduziram um outro sistema baseado em marcação probabilística de pacotes. Conforme os pacotes passam pelos roteadores, 1/20000 são sorteados e para cada um deles, uma mensagem ICMP (*Internet Control Message Protocol*) é enviada para o mesmo destino do pacote escolhido, carregando informações sobre o pacote selecionado e sobre o roteador que gerou esta mensagem ICMP, incluindo próximo salto, salto anterior, uma marcação de tempo e o tempo de vida (TTL-*Time to Live*) do pacote. Tal informação é usada pela vítima no momento da reconstrução da rota.

Alguns problemas encontrados para a adoção deste sistema são a quantidade de pacotes de ataque necessárias para se efetuar o rastreamento, o tráfego extra na rede devido a inserção das mensagens ICMP, a possibilidade do atacante enviar mensagens ICMP forjadas se não for utilizado um mecanismo de autenticação e o possível filtro de mensagens ICMP em diversas redes por motivos de segurança.

3.1.5 SISTEMA SPIE

Snoeren et al. (SNOEREN, 2002) propuseram o sistema SPIE (*Source Path Isolation Engine*), que tem como característica principal o armazenamento do resumo dos pacotes em Filtros de Bloom (BLOOM, 1970), a medida que estes são encaminhados pelos

roteadores. Uma visão geral da aplicabilidade de Filtros de Bloom em rede pode ser consultada em (BRODER, 2004). Esses resumos são gerados e armazenados por dispositivos chamados DGA (*Data Generation Agent*), acoplados aos roteadores. Outros dispositivos chamados SCAR (*SPIE Collection and Reduction Agent*) são responsáveis pela execução de consultas em DGAs específicos de algumas regiões da rede por onde o pacote passou para identicar os roteadores que os encaminharam. Dessa forma, cada SCAR da rede é capaz de gerar um grafo parcial do ataque. Em seguida, outro dispositivo denominado STM (*SPIE Traceback Manager*) fica responsável por criar o grafo final do ataque com as informações de grafos parciais recolhidas nos SCARs. Diferentemente dos sistemas baseados em marcação probabilística de pacotes, através do uso de Filtros de Bloom este sistema pode rastrear um pacote IP individual.

Um dos principais problemas para a adoção deste sistema é a necessidade de adquirir novos dispositivos (DGA, STM, SCAR).

3.1.6 SISTEMA RAT

Laufer et al. (LAUFER, 2005b) introduziram um outro sistema baseado em Filtros de Bloom. Porém, a forma de armazenamento do Filtro neste sistema foi modificado. Aqui, quando um pacote atravessa um roteador, é inserida uma marca dentro de um Filtro de Bloom Generalizado (FBG) (LAUFER, 2005c), presente no cabeçalho do pacote IP. Essa marca é o resultado de uma função de *hash* do endereço IP da interface de saída do roteador. Quando o pacote alcança o destino, ele carrega dentro do FBG a marca de todos os roteadores por onde passou. O processo de rastreamento pode ser acompanhado na (FIG. 3.2). Para iniciar o rastreamento, a vítima verifica quais dos roteadores vizinhos possuem a marca no FBG e envia um pacote de reconstrução de rota para ele (passo (1)). Por sua vez, este roteador também verifica o FBG a procura da marca de um de seus vizinhos (passo (2)). Este procedimento é repetido até que o último roteador no caminho reverso do ataque seja descoberto – ou que nenhum roteador tenha sua marca encontrada no FGB. Finalmente, para finalizar o rastreamento, o último roteador encontrado no processo envia uma mensagem de volta a vítima com a rota por onde o pacote passou (passo (3)). De forma similar ao SPIE, este sistema pode rastrear um único pacote.

Dentre os problemas para a adoção deste sistema, considera-se a duplicidade de caminhos no momento da reconstrução da rota (problema este abordado mais adiante na Seção 4.6) e a necessidade da vítima ser responsável por receber os pacotes de reconstrução de rota com os caminhos percorridos pelos pacotes de ataque para que alguma providência seja tomada, em um momento em que seus recursos já estão escassos durante um ataque (D)DoS.

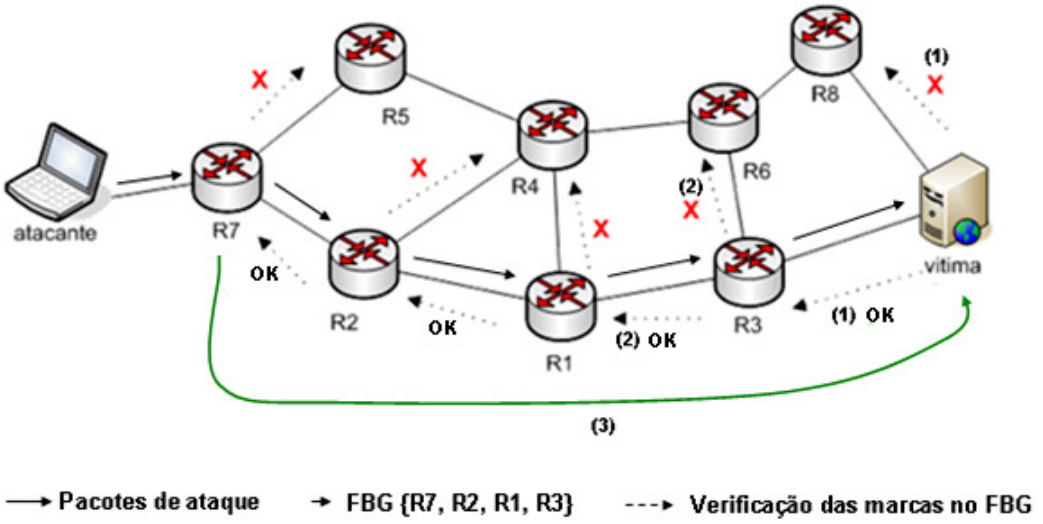

FIG. 3.2: Sistema de Laufer et al. (LAUFER, 2005b).

3.1.7 COMPARAÇÃO DOS PRINCIPAIS SISTEMAS DE RASTREAMENTO IP

Belenky e Ansari (BELENKY, 2003) fizeram uma análise dos principais sistemas de rastreamento propostos nos últimos anos. As métricas utilizadas para a comparação dos sistemas foram:

a) Envolvimento do ISP: foi considerado que atualmente o rastreamento mesmo em um único ISP é feito de forma manual e que os ISPs não possuem incentivos para monitorar os pacotes de ataque. Considerou-se também a necessidade de se adquirir

equipamentos adicionais e atualizações em equipamentos existentes. Além disso foi verificada a facilidade de implementar o sistema, implicando em apenas pequenas modificações na estrutura. Para esta métrica o resultado ideal deve ser baixo ou muito baixo;

b) Número de pacotes de ataques necessários para rastreamento: foi verificado que os ataques podem ser constituídos de poucos ou muitos pacotes e que o sistema deve precisar apenas de um número reduzido de pacotes para ser eficiente, de forma que se um sistema pode rastrear um ataque com um pequeno número de pacotes, ele é capaz de rastrear uma grande quantidade de atacantes mais rapidamente. Para esta métrica, o resultado ideal é um único pacote;

c) Efeito de instalação parcial: deve-se ter em mente que a instalação de um sistema de rastreamento em uma rede de larga escala, como a Internet por exemplo, não pode ser feita rapidamente e a curto prazo. Por este motivo, um sistema deve produzir resultados significativos mesmo quando não for instalaldo em toda estrutura da rede. Desta forma, além de ter os custos e a dificuldade de instalação diminuídos, é considerado mais prático e eficiente;

d) *Overhead* de processamento. Nesta métrica foram feitas duas considerações: (i) onde ocorre: geralmente na rede do ISP ou nas vítimas. O *overhead* nos roteadores do ISP é indesejável, pois pode significar atualizações e compra de novos equipamentos; (ii) quando ocorre: durante o tráfego dos pacotes pela rede ou considerando-se um sistema ideal, somente durante o rastreamento.

e) *Overhead* de largura de banda: o *overhead* alto é indesejável, pois pode esgotar capacidade dos enlaces e dispositivos da rede e requerer custos com atualizações. É ideal que seja pequeno e somente durante o processo de rastreamento;

f) Requisitos de memória: memória adicional nos roteadores pode significar atualizações, que é indesejável. Porém, o atualizações de memória nos servidores é tolerável;

g) Facilidade de evasão: a capacidade do atacante realizar um ataque burlando o sistema deve ser a mais baixa possível;

h) Proteção: é a habilidade de um sistema produzir resultados significativos se um número limitado de elementos participantes do rastreamento for subvertido. O bom sistema deve produzir bons resultados mesmo se isso acontecer;

i) Escalabilidade: relacionada a quantidade de configuração que deve ser feita se um novo dispositivo for adicionado no sistema de rastreamento. Também é considerado o funcionamento do sistema de acordo com o crescimento da rede. O sistema ideal deve ser escalável e a configuração de dispositivos envolvidos deve ser independente;

j) Número de funções necessárias para implementação: é a quantidade de funções diferentes que devem ser implementadas para que o sistema funcione. Por exemplo, uma função de marcação de pacotes e outra de reconstrução do caminho dos pacotes. O ideal é que apenas uma função seja implementada;

k) Habilidade de lidar com principais ataques (D)DoS: métrica extremamente importante. Ela reflete se o sistema pode executar o rastreamento em situações muito difíceis. Por exemplo, quando um grande número de atacantes utilizam endereços IP de origem forjados. Foi observado que muitos sistemas avaliados no artigo não conseguem lidar com todos os tipos de ataque, o que não é desejável em um sistema ideal;

l) Habilidade de rastrear pacotes transformados: a transformação nos pacotes ocorre durante seu encaminhamento na rede—através de NAT (*Network Address Translation*)[5], tunelamento em VPNs, fragmentação. O sistema ideal deve conseguir rastrear pacotes transformados. De outra forma, o atacante pode usar esta característica para não ser rastreado.

Dentre os sistemas avaliados no artigo, destacam-se os seguintes: (BELLOVIN, 2003; SAVAGE, 2000; SNOEREN, 2002; STONE, 2000). A TAB. 3.1 ilustra a comparação feita

[5]É a técnica utilizada para substituir o endereço IP de origem de um pacote que passa por um roteador ou *firewall*, de maneira que um computador com um endereço de origem inválido para a Internet possa acessá-la.

no artigo. Para este trabalho, foi inserido na comparação o sistema RAT, proposto por Laufer et al. (LAUFER, 2005b).

TAB. 3.1: Comparação dos sistemas de rastreamento que operam no nível de roteadores.

		Savage, 2000	Bellovin, 2003	Snoeren, 2002	Laufer, 2005b	Stone, 2000
Envolvimento do ISP		Baixo	Baixo	Médio	Médio	Alto
Escalabilidade		Alta	Alta	Média	Alta	Ruim
Funções implementadas pelo fornecedor		2	2	3	2	Nenhuma
N° de pacotes necessários para rastreamento		Milhares	Milhares	1	1	1
Implementação parcial é possível?		Sim	Sim	Sim	Não	Não
Necessidade de conhecimento da topologia e roteamento para rastreamento?		Sim, se implementado parcialmente	Sim, se implementado parcialmente	Sim, se implementado parcialmente	Não	Não
Possível implementar entre ISPs?		Sim	Sim	Sim	Não	Não
Overhead de processamento na rede	Cada pacote	Baixo	Baixo	Baixo	Baixo	Baixo
	Durante rastreamento	Nenhum	Nenhum	Baixo	Baixo	Baixo
Overhead de processamento na vítima	Cada pacote	Nenhum	Nenhum	Nenhum	Nenhum	Nenhum
	Durante rastreamento	Alto	Alto	Nenhum	Baixo	Nenhum
Overhead na largura de banda	Cada pacote	Nenhum	Baixo	Nenhum	Nenhum	Alto
	Durante rastreamento	Nenhum	Nenhum	Baixo	Baixo	Nenhum
Requisitos de memória	Na rede	Nenhum	Baixo	Médio	Baixo	Baixo
	Na vítima	Alto	Alto	Nenhum	Baixo	Nenhum
Facilidade de evasão		Baixa	Alta	Baixa	Baixa	Baixa
Proteção		Alta	Alta	Baixa	Baixa	Média
Habilidade no tratamento de ataques DDoS		Ruim	Ruim	Boa	Ótima	Boa
Habilidade de tratar pacotes transformados		Boa	Boa	Boa	Ótima	Boa

3.2 SISTEMAS DE RASTREAMENTO QUE OPERAM NO NÍVEL DE SISTEMAS AUTÔNOMOS

Analisando os sistemas discutidos até o momento, observamos que dificilmente eles podem ser adotados de forma efetiva em redes de larga escala, como a Internet. Algumas razões que contribuem para este argumento incluem: (i) a necessidade de se adquirir novos dispositivos; (ii) o aumento do processamento na rede, tanto nos roteadores intermediários quanto na vítima no momento em que o rastreamento é feito; (iii) a escalabilidade limitada; (iv) a necessidade de mecanismos de autenticação; (v) e a necessidade de conhecimento prévio da topologia da rede. Além de todos esses motivos, foi observado que todos os sistemas analisados necessitam que sua instalação seja feita em *todos* os roteadores da rede monitorada, desta forma contribuindo para que a instalação do sistema na Internet seja inviável – e limitando sua eficácia contra ataques DDoS em larga escala.

É importante ressaltar que a instalação de um sistema de rastreamento em *todos* os roteadores da rede monitorada pode não ser necessária para garantir um rastreamento eficiente. Na realidade, considerando-se que no caso de um ataque (D)DoS o principal

objetivo é encontrar o(s) atacante(s) para bloquear os pacotes enviados por ele(s), a instalação de um sistema de rastreamento se faz necessária apenas em alguns pontos críticos no caminho por onde os pacotes de ataque são encaminhados (por exemplo no SA que encaminha uma grande quantidade de pacotes de ataque) para que providências contra os atacantes possam ser tomadas de forma eficaz. Os sistemas que são desenvolvidos levando em consideração este argumento tipicamente operam no nível de Sistemas Autônomos.

3.2.1 MARCAÇÃO PROBABILÍSTICA DE PACOTES

Durresi et al. (DURRESI, 2004) propuseram um sistema de rastreamento no nível de SA usando a técnica de marcação probabilística de pacotes. Contudo, diferente de outros sistemas que usam esta técnica, a informação é inserida nos pacotes pelos roteadores de borda dos SAs usando o ASN (*Autonomous System Number*)[6] ao invés do endereço IP do roteador, desta forma necessitando de um espaço menor de armazenamento no cabeçalho do pacote. Entretanto, sistemas baseados em marcação probabilística de pacotes podem ser enganados por um atacante que insere marcações nos pacotes criando falsos positivos (PARK, 2001). Para tratar este problema, os autores introduzem um esquema de autenticação utilizando criptografia de chave simétrica que deve ser usada por todos os roteadores de borda dos SAs, o que acaba se tornando um dos problemas para a adoção do sistema.

Em 2006, Martins et al. (MARTINS, 2006) propuseram um sistema que utiliza o protocolo BGP como principal ferramenta para o rastreamento. Foi proposta uma extensão para o protocolo com a criação de duas novas mensagens: *traceback request*, que é enviada aos roteadores vizinhos quando é detectado um ataque e se deseja identificar o caminho, e *traceback reply*, usada pelos roteadores vizinhos como resposta a *traceback request*, contendo os endereços IPs dos roteadores que fazem parte do caminho de ataque. A mensagem *traceback request* possui dois parâmetros importantes para serem configurados: distância máxima de roteadores que a mensagem será enviada e o tempo que os roteadores vão permanecer monitorando o tráfego.

O sistema utiliza a marcação probabilistica de pacotes de forma diferente da tradicional

[6]Número identificador de um Sistema Autônomo. Possui 16 bits de tamanho e é atribuído pela IANA (*Internet Assigned Numbers Autority*).

pois antes do pacote ser escolhido verifica-se o endereço de destino. Além disso, o pacote não é marcado de fato, o que ocorre é a criação de uma mensagem BGP do tipo *traceback request*, que permite que o pacote original siga o seu caminho sem ser modificado. Este tipo de marcaçâo pode ser vista como uma vantagem uma vez que além de não modificar o pacote original, ainda aumenta a quantidade de pacotes úteis a serem analisados, com sua marcação baseada no endereço IP da vítima.

A estrutura de funcionamento básica do BGP Traceback pode ser visualizada na FIG. 3.3, onde é identificado um ataque contra uma vítima que está dentro do SA1. Neste caso, o administrador da rede, que possui acesso ao roteador de borda dentro de seu SA, inicia o processo de rastreamento enviando um pacote *traceback request* de distância 2 para os SAs adjacentes (passo (1)), solicitando que sempre que forem encontrados pacotes com o endereço da vítima como destino, os roteadores enviem uma mensagem *traceback reply*. Este processo, uma vez carregado ocorre de forma automática entre os roteadores dos SAs. SA2 e SA3 colocam o endereço da vítima em uma lista local que guarda todos os endereços a serem rastreados e repassam a mensagem *traceback request* para seus vizinhos, no caso SA4 e SA5, que também colocam o endereço da vítima lista local. A mensagem *traceback request* é repassada até que a distância configurada chegue a 0. Após este processo, todos os SAs que receberam o *traceback request* gerado pelo SA1, estão prontos a enviarem mensagens *traceback reply* sempre que encontrarem pacotes que se destinam a vítima.

Para ilustrar a reconstrução do caminho, imagina-se que os pacotes destinados a vítima comecem a passar pelo SA5. Este vai verificar na sua tabela local que existe um pedido de identificação de rota do tráfego com destino ao endereço IP da vítima e vai escolher com uma probabilidade p se vai enviar a mensagem *traceback reply*. Se sim, ele criará um pacote BGP com a mensagem, acrescentará seu endereço e enviará ao seu próximo salto no caminho até o destino (passo (3)). Este processo ocorre até a mensagem chegar ao SA1 (passo (4)), que verifica que ela foi em resposta a uma mensagem *traceback request* gerada por ele. O BGP vai concluir que o pacote BGP *traceback request* chegou ao destino, enviando ao administrador da rede o resultado SA5-SA2-SA1, finalizando o rastreamento (passo (5)).

As dificuldades neste sistema estão relacionadas ao tempo que os roteadores vão per-

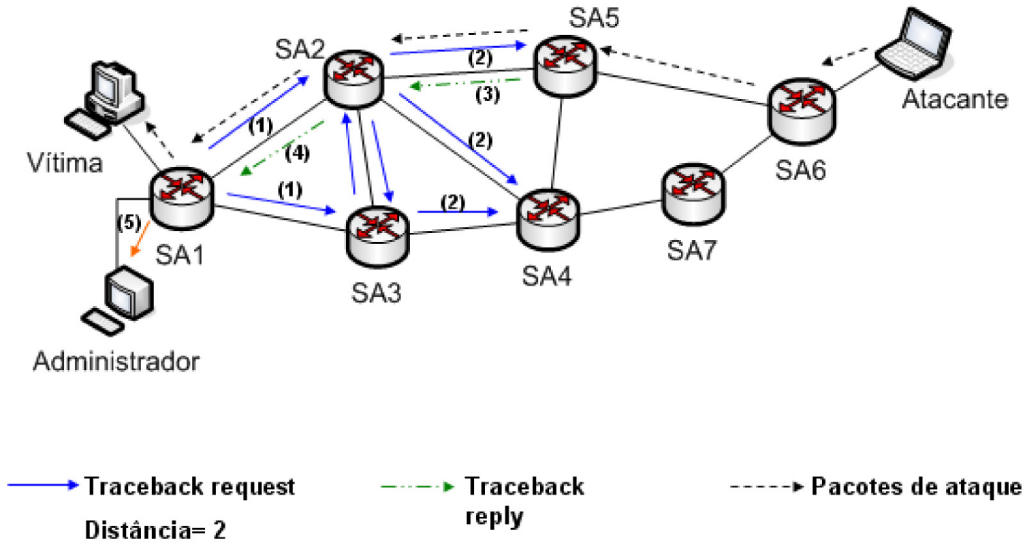

FIG. 3.3: Sistema de Martins e Moraes (MARTINS, 2006).

manecer monitorando o tráfego, uma vez que um tempo muito grande gera uma sobrecarga grande na rede e um tempo muito baixo resulta em pouca chance de encontrar o atacante e na forma de verificação de falsos positivos no rastreamento, que gera um processo muito trabalhoso para o administrador da rede, que deve verificar na vítima as conexões que completaram o *three-way handshake*, armazenar estes endereços de origem e executar um *traceroute* nos mesmos, comparando o resultado com o caminho gerado pelo BGP Traceback. Com este resultado, verificar os caminhos que coincidem, excluindo-os dos possíveis caminhos de ataque e deixando os caminhos restantes identificados pelo BGP Traceback como possíveis caminhos de ataque.

3.2.2 SISTEMA SPIE EM UM CENÁRIO DE INSTALAÇÃO PARCIAL

Foram propostas duas abordagens para este trabalho. Na versão inicial, Korkmaz et al. (KORKMAZ, 2005) propuseram um esquema para rastreamento de um único pacote IP no nível de SAs em um cenário de instalação parcial, onde utilizaram o sistema SPIE (SNOEREN, 2002) como o sistema de rastreamento dos SAs. A proposta é que os STMs fossem capazes de fazer consultas nível-a-nível em SAs para descobrir se o SA

possui o SPIE instalado e consequentemente buscar a origem dos pacotes de ataque.

O funcionamento básico do sistema é ilustrado na FIG. 3.4. Os SAs com uma bandeira possuem o SPIE instalado. Inicialmente, a vítima detecta um ataque e a partir do SA5 começa o processo do rastreamento dos pacotes enviando consultas aos SAs adjacentes de nível 1, neste caso SA4 e SA1 (passo (1)). Como SA1 não possui o SPIE instalado, ele não responde a consulta feita por SA5. Por outro lado, o SA4 responde com uma resposta negativa de que o pacote não passou por ele. SA5 então envia consultas para seus SAs vizinhos de nível 2, neste caso SA2 e SA3 (passo (2)). Então, SA2 envia para SA5 uma resposta positiva de que o pacote passou por ele. Esta resposta inclui os vizinhos de SA2 em até 2 níveis (SA3, SA8, SA9, SA4 e SA5). Contudo, como SA5 já sabe que o pacote passou pelo SA2, além de já ter recebido uma resposta negativa de SA3, SA5 envia uma consulta para SA8 (passo (3)), que depois de descobrir que a origem do pacote está dentro da sua rede, retorna uma mensagem positiva para SA5, finalizando o processo de rastreamento.

Nesta proposta não foi detalhado como os STMs (*SPIE Traceback Manager*) dos SAs vão se comunicar entre si de forma que possam trocar dados sobre o rastreamento dos pacotes.

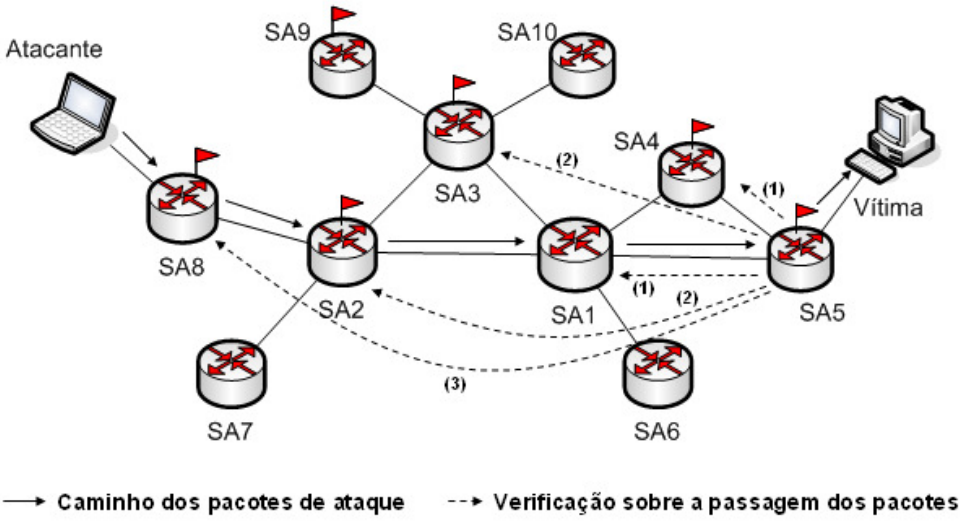

FIG. 3.4: Sistema de Korkmaz et al. (KORKMAZ, 2005).

A FIG. 3.5 mostra uma avaliação do sistema onde foi verificada a taxa de sucesso no rastreamento dependendo da quantidade de SAs com o sistema de rastreamento instalado. A topologia da simulação é composta por 3040 SAs e foi gerada pelo INET (INTERNET TOPOLOGY GENERATOR, 2002), um gerador de topologias da Internet no nível de SA. O rastreamento foi analisado considerando-se consultas entre SAs utilizando 1, 2, 4 e 8 níveis. Os melhores resultados foram encontrados para consultas em 4 e 8 níveis (os resultados foram praticamente iguais). Porém, a conclusão dos autores é que com uma taxa de instalação menor que 40% não existe grande chance de se detectar a origem dos ataques. Contudo, com uma taxa de instalação de pelo menos 70% consegue-se rastrear em média 50% dos atacantes.

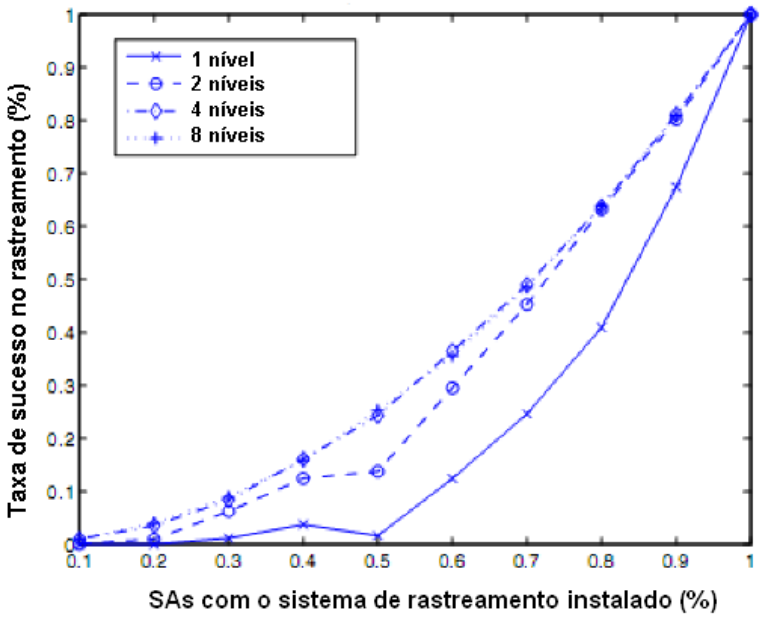

FIG. 3.5: Avaliação do Sistema do Korkmaz et al. (KORKMAZ, 2005).

Em uma segunda abordagem, Korkmaz et al. (KORKMAZ, 2007) propõem o sistema AS-SPT (*AS-level Single Packet Traceback*), também em um cenário de instalação parcial. Cada SA possui um ASTS (*Autonomous System Traceback Server*) responsável por monitorar os roteadores de borda do SA e armazenar os resumos dos pacotes. O ASTS também serve como ponto principal de contato para as requisições de rastreamento vindas de usuários locais ou remotos. A FIG. 3.6 mostra uma avaliação do sistema onde também

foi verificada a taxa de sucesso no rastreamento. A topologia da simulação é composta por 8998 SAs. A taxa de sucesso no rastreamento foi analisada considerando-se consultas entre SAs utilizando nenhum, 1, 2 e 3 saltos. O melhores resultados foram encontrados para consultas em 2 e 3 saltos.

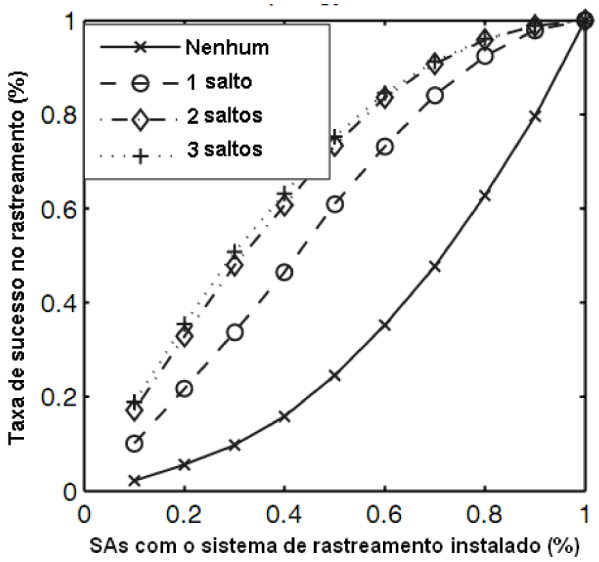

FIG. 3.6: Avaliação do Sistema do Korkmaz et al. (KORKMAZ, 2007).

Nesta abordagem, os autores basicamente definem a arquitetura do sistema sem propor um novo mecanismo de rastreamento para ser usado nos ASTSes, sugerindo novamente o SPIE (SNOEREN, 2002) como possível candidato dada sua popularidade.

Embora a arquitetura proposta permita instalação parcial do sistema, ela tem como necessidade o conhecimento prévio da topologia da rede para seu funcionamento. Além disso, ela apresenta algumas vulnerabilidades, já que o atacante pode usar um endereço IP forjado de forma a executar requisições de rastreamento nos ASTSes como se fosse um ASTS e os ASTSes podem ser atacados se tornando incapazes de executar o rastreamento. Para diminuir estes problemas, os autores propõem a utilização de um mecanismo qualquer existente contra ataques com endereços forjados, a utilização de um protocolo para a comunicação entre os ASTSes ou até mesmo uma forma dos ASTSes que estão realizando o rastreamento saltarem os ASTSes que estão sendo atacados. Vale ressaltar que a maneira como isso pode ser feito não foi determinada no trabalho.

4 O SISTEMA PROPOSTO

4.1 REDE SOBREPOSTA PARA RASTREAMENTO DE TRÁFEGO IP NO NÍVEL DE SISTEMAS AUTÔNOMOS

No sistema proposto neste trabalho, os pacotes que trafegam pela rede são marcados pelos roteadores de borda dos SAs à medida que passam por eles. A marcação dos pacotes é feita de forma similar ao sistema RAT (Rastreamento de ATaques), originalmente proposto por Laufer et al. (LAUFER, 2005b) e avaliado por Moreira et al. (MOREIRA, 2006). No RAT, o campo para o armazenamento da rota percorrida pelo pacote foi definido como uma nova `Opção` do protocolo IP (FIG. 4.1) (MOREIRA, 2006). O primeiro campo (Tipo) possui 1 octeto de tamanho e identifica as opções existentes no protocolo IP. A nova `Opção` tem o campo Tipo com o valor 0x99. O segundo campo (Tamanho), também com 1 octeto de tamanho, armazena o tamanho da `Opção`, incluindo os octetos dos campos Tipo, Tamanho e Dados. O terceiro campo, de tamanho variável, contém os Dados propriamente ditos, que no caso do sistema RAT e do sistema proposto neste trabalho são o FBG (LAUFER, 2005c). Vale lembrar que esta nova `Opção` deve estar presente em qualquer pacote que esteja trafegando pela rede, de forma que ele possa ser rastreado.

Para armazenar a rota, os dados inseridos no FBG de cada pacote carregam marcas dos roteadores por onde o pacote passou. Desta forma, quando o pacote chega ao destino, o FBG contém a rota do pacote. Na fase de rastreamento, o sistema aqui proposto utiliza o protocolo de roteamento BGP como veículo de comunicação entre os SAs que possuem o sistema de rastreamento instalado. Através desta comunicação, cada roteador de borda do SA participante do rastreamento preenche uma tabela, chamada tabela de *overlay*, que contém todos os SAs participantes do rastreamento que são conhecidos pelo SA dono da tabela. Essa estrutura permite que seja formada a rede sobreposta para rastreamento de tráfego IP e com sua utilização seja descoberto qual o próximo salto no caminho reverso ao utilizado pelos pacotes de ataque para alcançarem a vítima. Sendo assim, o sistema está

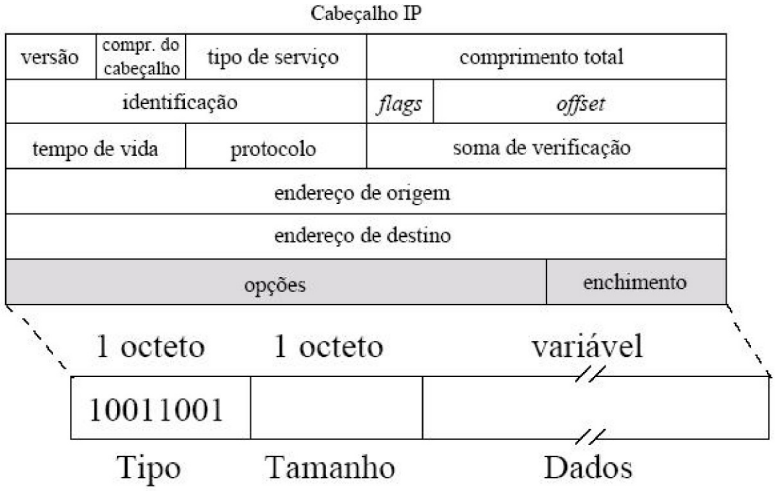

FIG. 4.1: Nova opção para o protocolo IP.

apto a operar em larga escala e no nível de SAs, eliminando a necessidade de ser instalado consecutivamente em todos os roteadores da rede. Em outras palavras, a instalação do sistema proposto pode ser realizada de forma *parcial* e *incremental* na Internet. Ao longo deste capítulo, apresentaremos os mecanismos pelos quais o sistema proposto: utiliza o protocolo BGP para suas finalidades, estabelece a rede sobreposta para rastreamento de tráfego IP no nível de SAs, marca os pacotes e realiza o rastreamento de tráfego.

4.2 FILTROS DE BLOOM

Nesta seção será explicado o funcionamento básico do Filtro de Bloom Original (FBO) (BLOOM, 1970) e do FBG (LAUFER, 2005c), que é o utilizado no sistema proposto, fazendo uma comparação entre eles.

4.2.1 FILTRO DE BLOOM ORIGINAL

O FBO pode ser considerado como uma estrutura de dados utilizada para representar de uma forma resumida um conjunto qualquer $S = \{s_1, s_2, s_3, ..., s_n\}$ de n elementos. O FBO é formado por um vetor de m *bits* e k funções de *hash* independentes h_1, h_2, h_3, ..., h_k cujas saídas variam uniformemente no espaço discreto {0, 1 , 2, 3,..., m -1}. Quando o vetor de *bits* é inicializado, todos os seus *bits* encontram-se zerados. Para todo

elemento $s_i \in S$ os *bits* do vetor correspondentes às posições $h_1(s_i)$, $h_2(s_i)$, $h_3(s_i)$,..., $h_k(s_i)$ são preenchidos com 1, sendo que os mesmos *bits* podem ser preenchidos várias vezes.

A FIG. 4.2 é um exemplo básico do funcionamento do FBO. O pacote atravessa o SA1, o SA3, o SA5 e o SA7 até alcançar a vítima e o FBO possui 10 bits de tamanho. Inicialmente, o FBO encontra-se com todos os bits zerados e a medida que o pacote atravessa os SAs, os bits referentes às posições de cada SA são preenchidos com 1, por exemplo, para o SA1 são preenchidos os bits 1 e 3 do FBO, para o SA3 os bits 6 e 7 e assim por diante.

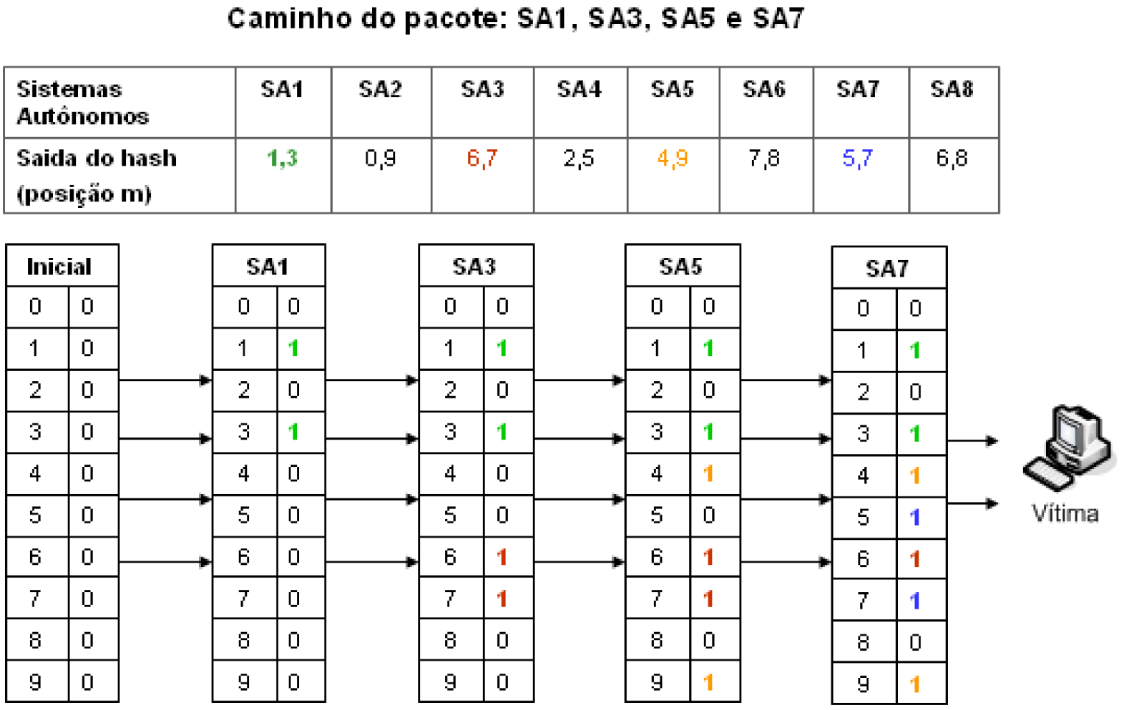

FIG. 4.2: Exemplo do preenchimento do Filtro de Bloom Original.

Considerando-se que o FBO representa um conjunto de elementos, pode-se realizar um teste para verificar se um elemento qualquer x pertence ou não ao conjunto S. A maneira pela qual esse teste é feito é através da verificação de se os *bits* do vetor nas posições $h_1(x)$, $h_2(x)$, $h_3(x)$,..., $h_k(x)$ estão preenchidos com 1. Se a resposta for positiva, então $x \in S$. De outra forma, se pelo menos um *bit* tiver o valor 0, então $x \notin S$. É claro que falsos positivos podem ocorrer, no caso de um elemento qualquer $x \notin S$ tenha todos os

bits correspondentes preenchidos com o valor 1.

4.2.2 FILTRO DE BLOOM GENERALIZADO

De forma semelhante ao FBO, o FBG é uma estrutura de dados utilizada para representar de uma forma resumida um conjunto qualquer $S = \{s_1, s_2, s_3, ..., s_n\}$ de n elementos. O FBG é formado por um vetor de m *bits* e $k_0 + k_1$ funções de *hash* independentes g_1, g_2, g_3, ..., g_{k0}, responsável por zerar os *bits* do vetor e h_1, h_2, h_3, ..., h_{k1}, responsável por preencher os *bits* do vetor com 1, cujas saídas variam uniformemente no espaço discreto {0, 1 , 2, 3,..., m -1}. O calculo do vetor de *bits* é feito da mesma forma que no FBO. Porém, diferentemente do FBO, na inicialização do vetor, não importa se os *bits* estão zerados ou preenchidos com 1. Desta forma, a interferência do atacante no preenchimento inicial do vetor não interfere no resultado final do preenchimento, conforme será abordado na próxima seção.

A FIG. 4.3 é um exemplo básico do funcionamento do FBG. Para alcançar a vítima, o pacote atravessa o SA1, o SA3, o SA5 e o SA7. A medida que o pacote atravessa os SAs, os bits referentes as posições de cada SA são preenchidos com 0 ou 1, dependendo da função de *hash*, por exemplo, para o SA1 o bit 1 do FBG é zerado e o bit 3 é preenchido com 1, para o SA5 o bit 4 do FBG é zerado e o bit 9 é preenchido com 1.

4.2.3 COMPARAÇÃO DOS FILTROS DE BLOOM

A principal diferença entre o FBO e o FBG é utilidade das funções de *hash*. Enquanto no FBO as funções de hash apenas preenchem bits, no FBG existem funções que zeram e funções que preenchem bits. Esta diferença influencia diretamente na taxa de falsos positivos e falsos negativos encontradas nos filtros. Quando ocorre um falso positivo nos Filtros de Bloom considerando sua utilização nos sistemas de rastreamento, isto indica que um roteador por onde o pacote não passou foi reconhecido como integrante do caminho de ataque. Por outro lado, quando ocorre um falso negativo, um roteador por onde o pacote passou não é reconhecido como parte do caminho de ataque.

Como no FBO os bits encontram-se inicialmente zerados e são preenchidos conforme o pacote atravessa os roteadores, a taxa de falsos positivos pode chegar a 100%, uma vez

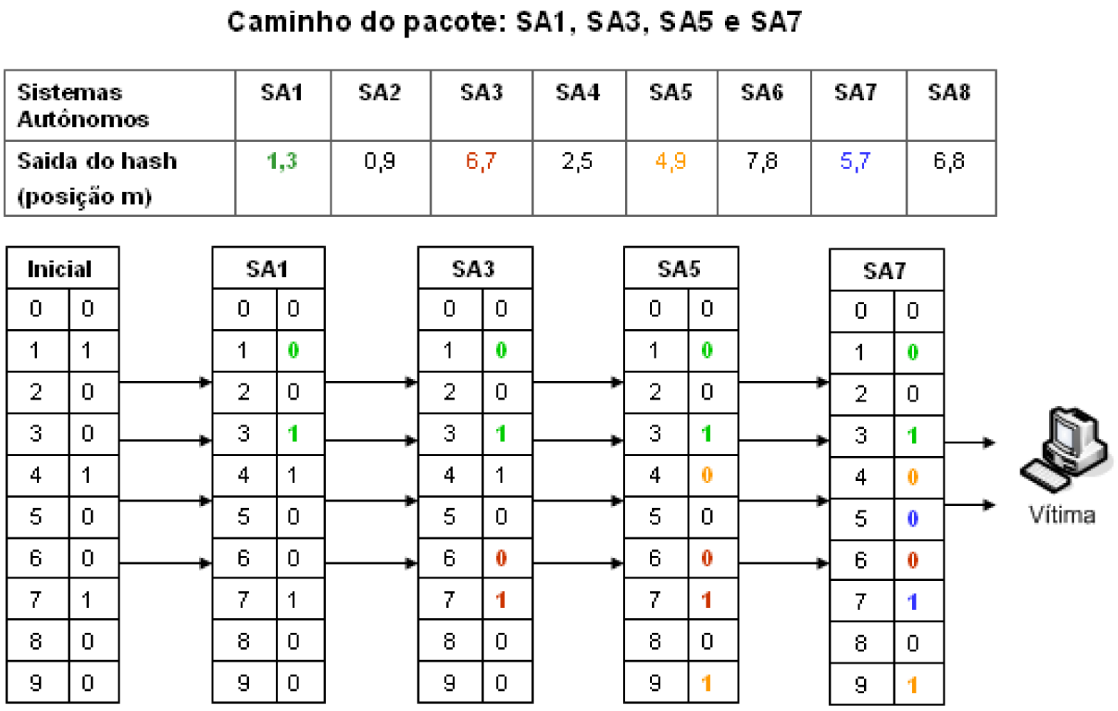

FIG. 4.3: Exemplo do preenchimento do Filtro de Bloom Generalizado.

que o atacante tem o controle sobre o conteúdo inicial dos pacotes, podendo enviá-los com todos os bits do FBO preenchidos. Quando isto ocorre, no momento da reconstrução do caminho reverso dos pacotes de ataque, roteadores que não fazem parte deste caminho podem ser reconhecidos como tal. Por outro lado, a taxa de falsos negativos é sempre zero, já que um roteador sempre marca um pacote que o atravessa.

A utilização de funções de *hash* que zeram e preenchem os bits existentes no FBG tornam o resultado final independente da sua condição inicial. Em outras palavras, mesmo que um atacante preencha todos os bits do FBG, estes bits podem ser sobrescritos com zero ao serem submetidos a função que possui esta finalidade e neste caso a taxa de falsos positivos é reduzida de 100% do FBO para no pior caso 25% no FBG (LAUFER, 2005b). Por outro lado, esta independência da condição inicial do FBG introduz uma certa probabilidade de falsos negativos. Isto ocorre porque quanto mais roteadores inserem suas marcas no FBG, maior é a possibilidade destes roteadores sobreescreverem os bits preenchidos ou zerados por outros roteadores. Em (LAUFER, 2005b) é mostrado que

com um FBG de 256 bits em uma rota de 15 saltos, 7 roteadores foram rastreados, ou seja, em média 8 roteadores tiveram suas marcas sobrescritas. É claro que se estes números forem trazidos para a proposta deste trabalho, onde o rastreamento é feito no nível de SAs, onde o menor caminho médio entre dois SAs é 4,19 com ± 0.14 (ALVES, 2007), um FBG com 256 bits é mais do que o suficiente para que todos os SAs integrantes da rota de ataque sejam descobertos. Isto sem levar em consideração que no sistema proposto neste trabalho cada SA insere uma marca a partir de um valor de 16 bits, o seu ASN (conforme será mostrado na Seção 4.6), enquanto no sistema RAT a marca é gerada a partir do endereço IP do roteador, ou seja 32 bits. Portanto, a quantidade de informação a ser armazenada no FBO é menor no sistema proposto e com isso a quantidade de falsos negativos também.

Uma análise detalhada das probabilidades de falsos negativos e falsos positivos e suas implicações no FBG podem ser encontradas em (LAUFER, 2005c). O artigo mostra que elas estão diretamente relacionadas com a quantidade de funções de *hash* utilizadas e com o tamanho do FBG. Na Seção 4.7 serão feitas algumas considerações a respeito de falsos positivos e negativos no sistema proposto.

4.3 O PROTOCOLO BGP

O BGP (REKHTER, 1995) é o protocolo de roteamento utilizado na internet para a troca de informações de roteamento entre os SAs. Um SA pode ser classificado como um conjunto de roteadores subordinados a uma mesma entidade administrativa, respeitando uma política comum de roteamento. Externamente, um SA pode ser visto como um único domínio de roteamento. Através do BGP, os roteadores de borda dos SAs trocam informações sobre rotas para determinar o caminho fim-a-fim entre os pacotes até alcançarem o destino. Em outras palavras, através do uso do BGP, os dados são encaminhados desde o SA de origem até o SA de destino, onde posteriormente serão encaminhados utilizando outros protocolos intra-domínios até chegarem ao *host* de destino.

O BGP utiliza o TCP como protocolo de transporte confiável, o que elimina a necessidade do BGP tratar de retransmissões. Os roteadores que usam o BGP são chamados BGP *speakers*. Dois BGP *speakers* que participam de uma sessão BGP são chamados

peers ou *neighbors* BGP e se comunicam através da porta 179 do TCP. Os *peers* BGP trocam quatro tipo de mensagens:

- *Open*: esta mensagem é enviada para que seja aberta uma sessão BGP entre *peers*;
- *Notification*: é enviada para relatar erros ocorridos durante ou após o estabelecimento de uma sessão BGP;
- *Keepalive*: estas mensagens são enviadas para manter a comunicação entre os *peers* BGP ativa caso não sejam feitas atualizações através de mensagens `update`;
- *Update*: são utilizadas para as trocas de rotas entre os peers BGP, desde novas rotas que devem ser incluídas até rotas antigas que devem ser removidas.

Neste trabalho é dada uma atenção especial a mensagem do tipo `Update`, que é utilizada para carregar informações sobre qual SA possui o sistema de rastreamento proposto instalado, como será mostrado mais adiante.

4.3.1 A MENSAGEM UPDATE

Conforme citado anteriormente, as mensagens do tipo `Update` são trocadas entre os *peers* BGP levando informações sobre atualizações nas suas tabelas de rotas. O formato da mensagem `Update` pode ser visto na FIG. 4.4.

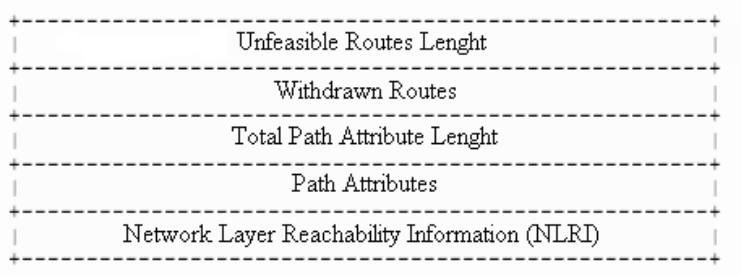

FIG. 4.4: Formato da mensagem Update.

- *Unfeasible Routes Lenght*: este campo tem 2 octetos de tamanho e indica o comprimento total dos prefixos de endereços IP que devem ser removidos. Se o comprimento for igual a 0, nenhuma rota deve ser removida nesta mensagem `update`;

- *Withdrawn Routes*: é um campo de tamanho variável que contém a lista de prefixos de endereços IP que devem ser removidos da tabela de rotas;
- *Total Path Attribute Lenght*: indica o tamanho total do campo *Path Attributes*;
- *Path Attributes*: é um campo de tamanho variável que representa uma coleção de atributos associados a uma determinada rota e que pode influenciar no processo de seleção de rotas. Existem vários tipos de *Path Attributes*, tais como: Origin, AS_path, Next_hop, Multi_exit_disc, Local_pref, etc. Todos eles foram definidos na RFC 1771(REKHTER, 1995). O *Path Attribute* mais importante para o desenvolvimento do sistema de rastreamento IP no nível de SAs proposto neste trabalho é o *Communities Attribute*, definido na RFC 1997 (CHANDRA, 1996), que será explicado mais adiante neste capítulo.
- *Network Layer Reachability Information (NLRI)*: é um campo de tamanho variável que contém informações sobre as rotas que podem ser alcançadas.

4.3.2 O PATH ATTRIBUTE

Conforme citado anteriormente, este atributo representa uma coleção de atributos associados a uma determinada rota e que pode influenciar no processo de seleção de rotas. Eles estão classificados em 2 grupos e 4 categorias:

- Grupo *Well-known*:
  - *Mandatory* (conhecido obrigatório);
  - *Discretionary* (conhecido arbitrário);
- Grupo *Optional*:
  - *Transitive* (opcional transitivo);
  - *Non-transitive* (opcional não transitivo).

Os atributos *Well-known* devem ser reconhecidos e estar presentes em *todas* as implementações do BGP. Quando são do tipo *Mandatory* devem estar incluídos em todas as

mensagens do tipo `Update`. Caso contrário, uma mensagem do tipo *Notification* é enviada com o código do erro referente a *Missing well-known attribute*. Já os atributos do tipo *Discretionary* podem ou não ser enviados em uma mensagem `Update` específica.

Os atributos do tipo *Optional* não precisam ter suporte de todas as implementações do BGP. Isso significa que se a implementação do BGP operando no roteador de um SA não reconhece um atributo *Optional* presente na mensagem `Update` recebida, uma verificação se o *flag Transitive* está ativado ou não para este atributo é feita. Em caso positivo, o atributo é repassado nas mensagens `Update` seguintes enviadas pelo roteador do SA para seus *peers*. Caso contrário, este atributo é ignorado, não sendo repassado para os *peers* BGP em uma nova mensagem `Update`.

4.3.3 O COMMUNITIES ATTRIBUTE

O *Communities Attribute* definido na RFC 1997 (CHANDRA, 1996), é um *Path Attribute* usado por um grupo de SAs que possuem características comuns. Esse atributo mostra-se bastante versátil (QUOITIN, 2002; AGARWAL, 2004; BONAVENTURE, 2003) e pode ser utilizado com diferentes propósitos, tais como roteamento *multi-home* (CHEN, 1996), engenharia de tráfego (HUSTON, 2004), suporte para VPNs (ROSEN, 2006), sistemas de *honeypot* móveis (KRISHNAMURTHY, 2004), bloqueio de ataques DoS (TURK, 2004) e coleta de dados do BGP (MEYER, 2006).

Por definição da RFC 1997, o *Communities Attribute* é representado por um conjunto de valores de 4 octetos, cada um representando uma *Community*. O atributo é um *Path Attribute* de *Type Code* igual a 8 e possui uma faixa de valores entre 0x00000000 até 0xFFFFFFFF, onde os valores de 0xFFFF0000 e 0xFFFFFFFF são reservados. O ASN fica codificado nos 2 primeiros octetos e os 2 octetos finais são definidos de acordo com o SA que está propondo ou usando a *Community*. Por exemplo, se o SA 690 está propondo uma *Community*, então: SA 690_{16} = 02B2, logo possui uma faixa de valores de 0X02B20000 até 0x02B2FFFF.

Em sua operação, um BGP *speaker* pode usar o *Communities Attribute* para controlar quais informações de roteamento vai aceitar, dar preferência ou distribuir para outros vizinhos. Pode ainda, ao receber uma rota sem este atributo, inserí-lo no momento de

propagar uma rota para seus *peers* ou modificá-lo de uma rota recebida de acordo com a política local.

4.4 USO DO BGP COMO VEÍCULO DE COMUNICAÇÃO DO SISTEMA PROPOSTO

Para o sistema de rastreamento de tráfego IP proposto neste trabalho, é criado um novo *Community Attribute* chamado `IP Traceback Community` que contém informações sobre a presença do sistema nos SAs, indicando que estes estão aptos a formar a rede sobreposta e realizar o rastreamento do tráfego no nível de SAs. Uma característica importante sobre o *Community Attribute* refere-se a ele ser um atributo BGP *optional transitive*. Essa característica permite que a informação sobre o `IP Traceback Community` seja repassada de forma transparente pelos SAs que não possuam o sistema de rastreamento instalado para seus *peers*. Ao final de uma seqüência de mensagens `Update`, a rede sobreposta de rastreamento, incluindo todos os SAs que possuem o sistema proposto instalado, é estabelecida ou atualizada. Nesse ponto, cada SA com o sistema instalado contém uma tabela, chamada tabela de *overlay*, com a lista de todos os SAs com o sistema instalado que são conhecidos pelo SA dono da tabela, ou seja, os seus vizinhos na rede sobreposta de rastreamento de tráfego IP no nível de SAs. O funcionamento deste mecanismo será detalhado na próxima Seção.

4.5 CRIAÇÃO DA REDE SOBREPOSTA PARA RASTREAMENTO DE TRÁFEGO IP

A rede sobreposta permite que o rastreamento de tráfego seja realizado entre os roteadores participantes da rede sobreposta (não necessariamente contíguos no nível de roteamento) por onde o pacote passou. O rastreamento é portanto realizado salto a salto na rede sobreposta no nível dos SAs. Isso elimina a necessidade, comum em muitas propostas anteriores, do sistema de rastreamento ser instalado em todos os roteadores das redes monitoradas.

Para a criação da rede sobreposta, cada SA participante do rastreamento preenche sua

tabela de *overlay* com informações sobre SAs conhecidos que estão habilitados a realizar o rastreamento. Esta tabela tem como objetivo relacionar quais SAs devem ser verificados no momento da reconstrução da rota dos pacotes. Um ponto que deve ser levado em consideração é o espaço que deve ser utilizado pelos roteadores dos SAs para armazenar a tabela de *overlay*. Devido aos dados obtidos recentemente em Alves et al. (ALVES, 2005), onde foi mostrado que o número médio de vizinhos que um SA possui é 3,54 para a Internet Brasileira e 3,37 para a Internet Mundial, sendo que apenas 14,6% e 7% dos SAs tem número maior de vizinhos que a média no primeiro e segundo caso respectivamente e que o dado armazenado na tabela de *overlay* é o ASN de cada vizinho na rede sobreposta, a tendência é que o espaço utilizado pelos roteadores para o armazenamento da tabela de *overlay* seja relativamente pequeno.

Um exemplo da criação de uma rede sobreposta pode ser visto na topologia da FIG. 4.5. Os SAs marcados com uma bandeira possuem o sistema de rastreamento instalado. Inicialmente, suas tabelas de *overlay* estão vazias. Quando SA1 envia uma mensagem `Update` para seus *peers* (passo (1)), SA3 insere na sua tabela de *overlay* o SA1 como seu vizinho. Por outro lado, como SA2 não possui o sistema instalado, ele simplesmente faz a atualização na sua tabela de rotas com as informações recebidas do SA1 na mensagem `Update` e, ao gerar uma nova mensagem `Update`, repassa de forma transparente a informação recebida anteriormente sobre o `IP Traceback Community` para seus *peers* SA4 e SA3 (passo (2)) por esta ser uma informação assinalada como transitiva na mensagem `Update` recebida. SA3 recebe a mensagem `Update` vinda de SA2 e simplesmente atualiza sua tabela de *overlay* que já possuia a informação sobre SA1. Por sua vez, SA4 insere SA1 como seu vizinho em sua tabela de *overlay*. Ao criarem uma nova mensagem `Update`, SA3 e SA4 inserem seus dados sobre a `IP Traceback Community` e enviam a mensagem para seus vizinhos (passos (3) e (4) respectivamente). Após o recebimento da mensagem `Update` de SA3, SA4 o insere como vizinho na tabela de *overlay*. O mesmo procedimento é feito por SA3 após receber a mensagem `Update` de SA4. Esse processo se repete por todos os SAs da rede.

Vale relembrar que as informações sobre a `IP Traceback Community` não geram nenhuma sobrecarga adicional na rede devido as trocas de mensagens, pois as informações

são carregadas dentro das mensagens `Update` do BGP são trocadas periodicamente entre os *peers*.

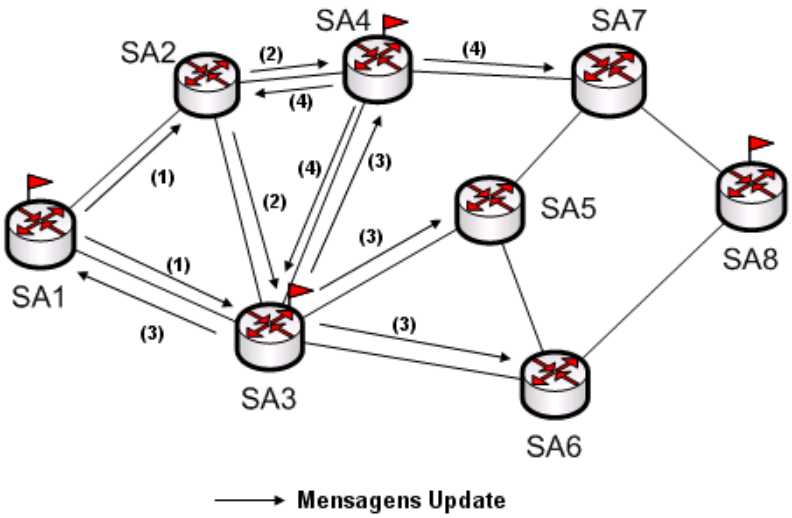

FIG. 4.5: Troca de mensagens Update do BGP.

Uma observação importante que deve ser ressaltada é que quando o SA possui o sistema instalado ele armazena na tabela de *overlay* a informação sobre qual SA gerou os dados sobre o `IP Traceback Community` e, ao enviar uma nova mensagem `Update`, ele sobreescreve esta informação com seus próprios dados, conforme nos exemplos do SA3 (passo (3)) e do SA4 (passo (4)). Entretanto, como ocorrido no exemplo do SA2, quando um SA não possui o sistema instalado, ele repassa a informação transitiva recebida sobre o `IP Traceback Community` de forma transparente em uma nova mensagem `Update` para seus *peers* (passo (2)). Ao final das trocas das mensagens `Update`, cada SA com o sistema proposto instalado possui na sua tabela de *overlay* seus vizinhos na rede sobreposta recém atualizada. A TAB. 4.1 é um exemplo das tabelas de *overlay* para a topologia utilizada. Cada coluna representa a tabela de *overlay* individual de cada SA que possui o sistema proposto instalado. Por exemplo, o SA1 tem como vizinhos na rede sobreposta o SA3 e o SA4.

A rede sobreposta resultante é ilustrada na FIG. 4.6, onde as linhas de maior espessura representam suas conexões.

TAB. 4.1: Tabela de overlay dos SAs.

	Sistemas Autônomos			
	SA1	**SA3**	**SA4**	**SA8**
Vizinhos	SA3	SA1	SA1	SA3
	SA4	SA4	SA3	SA4
		SA8	SA8	

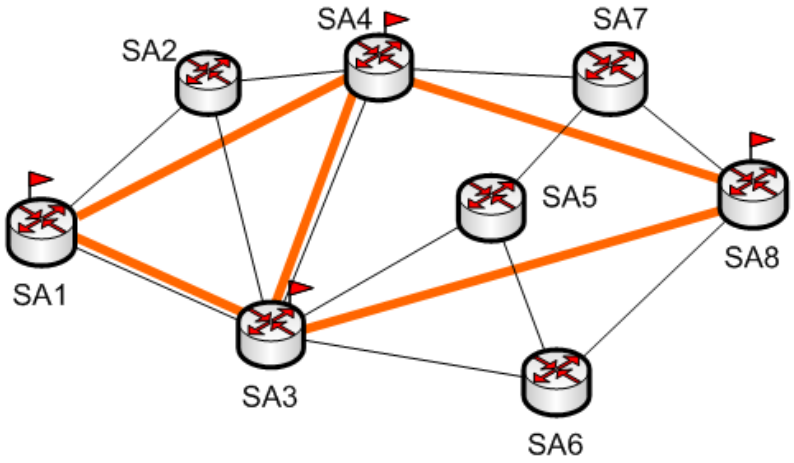

FIG. 4.6: Rede sobreposta resultante da troca de mensagens Update do BGP.

4.6 PROCESSO DE MARCAÇÃO DE PACOTES

O processo de marcação de pacotes proposto originalmente por Laufer et al. (LAUFER, 2005b) foi modificado para operar de acordo com o sistema proposto neste trabalho. No processo original, quando um pacote passa pelo roteador, este insere uma marca no FBG de forma que o pacote chegue ao destino com as marcas de todos os roteadores por onde passou. Porém, quando um roteador está fazendo o processo de reconstrução do caminho do ataque, ele pode encontrar a marca de mais de um de seus roteadores vizinhos no FBG. Este problema pode ser observado na FIG. 4.7 – as setas indicam o caminho do ataque – onde o roteador RT1 verifica que existem as marcas dos roteadores RT2 e RT3,

ambos seus vizinhos, no FBG, pois ambos participaram da rota tomada pelos pacotes de ataque. Note que, nesse caso, RT1 não possui um critério claro para decidir se o próximo roteador no caminho reverso de ataque é o seu vizinho RT2 ou RT3. Logo, se o roteador RT1 enviar o pacote de reconstrução de rota para RT2, o rastreamento tende a ser concluído sem problemas. Entretanto, se o pacote de reconstrução de rota é enviado para RT3, o problema volta a ocorrer, pois RT3 encontrará as marcas de RT2 e RT5. No caso de RT3 enviar o pacote de reconstrução de rota para RT2, o rastreamento pode terminar inesperadamente ou gerar mensagens repetidas desnecessárias na rede.

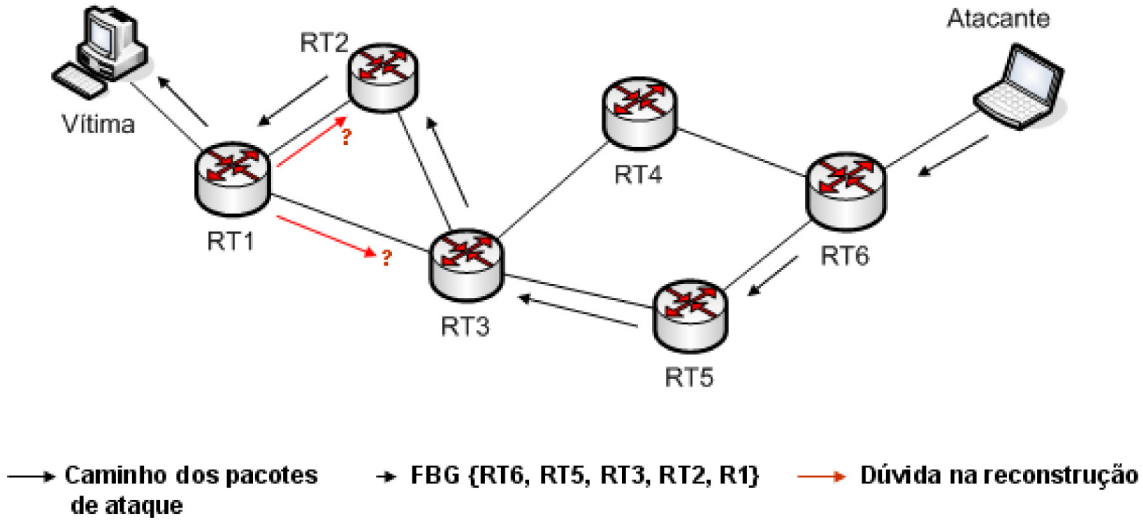

FIG. 4.7: Problema de identificação de duas marcas no FBG.

No sistema proposto neste trabalho, para se evitar problemas como este, antes do FBG ser preenchido com a marca de um roteador, é proposta uma marcação da seqüência dos roteadores dos SAs. Esta marcação é feita da seguinte forma: ao receber um pacote, o roteador do SA que possui o sistema de rastreamento instalado realiza uma operação lógica XOR entre número identificador do SA – que tem 16 bits de tamanho – e um valor de 16 bits formado pelo TTL do pacote naquele momento (8 bits de tamanho) mapeado nos 8 bits mais significativos deste valor e completado de bits de valor 1 nos 8 bits menos significativos. Após este processo, é feita a marcação do pacote propriamente dita, onde

o resultado da operação XOR é submetido à função *hash*, gerando a marca a ser feita no FBG. Esse processo é realizado em todos os SAs que possuem o sistema instalado. Assim quando o pacote chega ao destino, ele possui a marca de todos os SAs que possuem o sistema proposto por onde o pacote passou. Essa marcação elimina a incerteza no momento da reconstrução do caminho reverso dos pacotes de ataque conforme ilustrado na Seção 4.7 ao descrevermos o processo de rastreamento de tráfego na rede sobreposta.

4.7 PROCESSO DE RASTREAMENTO DE TRÁFEGO

O administrador de um SA que possui o sistema proposto instalado que deseja realizar o rastreamento deve iniciar o processo buscando no FBG as marcas dos SAs por onde o pacote passou. Para fazer esta busca, o roteador de borda do SA por onde o processo é iniciado faz o procedimento inverso da marcação de pacotes. A medida que as marcas do FBG são descobertas e o caminho reverso é delineado, o SA que está efetuando o rastreamento naquele momento envia um pacote de reconstrução de rota para o SA que teve sua marca encontrada nos pacotes de ataque. Este pacote de reconstrução contém uma lista de SAs por onde passou, sendo iniciada pelo SA que gerou o pedido de rastreamento, o TTL do pacote de ataque no momento que chegou à vítima e o FBG do pacote de ataque.

O processo de rastreamento é ilustrado na FIG. 4.8. As setas indicam o caminho do ataque e a numeração indica o TTL do pacote IP naquele momento. O sistema autônomo da vítima (SA8) inicia o rastreamento do ataque. Primeiramente, o roteador de borda do SA8 verifica sua tabela de *overlay* (Tabela 4.1) e assim constata que deve buscar no FBG pelas marcas de SA3 ou SA4, seus vizinhos na rede sobreposta (FIG. 4.6). Então, é realizada uma operação XOR entre um valor constituído pelo número identificador do SA3 com TTL do pacote no SA8 (251) acrescido de 1 (252) mapeado nos 8 bits mais significativos deste valor, completado de bits de valor 1 nos 8 bits menos significativos. Após este processo, é feito o *hash* deste resultado e verificado que a marca do SA3 não está presente no FBG. O mesmo processo é feito com o número identificador do SA4. Como a resposta é negativa para ambos, o mesmo procedimento é novamente realizado incrementando-se de 1 o TTL (253). Nesta nova realização do procedimento, a marca é positiva para SA4. Portanto, SA8 envia um pacote de reconstrução de rota

para SA4 (passo (1)), que por sua vez incrementa o TTL (254) e faz o mesmo processo, buscando pelas marcas de SA1 e SA3, sendo esta positiva para SA3 (passo (2)). O mesmo processo é repetido no SA3 e termina quando o pacote de reconstrução de rota chega ao SA1 (passo (3)) – neste caso, a origem do ataque está além do SA1. Vale lembrar que o processo de rastreamento pode ser terminado de duas formas: quando o TTL chega a 256 ou quando um SA não consegue encontrar a marca de nenhum outro vizinho no FBG.

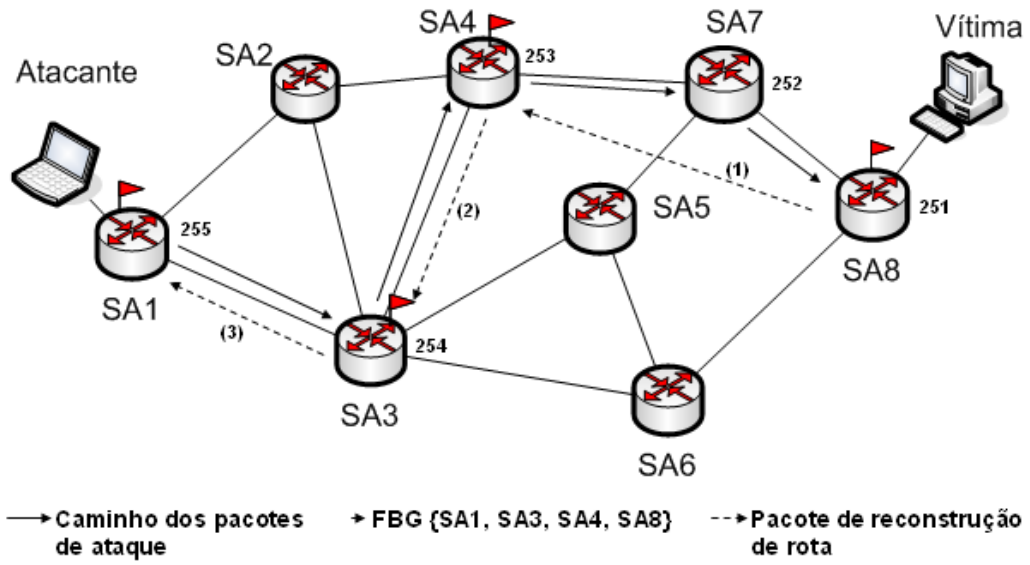

FIG. 4.8: Funcionamento do processo de rastreamento.

Utilizando o exemplo do ocorrido com SA8 e posteriormente com SA4, pode-se perceber que mesmo o pacote tendo passado por dois SAs vizinhos da rede sobreposta em relação ao SA atual no momento em que está buscando pelas marcas no FBG, o problema de indecisão sobre o encaminhamento a ser dado ao pacote de reconstrução não ocorre no sistema proposto, pois o TTL também armazenado no FBG auxilia a indicação da seqüência de roteadores pelos quais os pacotes de ataque passaram. Em outras palavras, com a utilização da marcação de sequência dos roteadores, o valor encontrado antes de ser submetido ao *hash* que posteriormente gera as marcações no FBG é sempre único, fazendo com que 2 ou mais SAs não possam ter o mesmo resultado.

Ao final do processo de rastreamento, os administradores dos SAs pertencentes à

rede sobreposta que fazem parte da rota de ataque estão cientes disso, inclusive o SA mais próximo da origem dos pacotes de ataque. Os SAs com o sistema de rastreamento instalado que se encontram mais próximos da origem dos ataques podem então iniciar procedimentos de filtragem para conter o ataque o mais próximo possível de sua origem, evitando assim, além do ataque em si, também o consumo de recursos de rede para o encaminhamento dos pacotes até a vítima. A técnica de filtragem a ser adotada para bloquear o ataque em curso está fora do escopo deste trabalho em particular, que é focado na etapa de rastreamento de tráfego. Porém, na Seção 2.6 foram mostradas algumas dessas técnicas.

Para verificar algumas implicações de falsos positivos, considera-se o cenário da FIG. 4.9, onde os pacotes de ataque atravessaram os SAs 1, 3, 6 até alcançarem o destino no SA8. Neste caso, ocorreu um falso positivo e o FBG contém, a marca do SA4. O processo de rastreamento é o mesmo exemplificado anteriormente, porém o SA8, devido a ocorrência de falso positivo para o SA4, deixa de enviar o pacote de reconstrução de rota para SA3 (passo(1)), que na verdade é o próximo roteador na rede sobreposta no caminho reverso dos pacotes de ataque, e o envia para SA4. Contudo, SA4 acaba enviando o pacote de reconstrução de rota para SA3 (passo(2)), pois SA3 é vizinho de SA4 na mesma rede sobreposta. Com isso, o rastreamento tende a ser realizado sem problemas, com SA1 recebendo o pacote de reconstrução de rota de SA3 (passo(3)) e sendo identificado como o SA de onde partiram os pacotes de ataque.

A mesma verificação pode ser feita na FIG. 4.10 para falsos negativos, em que os pacotes atravessam os SAs 1, 3, 4 e 7 até alcançarem o destino no SA8. Neste exemplo, ocorreu um falso negativo e o FBG não contém a marca do SA4. Porém, como SA8 é vizinho de SA3 na rede sobreposta, SA3 recebe o pacote de reconstrução de rota de SA8 (passo(1)). Deste modo, mais uma vez o rastreamento tende a ser realizado com sucesso mesmo com um dos SAs que fazem parte da rota de ataque não sendo identificado, pois SA1 consegue receber o pacote de reconstrução de rota de SA3 (passo(2)).

Estes dois exemplos mostram que mesmo com a ocorrência de falsos positivos e negativos no FBG, não significa que o sistema de rastreamento proposto não seja capaz de efetuar o rastreamento atingindo seu objetivo principal de encontrar as fontes dos

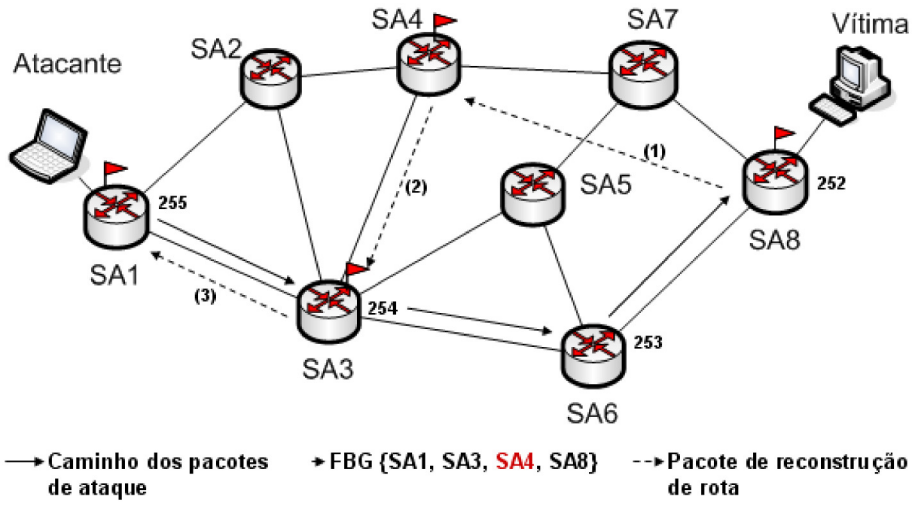

FIG. 4.9: Exemplo de ocorrência de falso positivo no processo de rastreamento.

pacotes de ataque. É claro ainda podem ocorrer situações que falsos positivos ou negativos implicariam em não se encontrar a origem do ataque. Porém, mesmo nesses casos o rastreamento pode sinalizar parte do caminho desses pacotes, permitindo que eles sejam filtrados de forma distribuída diminuindo o impacto do ataque.

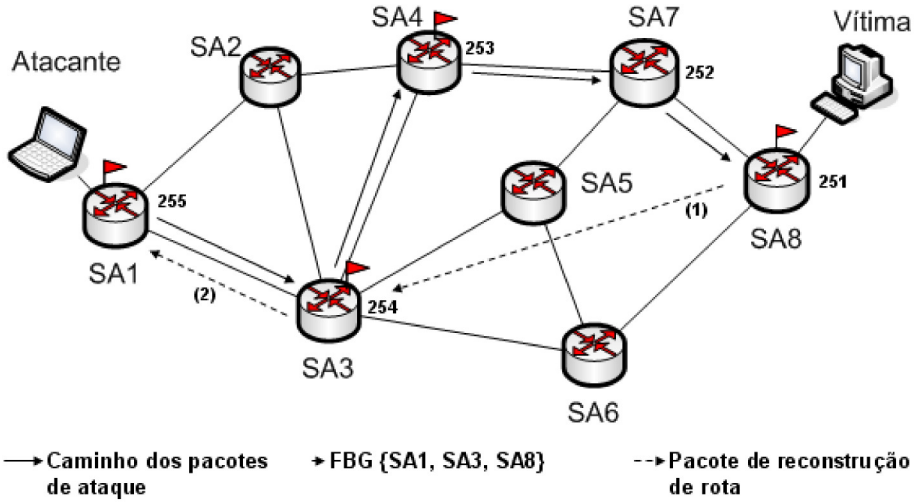

FIG. 4.10: Exemplo de ocorrência de falso negativo no processo de rastreamento.

5 AVALIAÇÃO DO SISTEMA

Neste capítulo, é investigado o problema de posicionamento do sistema de rastreamento IP proposto. Foram testadas duas abordagens de colocação do sistema na rede: (i) posicionamento estratégico, onde os SAs com maior número de conexões com outros SAs tiveram o sistema de rastreamento instalado primeiro; (ii) posicionamento aleatório, onde a instalação do sistema de rastreamento foi feita aleatoriamente entre SAs.

A abordagem estratégica foi delineada com base em análises feitas recentemente sobre a topologia da Internet (FALOUTSOS, 1999; MEDINA, 2000; ALVES, 2005), considerada uma topologia livre de escala, onde existe a tendência de que, conforme a rede aumenta, novos nós se conectem a outros nós que possuem um alto grau de conectividade. Esta tendência ajuda a explicar porque a topologia da Internet possui poucos nós com um grande número de conexões, enquanto muitos nós possuem poucas conexões. Os resultados de simulação confirmam que o posicionamento estratégico do sistema proposto em um número relativamente reduzido de nós em uma topologia com estas características – similar a da Internet – é suficiente para realizar um rastreamento eficiente.

5.1 CONFIGURAÇÃO DA SIMULAÇÃO

Para gerar as topologias usadas nas simulações foi utilizado o software Nem (Network Manipulator) (MAGONI, 2002) com o modelo Barabási-Albert (ALBERT, 2000). O Nem recebe como entrada um arquivo que contém mapas da rede e extrai aleatoriamente um subgrafo deste mapa, respeitando as características das topologias consideradas livres de escala, como as da Internet. O arquivo de saída serve como topologia para o simulador de rede NS-2 versão 2.26 (NETWORK SIMULATOR 2, 1995) modificado pelo módulo de simulação BGP++ (DIMITROPOULOS, 2006). Este módulo é uma implementação do Zebra bgpd, que é a implementação do BGP nas plataformas Unix. Através deste módulo, foi possível executar perfeitamente o BGP nos roteadores das topologias geradas, usando

suas tabelas de rotas como entradas para as rotinas criadas em *shell-script*[7], rotinas estas que foram utilizadas para gerar os resultados utilizados na construção dos gráficos apresentados neste capítulo.

Para as primeiras simulações, que têm como resultados os gráficos da FIG. 5.1, FIG. 5.2, da FIG. 5.3, da FIG. 5.4, da FIG. 5.5 e da FIG. 5.6, foram utilizadas topologias de redes no nível de SAs contendo 300, 600 e 900 SAs. Para cada amostra, foram simuladas sete diferentes topologias com cinco conjuntos aleatórios de atacantes (10% de SAs) enviando tráfego para uma vítima, escolhida de forma aleatória para cada rodada de simulação. Os resultados das simulações possuem um intervalo de confiança de 99%, com valores médios de $\pm 2.1\%$ para o posicionamento estratégico e $\pm 3.8\%$ para o posicionamento aleatório.

Devido a esta similaridade nos resultados das simulações e ao fato de que as topologias utilizadas preservam as características de serem livres de escala, acreditamos que simulações com maiores quantidades de SAs também apresentem resultados similares.

Para as simulações que originaram os resultados dos gráficos das FIG. 5.7, FIG. 5.8, FIG. 5.9 e FIG. 5.10 foram usadas topologias no nível de SAs com 300 SAs. Para cada ponto do gráfico, foram utilizados dez conjuntos aleatórios de atacantes extraídos de quatro topologias diferentes, enviando pacotes para uma vítima, também escolhida de forma aleatória para cada rodada da simulação. Nestas simulações a quantidade de atacantes utilizada foi 30, 60, 120, 180 e 240, ou seja, respectivamente 10%, 20%, 40%, 60% e 80% da rede. Os resultados das simulações possuem um intervalo de confiança de 99% com valores médios de $\pm 3.2\%$ e $\pm 2.3\%$ para os gráficos do posicionamento estratégico e $\pm 5.1\%$ e $\pm 2.9\%$ para os gráficos do posicionamento aleatório.

Em todas as simulações realizadas nesta dissertação, considerou-se que vários atacantes podem estar localizados no mesmo SA e que se o último SA no caminho reverso do pacote for encontrado, significa que o atacante também foi encontrado, uma vez que o rastreamento dentro do SA não pode ser realizado e que a filtragem dos pacotes que partem deste SA pode ser feita.

Um dos propósitos das simulações é analisar o desempenho da instalação parcial (e incremental) do sistema proposto. Em outras palavras, a intenção é avaliar o compromisso

[7]Programa escrito em linguagem de programação interpretada, isto é, não compilada, que é executado em sistemas do tipo Unix.

entre a quantidade de SAs com o sistema instalado e a acurácia no rastreamento. Para isto, foram observadas características no caminho reverso dos pacotes indicado pelo sistema proposto, variando-se a porcentagem de instalação do sistema na rede, respeitando os dois tipos de estratégia utilizados. No posicionamento estratégico, os SAs foram classificados de acordo com a quantidade de conexões existentes com outros SAs. A ordem de instalação do sistema de rastreamento respeitou esta classificação. Por outro lado, no posicionamento aleatório, o sistema de rastreamento foi instalado sem levar em consideração qualquer tipo de classificação. A única regra foi que um SA só poderia ser sorteado para ter o sistema de rastreamento instalado uma vez por rodada de simulação, de forma a garantir que ao final de cada rodada todos os SAs possuiriam o sistema instalado.

Outro objetivo das simulações é verificar o comportamento do sistema de acordo com o crescimento do número de atacantes. Neste caso, foi variada a quantidade de atacantes na rede, de forma a analisar a eficiência do sistema em redes com um volume diversificado de caminhos entre as origens e o destino dos ataques, considerando que a filtragem ou bloqueio dos pacotes deve ser feita da forma mais distribuída possível.

Neste capítulo, além de apresentar os resultados das simulações para o sistema proposto, será feita uma breve comparação dos resultados obtidos com os resultados do sistema proposto por Korkmaz et al. (KORKMAZ, 2007), descrito anteriormente na Seção 3.2.2. Essa comparação foi feita com base no argumento que o sistema proposto por Korkmaz et al. (KORKMAZ, 2007) utilizou topologias que mantêm as características livres de escala, as mesmas utilizadas neste trabalho.

5.2 RESULTADOS

Na FIG. 5.1 é apresentado o percentual de caminho de ataque descoberto dependendo da quantidade de SAs da rede com o sistema de rastreamento instalado. Os resultados mostram que se o sistema for instalado de forma estratégica, são descobertos quase 100% do caminho reverso dos ataques no nível de SAs com aproximadamente 70% dos SAs da rede com o sistema instalado.

Na FIG. 5.2 é mostrado que para alcançar os mesmos resultados usando o posicionamento aleatório, o sistema deve estar instalado em quase 100% dos SAs da rede.

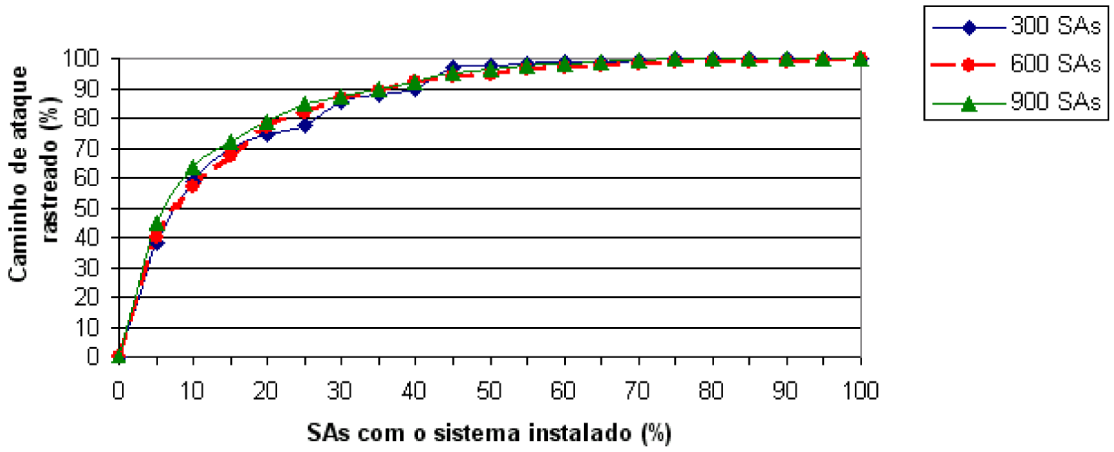

FIG. 5.1: Descoberta do caminho de ataque - Posicionamento estratégico.

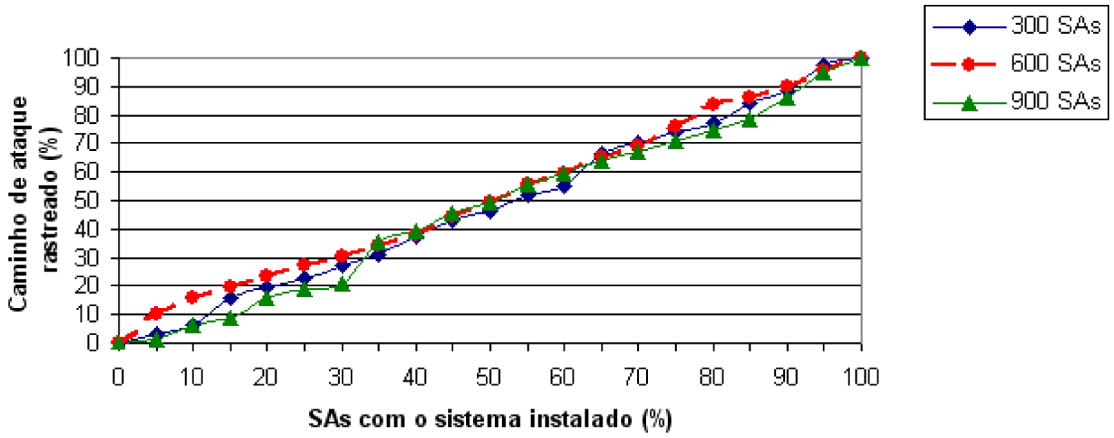

FIG. 5.2: Descoberta do caminho de ataque - Posicionamento aleatório.

Relaxando-se a exigência de encontrar-se todo o caminho percorrido pelo ataque, o posicionamento estratégico permite encontrar, por exemplo, 70%, 80% e 90% da rota percorrida pelo tráfego de ataque no nível de SAs com aproximadamente 15%, 20% e 40% dos SAs com o sistema de rastreamento proposto instalado. Ou seja, com uma porção relativamente pequena dos SAs possuindo o sistema proposto instalado – desde que escolhidos estrategicamente – é possível identificar-se uma grande porção da rota no nível de SAs tomada pelos pacotes de ataque.

Na FIG. 5.3 é observado que usando o sistema aqui proposto no posicionamento es-

tratégico, para que sejam identificados quase 100% dos atacantes, é necessário instalá-lo em aproximadamente 65% dos SAs da rede. Vale lembrar que neste caso, o último SA no caminho reverso do pacote foi encontrado, ou seja, o SA de onde os pacotes de ataque são originados. Isto ocorre porque foi considerado que este SA possui o sistema de rastreamento instalado e desta forma, assumiu-se que o atacante foi identificado, uma vez que o rastreamento foi capaz de determinar o SA do origem do ataque e dentro deste SA não se pode dar continuidade ao rastreamento.

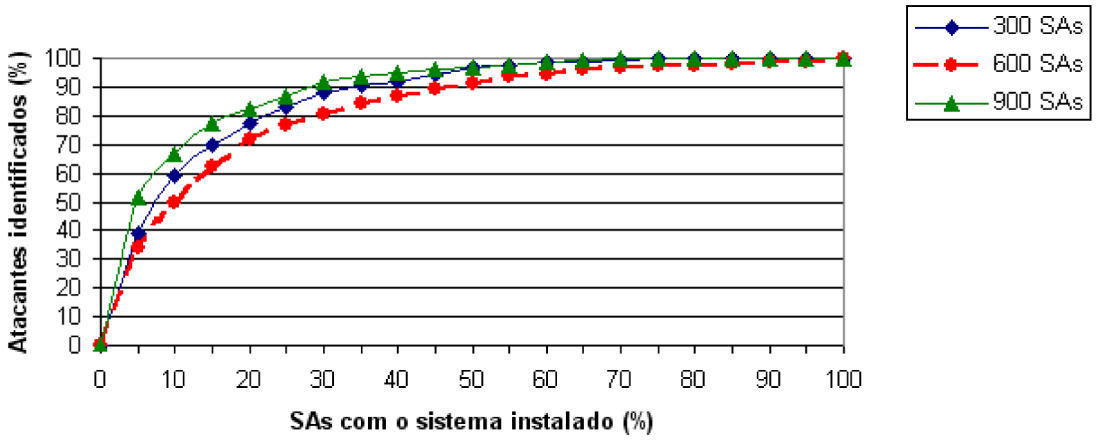

FIG. 5.3: Quantidade de atacantes identificados - Posicionamento estratégico.

Para conseguir identificar 100% dos atacantes utilizando o posicionamento aleatório, aproximadamente 96% dos SAs devem ter o sistema de rastreamento instalado, conforme pode ser observado na FIG. 5.4.

Na FIG. 5.5, pode-se observar que se o sistema de rastreamento for instalado no posicionamento estratégico, para que aproximadamente 100% dos SAs a 2 saltos dos atacantes seja descoberto, é necessário instalá-lo em aproximadamente 68% dos SAs da rede.

Para conseguirmos o mesmo resultado com o posicionamento aleatório, é necessário instalar o sistema de rastreamento proposto em 95% dos SAs da rede, conforme ilustrado na FIG. 5.6.

A FIG. 5.7 se refere ao posicionamento estratégico e mostra que a medida que o número de atacantes cresce, a eficiência do sistema tende a cair um pouco quando a rede possui

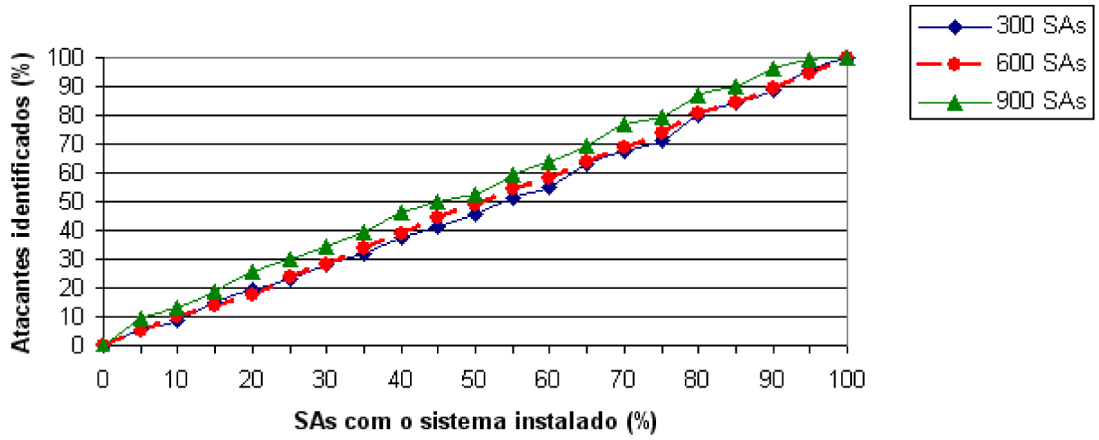

FIG. 5.4: Quantidade de atacantes identificados - Posicionamento aleatório.

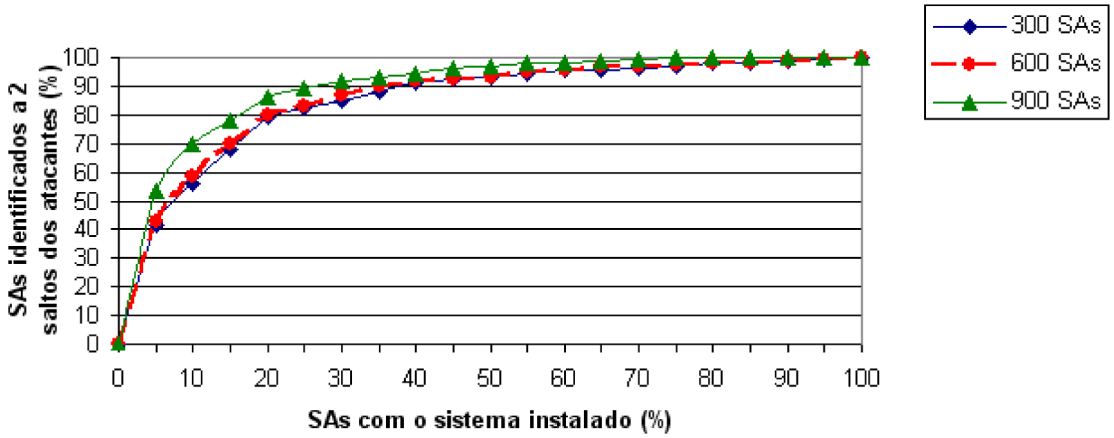

FIG. 5.5: Quantidade de SAs identificados a 2 saltos dos atacantes - Posicionamento estratégico.

uma porcentagem relativamente baixa de SAs com o sistema instalado (entre 10% e 35%). Como exemplo, se 30% dos SAs da rede possuírem o sistema de rastreamento instalado e a quantidade de atacantes for 10% da rede, o sistema consegue rastrear aproximadamente 86% do caminho; com 80% de atacantes na rede, é rastreado aproximadamente 63% do caminho, ou seja, uma diferença de 23%. Este comportamento ocorre porque os sistemas são instalados de forma estratégica e os atacantes são selecionados de forma aleatória. Sendo assim, a medida que a quantidade de atacantes na rede aumenta, alguns atacantes

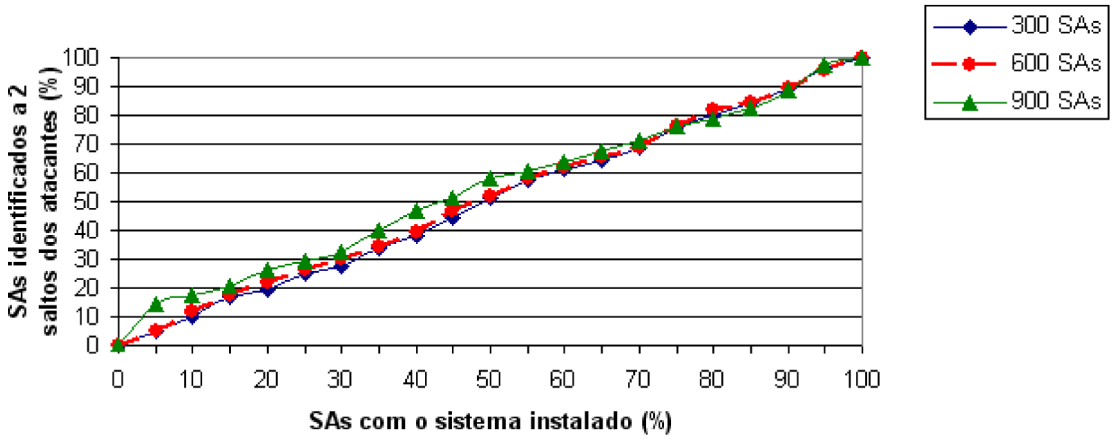

FIG. 5.6: Quantidade de SAs identificados a 2 saltos dos atacantes - Posicionamento aleatório.

podem estar mais longe dos SAs que possuem o sistema instalado do que outros, fazendo com que a porcentagem do caminho descoberto seja reduzida. Pode-se observar também que a medida que a quantidade de SAs com o sistema instalado aumenta, mesmo que a quantidade de atacantes na rede também aumente, a diferença na porcentagem do caminho rastreado diminui, sendo praticamente igual a partir do momento que 70% dos SAs da rede possuem o sistema instalado. Isto ocorre porque mais caminhos passam a ser rastreados quando a quantidade de sistemas de rastreamento na rede aumenta.

O mesmo comportamento pode ser observado na FIG. 5.8, que ilustra a quantidade de atacantes identificados, ainda que os caminhos completos dos pacotes de ataque não sejam descobertos.

As FIG. 5.9 e FIG. 5.10 referem-se ao posicionamento aleatório e mostram respectivamente a porcentagem do caminho rastreado e atacantes encontrados mesmo que o caminho completo não seja rastreado, dependendo da quantidade de SAs da rede com o sistema instalado. O comportamento dos gráficos é similar aos gráficos do posicionamento estratégico, mostrando uma certa independência quanto a eficiência do sistema em relação ao aumento do número de atacantes.

Na FIG. 5.11 é feita uma comparação da eficiência na busca pelos atacantes utilizando o sistema proposto neste trabalho e o sistema proposto por Korkmaz et al. (KORKMAZ,

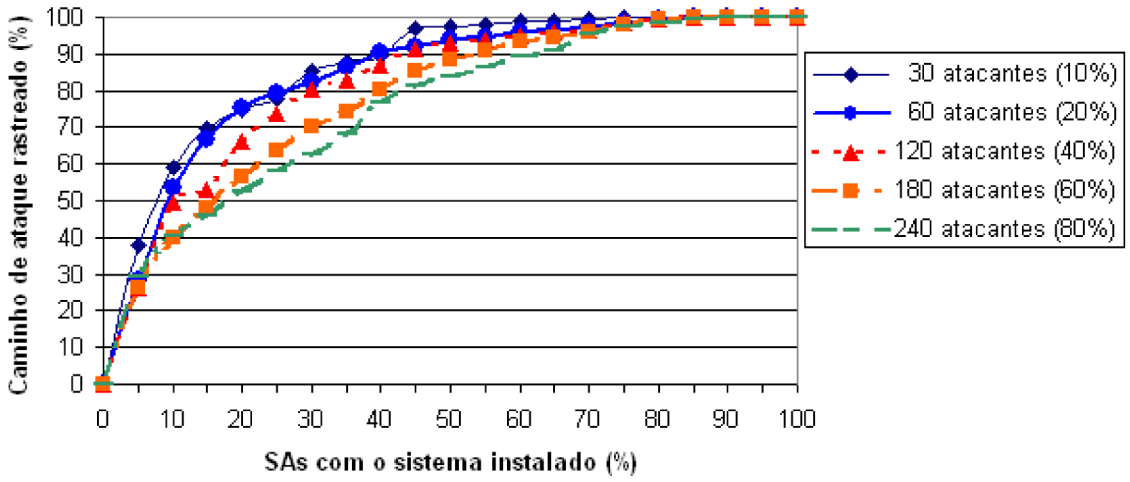

FIG. 5.7: Posicionamento estratégico - Descoberta do caminho do ataque de acordo com o crescimento do número de atacantes.

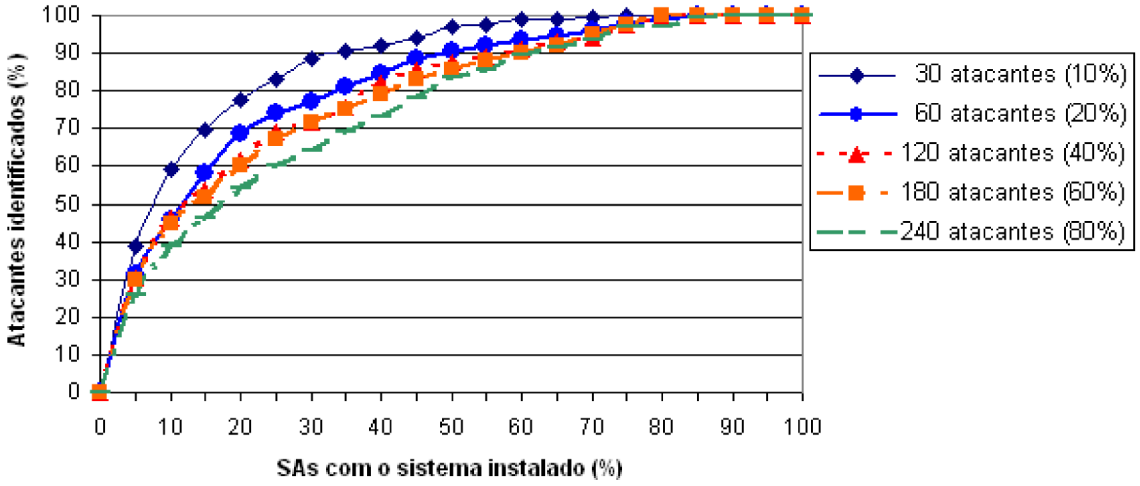

FIG. 5.8: Posicionamento estratégico - Percentual de atacantes identificados de acordo com o crescimento do número de atacantes.

2007)(detalhado anteriormente na 3.2.2) realizando consultas entre SAs com 3 níveis, que foi o melhor resultado encontrado para este sistema. Pode ser observado que usando o sistema aqui proposto no posicionamento estratégico, para que seja descoberto quase 100% dos atacantes, é necessário instalá-lo em aproximadamente 80% dos SAs da rede (este é um valor médio entre todos os valores encontrados variando-se a quantidade de atacantes na rede de 10% a 80%). Da mesma forma, para conseguir estes resultados

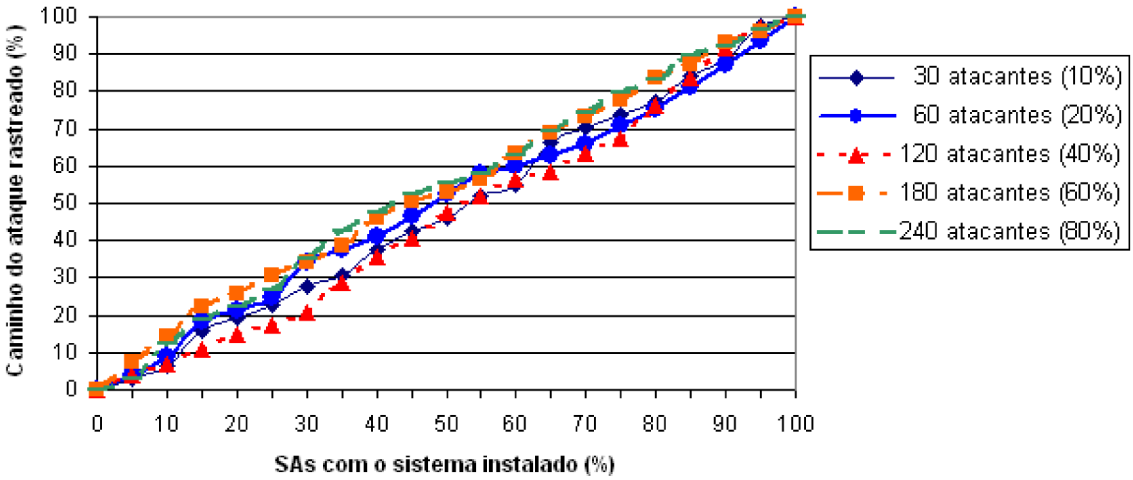

FIG. 5.9: Posicionamento aleatório - Descoberta do caminho do ataque de acordo com o crescimento do número de atacantes.

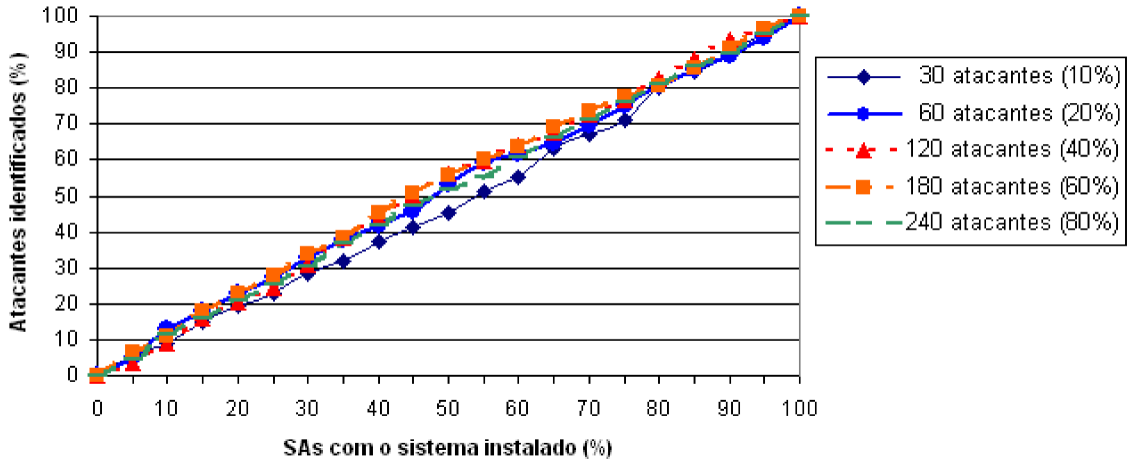

FIG. 5.10: Posicionamento aleatório - Percentual de atacantes identificados de acordo com o crescimento do número de atacantes.

utilizando o posicionamento aleatório, 100% dos SAs devem ter o sistema de rastreamento instalado. Para efeito de comparação com trabalhos anteriores, o resultado apresentado para o sistema proposto por Korkmaz et al. (KORKMAZ, 2007) é reproduzido na FIG. 5.11. Neste sistema, para que 100% dos atacantes sejam encontrados, o sistema deve ser instalado em aproximadamente 85% dos SAs da rede. Por outro lado, com uma taxa relativamente baixa de sistemas de rastreamento na rede, aproximadamente 30%, o

sistema aqui proposto consegue identificar mais de 70% dos atacantes, enquanto o sistema proposto por Korkmaz et al. (KORKMAZ, 2007) possui uma taxa de identificação de atacantes de 50%. Como um todo, avaliando os resultados apresentados na FIG. 5.11, evidencia-se a eficiência que pode ser alcançada pelo sistema ora proposto se utilizado o posicionamento estratégico.

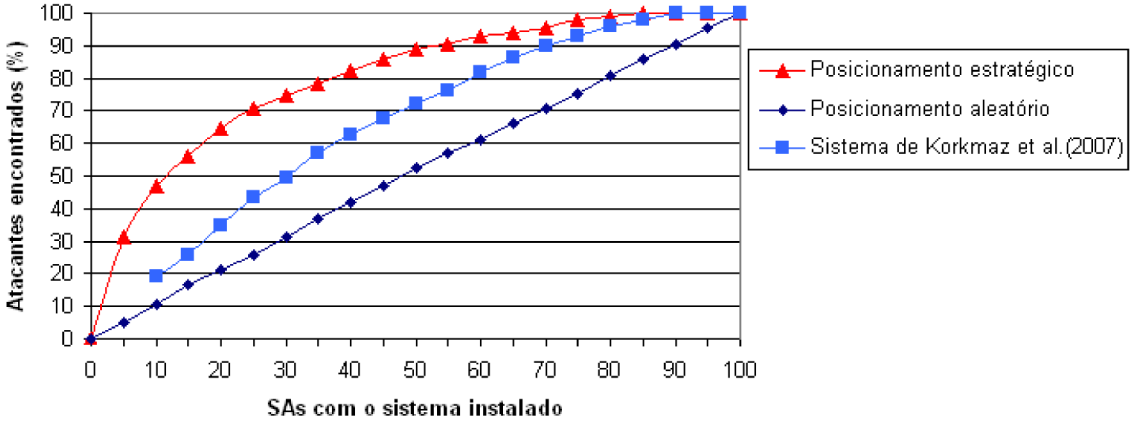

FIG. 5.11: Comparação de eficiência: Sistema proposto x Sistema de Korkmaz et al. (KORKMAZ, 2007).

Vale ressaltar que o gráfico ilustra a quantidade de atacantes encontrados, mas isto não significa que os atacantes que não foram rastreados não podem ser bloqueados ou ter seus pacotes filtrados, uma vez que pelo menos parte do caminho dos pacotes enviados por estes atacantes foi descoberto. Em outras palavras, se por exemplo 80% dos atacantes foram encontrados, o sistema conseguiu certamente descobrir parte do caminho por onde os 20% de atacantes restantes enviaram os pacotes de ataque e com isso os SAs podem realizar algum tipo de bloqueio contra esses pacotes.

Com o resultado das simulações, pode-se concluir que a medida que os SAs com uma quantidade maior de conexões encaminham mais tráfego, é recomendado que eles tenham o sistema de rastreamento instalado primeiro. Desta maneira, o processo de rastreamento será mais eficaz.

Os resultados sugerem que se o sistema proposto for instalado estrategicamente em aproximadamente 45% dos SAs da rede, providências e contramedidas contra ataques DDoS podem ser realizadas eficientemente, já que com esta taxa de instalação do sistema,

por volta de 90% do caminho de ataques no nível de SAs é descoberto. Com uma taxa similar a esta, o sistema de rastreamento proposto descobre aproximadamente 86% dos atacantes, além de apontar mais de 90% dos SAs a 2 saltos deles. Além disto, mesmo que uma quantidade pequena de SAs tenham o sistema instalado – em torno de 25% – o processo de rastreamento pode ainda sinalizar mais de 70% do caminho reverso do ataque. Estes dados sugerem que medidas eficientes podem ser tomadas de forma distribuída, uma vez que quando um atacante não é descoberto, existe uma grande chance de um SA a 2 saltos dele ter sido identificado, além de outros SAs no caminho reverso do ataque.

Pode-se concluir também, que mesmo que a quantidade de atacantes na rede seja muito grande, aproximadamente 80%, se o sistema for instalado estrategicamente, ele ainda pode rastrear uma grande quantidade de atacantes sem que sua eficiência seja muito comprometida.

6 CONSIDERAÇÕES FINAIS

Ataques distribuidos de negação de serviço representam uma séria ameaça à operação adequada dos serviços na Internet. Devido a forma com que o protocolo IP e o roteamento dos pacotes nas redes funcionam, os atacantes têm uma garantia virtual de anonimato no momento de realizar os ataques. Por este motivo, encontrar a origem de um ataque é uma tarefa desafiadora.

Os sistemas de rastreamento IP têm a função de encontrar a origem de um ataque através da reconstrução do caminho reverso utilizado pelos pacotes de ataque para alcançar a vítima. O grande desafio destes sistemas de rastreamento é criar incentivos para que possam ser adotados. Estes incentivos vão desde a facilidade de implementação aos custos de instalação.

Neste trabalho, os sistemas de rastreamento IP foram classificados em duas categorias: os que operam no nível de roteadores (*router-level*), que são os sistemas considerados mais tradicionais e os que trabalham no nível de Sistemas Autônomos (*AS-level*), que são os sistemas propostos mais recentemente.

Os sistemas que operam no nível de roteadores têm como principal requisito a necessidade de ser instalado em todos os roteadores da rede que se quer monitorar. Isto acontece devido ao resultado esperado para o rastreamento, que no caso desse tipo de sistema, é o caminho completo por onde o pacote trafegou na rede até alcançar seu destino. Isto limita muito a possibilidade desses tipos de sistema serem adotados em redes de larga escala, como por exemplo a Internet.

É importante lembrar que encontrar o caminho *completo* por onde os pacotes de ataque foram encaminhados não é necessário para garantir um rastreamento eficiente. De fato, se for considerado que o principal objetivo é bloquear os pacotes enviados por um ou mais atacantes, a instalação de um sistema de rastreamento se faz necessária apenas em alguns pontos críticos no caminho por onde os pacotes de ataque são encaminhados, de forma que providências contra os atacantes possam ser tomadas de forma eficaz e distribuída.

Os sistemas propostos nos últimos anos que levam este argumento em consideração são os sistemas que operam no nível de SAs.

Neste trabalho é proposto um sistema de rastreamento de tráfego IP no nível de SAs, que considera as características do protocolo de roteamento BGP, para permitir a criação de uma rede sobreposta no nível de SAs, que será utilizada pelos SAs participantes do rastreamento. É proposta a criação de um novo *Community Attribute* para o protocolo BGP, que será responsável por identificar qual SA possui o sistema de rastreamento IP proposto instalado. Estas características permitem que o sistema seja instalado *parcialmente* e *incrementalmente* na rede.

Foi proposto também um mecanismo de marcação de sequência dos roteadores, antes do pacote ser efetivamente marcado por um roteador de borda de um SA. Este mecanismo utiliza o TTL do pacote no momento que passa por um roteador de borda de um SA para identificar a ordem de passagem dos pacotes. É importante que esta ordem seja conhecida no momento da reconstrução da rota do pacote, de forma que os roteadores que fazem parte do rastreamento não tenham dúvidas de qual vizinho na rede sobreposta deve receber o pacote de reconstrução de rota.

O sistema de rastreamento de tráfego proposto neste trabalho, portanto, possui algumas vantagens quando comparado aos trabalhos anteriores, vantagens estas que caracterizam as contribuições da proposta. Ele pode ser instalado em apenas alguns SAs, contrastando com os sistemas de rastreamento tradicionais que em geral precisam ser instalados em todos os roteadores da rede monitorada. Acredita-se que esta abordagem é suficiente para encontrar os SAs que encaminham mais tráfego de ataque (ou pelo menos SAs mais próximos a ele) para que este seja alertado e tome providências para filtrar os ataques de forma distribuída.

O sistema proposto pode ainda ser instalado incrementalmente na Internet, permitindo que SAs possam colaborar gradualmente com a estrutura do rastreamento a qualquer momento, desta forma contribuindo para o aumento da eficiência do rastreamento. Além disso, os custos de implementação são diminuídos, pois mesmo que o sistema seja instalado em uma rede de larga escala, ele não precisa estar presente em todos os pontos da rede.

Foram realizadas simulações para avaliar a implementação parcial e incremental do

sistema, além de seu comportamento com o crescimento do número de atacantes na rede. Utilizou-se dois tipos de posicionamento para avaliar o sistema: estratégico, que levou em consideração a quantidade de conexões entre os SAs no momento da escolha de qual SA teria o sistema de rastreamento instalado primeiro; e aleatório, onde os SAs escolhidos para ter o sistema instalado foram simplesmente sorteados.

Os resultados das simulações mostram que através do posicionamento estratégico do sistema proposto, pode-se ter informação suficiente para bloquear ou filtrar de forma distribuída ataques de larga escala – DDoS – perto de suas fontes, suavizando seus efeitos antes que os pacotes alcancem o SA da vítima. Os resultados sugerem que tais bloqueios ou filtragens podem ser efetuadas se o sistema proposto for instalado estrategicamente em aproximadamente 45% dos SAs da rede, já que com esta taxa de instalação do sistema, aproximadamente 90% do caminho de ataques no nível de SAs é descoberto. Com uma taxa similar a esta, o sistema de rastreamento proposto descobre aproximadamente 86% dos atacantes, isto é, os SAs de onde os pacotes de ataque são originados, além de apontar mais de 90% dos SAs a 2 saltos dos atacantes. Além disto, mesmo que uma quantidade pequena de SAs tenham o sistema instalado – em torno de 25% – o processo de rastreamento pode ainda sinalizar mais de 70% do caminho reverso do ataque, permitindo que medidas eficientes sejam tomadas de forma distribuída.

Durante as simulações, foi feita uma comparação com um outro sistema no nível de SAs presente na literatura, proposto por Korkmaz et al. (KORKMAZ, 2007). Os resultados mostram que utilizando o posicionamento estratégico proposto aqui nesta dissertação, pode-se obter resultados superiores ao posicionamento estratégico utilizado por Korkmaz et al. (KORKMAZ, 2007). Para efeito de comparação, pode-se dizer que para o posicionamento estratégico ser utilizado em ambos os sistemas, a topologia da rede deve ser conhecida. Porém, sem este conhecimento, o sistema aqui proposto ainda pode ser utilizado, mesmo que em um posicionamento aleatório, ou em alguns casos, a partir de algum conhecimento prévio da topologia, com um outro tipo de posicionamento estratégico. Por outro lado, o sistema de Korkmaz et al. (KORKMAZ, 2007) possui como requisito principal para seu funcionamento o conhecimento prévio da topologia da rede.

Ao longo do desenvolvimento deste trabalho foram publicados trabalhos em 4 con-

gressos. São eles: o Lanoms'07 (CASTELUCIO, 2007b), o CoNEXT'07 (CASTELUCIO, 2007a), o ACM/SAC'08 (CASTELUCIO, 2008a) e o SBRC'08 (CASTELUCIO, 2008b).

Como trabalhos futuros pretende-se estudar a possibilidade de integrar o sistema proposto neste trabalho com um sistema de rastreamento que opera no nível de roteadores, com a finalidade de realizar um rastreamento em níveis, onde em um primeiro momento o SA de onde são originados os pacotes de ataque possa ser descoberto, e em um segundo momento possa haver a descoberta do atacante dentro deste SA, aumentado assim as chances de se chegar mais perto do atacante e realizar uma filtragem ainda mais eficiente.

Pretende-se também avaliar o desempenho do sistema proposto em um ambiente mais próximo do real. Da mesma forma, considera-se a possibilidade de utilizar a idéia proposta neste trabalho com o protocolo BGP em um protocolo de roteamento interno aos SAs, como por exemplo o OSPF (*Open Shortest Path First*) (MOY, 1998), para permitir que o rastreamento dentro de um SA possa ser feito mesmo se o sistema for instalado parcialmente e incrementalmente, aumentando assim a possibilidade de adoção deste novo sistema em SAs muito grandes, que teriam como principal incentivo para adoção de um sistema de rastreamento o baixo custo de implementação.

7 REFERÊNCIAS BIBLIOGRÁFICAS

AGARWAL, Sharad e GRIFFIN, Timothy G. **BGP Proxy Community Community**. IETF Internet Draft, January 2004.

ALBERT, Reka e BARABASI, Albert-Laszlo. **Topology of evolving networks: local events and universality**. Physical Review Letters, v. 85, p. 5234, 2000. URL `http://www.citebase.org/abstract?id=oai:arXiv.org:cond-mat/0005085`.

ALJIFRI, Hassan. **IP traceback: A new denial-of-service deterrent?** IEEE Security and Privacy, v. 1, n. 3, p. 24–31, 2003. ISSN 1540-7993.

ALVES, Nilton. **Caracterização de Redes Complexas - Aplicação à Modelagem Relacional entre Sistemas Autônomos da Internet**. Tese de Doutorado - Universidade do Estado do Rio de Janeiro, Março 2007.

ALVES, Nilton, DE ALBUQUERQUE, Márcio Portes, DE ALBUQUERQUE, Marcelo Portes e DE ASSIS, Joaquim Teixeira. **Topologia e modelagem relacional da Internet Brasileira**. Em XXVI Iberian Latin American Congress on Computational Methods in Engineering- CILAMCE'05, Guarapari, Brasil, October 2005.

BELENKY, A. e ANSARI, N. **On IP traceback**. IEEE Communications Magazine, v. 41, n. 7, , July 2003.

BELLOVIN, Steve, LEECH, Marcos e TAYLOR, Tom. **ICMP Traceback messages**. IETF Internet Draft, February 2003.

BLOOM, Burton. **Space/time tradeoffs in hash coding with allowable errors**. Communications of the ACM, v. 13, n. 7, p. 422–426, 1970.

BONAVENTURE, O. e QUOITIN, B. **Common utilizations of the BGP community attribute**. IETF Internet Draft, June 2003.

BRODER, Andrei e MITZENMACHER, Michael. **Network applications of Bloom filters: A survey**. Internet Mathematics, v. 1, n. 4, p. 485–509, 2004.

BURCH, Hal e CHESWICK, Bill. **Tracing anonymous packets to their approximate source**. Em Proceedings of the USENIX LISA Conference, 2000.

CAIDA. **Nameserver DoS Attack October 2002**. Technical report, CAIDA- Cooperative Association for Internet Data Analysis, 2002. URL `http://www.caida.org/funding/dns-analysis/oct02dos.xml, visitado em Janeiro de 2008`.

CASTELUCIO, André O., SALLES, Ronaldo M. e ZIVIANI, Artur. **An AS-level IP traceback system**. Em Proceedings of the 3rd International Conference on emerging Networking EXperiments and Technologies - CoNEXT'07, New York, NY, USA, December 2007a. Poster.

CASTELUCIO, André O., SALLES, Ronaldo M. e ZIVIANI, Artur. **Towards a large-scale AS-level IP traceback system**. Em Proceedings of the 5th Latin American Network Operations and Management Symposium - Lanoms'07, Petrópolis, Rio de Janeiro, Brasil, September 2007b. Short-paper.

CASTELUCIO, André O., SALLES, Ronaldo M. e ZIVIANI, Artur. **Evaluating the partial deployment of an AS-level IP traceback system**. Em Proceedings of the ACM Symposium on Applied Computing – ACM SAC'08, Fortaleza, Brasil, March 2008a.

CASTELUCIO, André O., SALLES, Ronaldo M. e ZIVIANI, Artur. **Uma rede sobreposta no nível de sistemas autônomos para rastreamento de tráfego IP**. Em Simpósio Brasileiro de Redes de Computadores - SBRC'08, Rio de Janeiro, Brasil, Maio 2008b.

CERT. **CERT Advisory CA-1996-21 TCP SYN flooding and IP spoofing attacks**. Technical report, CERT- Computer Emergency Response Team, 1996. URL `http://www.cert.org/advisories/CA-1996-21.html, visitado em Março de 2007`.

CERT. **CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks**. Technical report, CERT- Computer Emergency Response Team, 2000. URL `http://www.cert.org/advisories/CA-1998-01.html, visitado em Dezembro de 2007`.

CERT. **Denial of service attacks**. Technical report, CERT- Computer Emergency Response Team, 2001. URL `http://www.cert.org/tech_tips/denial_of_service.html, visitado em Março de 2007`.

CHANDRA, R., TRAINA, P. e LI, T. **BGP Communities Attribute**. Internet Engineering Task Force. RFC 1997, 1996. URL `http://www.ietf.org/rfc/rfc1997.txt`.

CHEN, E. e BATES, T. **An Application of the BGP Community Attribute in Multi-home Routing**. Internet Engineering Task Force. RFC 1998, 1996. URL `http://www.ietf.org/rfc/rfc1998.txt`.

CHEN, Eric Y. **Detecting DoS attacks on SIP systems**. Em In Proceedings of the 1st IEEE Workshop on VoIP Management and Security, p. 53–58, April 2006.

CSI/FBI. **Computer crime and security survey**. Technical report, CSI/FBI - Computer Security Institute / Federal Bureau of Investigation, 2006. URL `http://www.gocsi.com/press/20060712.jhtml, visitado em Março de 2007`.

DARPA. **Transmission Control Protocol**. Internet Engineering Task Force. RFC 793, September 1981. URL `http://www.ietf.org/rfc/rfc793.txt`.

DIMITROPOULOS, Xenofontas, VERKAIK, Patrick e RILEY, George. **BGP++** ***http://www.ece.gatech.edu/research/labs/MANIACS/ BGP++*** , 2006.

DUFFIELD, N.G. e GROSSGLAUSER, M. **Trajectory sampling for direct traffic observation**. IEEE/ACM Transactions on Networking, v. 9, n. 3, p. 280–292, 2001.

DURRESI, Arjan, PARUCHURI, Vamsi, BAROLLI, Leonard, KANNAN, Rajgopal e IYENGAR, S. Sitharama. **Efficient and secure autonomous system based traceback**. Journal of Interconnection Networks, v. 5, n. 2, p. 151–164, 2004.

FALOUTSOS, Michalis, FALOUTSOS, Petros e FALOUTSOS, Christos. **On power-law relationships of the internet topology**. Em SIGCOMM '99: Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication, p. 251–262, New York, NY, USA, 1999. ACM Press. ISBN 1-58113-135-6.

FERGUSON, P. e SENIE, D. **Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing**. Internet Engineering Task Force. RFC 2827, 2002. URL `http://www.ietf.org/rfc/rfc2827.txt`.

HUSSAIN, Alefiya, HEIDEMANN, John e PAPADOPOULOS, Christos. **A framework for classifying denial of service attacks**. Em SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, p. 99–110, New York, NY, USA, 2003. ACM Press. ISBN 1-58113-735-4.

HUSTON, G. **NOPEER Community for Border Gateway Protocol (BGP) Route Scope Control**. Internet Engineering Task Force. RFC 3765, 2004. URL `http://www.ietf.org/rfc/rfc3765.txt`.

INTERNET TOPOLOGY GENERATOR. **http://topology.eecs.umich.edu/inet/**, 2002.

ISS. **Distributed denial of service attack tools**. Technical report, ISS- Internet Security Systems, 2000. URL `http://www.iss.net/documents/whitepapers/ddos.pdf, visitado em Março de 2007`.

KORKMAZ, Turgay, GONG, Chao, LE, Trinh e SARAC, Kamil. **Single packet IP traceback in AS-level partial deployment scenario**. Em IEEE Global Communications Conference (GLOBECOM), November 2005.

KORKMAZ, Turgay, GONG, Chao, SARAC, Kamil e DYKES, Sandra. **Single packet IP traceback in AS-level partial deployment scenario**. International Journal of Security and Networks, v. 2, n. 1/2, p. 95–108, 2007.

KRISHNAMURTHY, Balachander. **Mohonk: mobile honeypots to trace unwanted traffic early**. Em NetT '04: Proceedings of the ACM SIGCOMM workshop on Network troubleshooting, p. 277–282, New York, NY, USA, 2004. ACM Press. ISBN 1-58113-942-9.

LAUFER, Rafael P., VELLOSO, Pedro B., DE O. CUNHA, Daniel, MORAES, Igor M., BICUDO, Marco D. D., CAMPISTA, Miguel Elias M., COSTA, Luis Henrique M. K. e DUARTE, Otto Carlos M. B. **Negação de serviço: Ataques e contramedidas**. Em Minicurso do Simpòsio Brasileiro de Segurança da Informação e de Sistemas Computacionais- SBSeg'2005, p. 1–63, Florianòpolis, Brasil, Setembro 2005a.

LAUFER, Rafael P., VELLOSO, Pedro B., DE O. CUNHA, Daniel, MORAES, Igor M., BICUDO, Marco D. D. e DUARTE, Otto Carlos M. B. **A new IP traceback system against denial-of-service attacks**. Em 12th International Conference on Telecommunications - ICT'2005, Capetown, South Africa, May 2005b.

LAUFER, Rafael P., VELLOSO, Pedro B. e DUARTE, Otto Carlos M. B. **Generalized bloom filters, gta-05-43**. Technical report, COPPE/UFRJ, September 2005c. URL `http://www.cs.ucla.edu/ rlaufer/publications/gbf.pdf`.

MAGONI, Damien. **Network manipulator. *https://dpt-info.u-strasbg.fr/ magoni/nem***, 2002.

MAHAJAN, Ratul, BELLOVIN, Steven M., FLOYD, Sally, IOANNIDIS, John, PAXSON, Vern e SHENKER, Scott. **Controlling high bandwidth aggregates in the network**. SIGCOMM Comput. Commun. Rev., v. 32, n. 3, p. 62–73, 2002. ISSN 0146-4833.

MARTINS, Denilson Vedoveto e DE MORAES, Luis Felipe M. **BGP traceback: Um novo método para identificação de caminhos de ataque na internet**. Em Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg'06, Setembro 2006.

MEDINA, Alberto, MATTA, Ibrahim e BYERS, John. **On the origin of power laws in internet topologies**. SIGCOMM Comput. Commun. Rev., v. 30, n. 2, p. 18–28, 2000. ISSN 0146-4833.

MEYER, D. **BGP Communities for Data Collection**, 2006. URL `http://www.ietf.org/rfc/rfc4384.txt`.

MIRKOVIC, Jelena e REIHER, Peter. **A taxonomy of DDoS attack and DDoS defense mechanisms**. SIGCOMM Comput. Commun. Rev., v. 34, n. 2, p. 39–53, 2004. ISSN 0146-4833.

MOCKAPETRIS, P. **Domain names: Concepts and Facilities**. Internet Engineering Task Force. RFC 1034, 1987. URL `http://www.ietf.org/rfc/rfc1034.txt`.

MOORE, David, SHANNON, Colleen, BROWN, Douglas J., VOELKER, Geoffrey M. e SAVAGE, Stefan. **Inferring internet denial-of-service activity**. ACM Trans. Comput. Syst., v. 24, n. 2, p. 115–139, 2006. ISSN 0734-2071.

MOREIRA, Marcelo D. D., COUTINHO, Gustavo L., MORAES, Igor M., LAUFER, Rafael P. e DUARTE, Otto Carlos M. B. **RAT: Implementação de um serviço de rastreamento de pacotes**. Em XI Workshop de Gerência e Operação de Redes e Serviços - WGRS'2006, Curitiba, PR, Brazil, May 2006.

MOY, J. **OSPF version 2**. Internet Engineering Task Force. RFC 2328, 1998. URL `http://www.ietf.org/rfc/rfc2328.txt`.

NETWORK SIMULATOR 2. **http://www.isi.edu/nsnam/ns**, 1995.

NIST. **Guide to Intrusion Detection and Prevention Systems - (IDPS)**. Technical report, NIST- National Institute of Standards and Technology, 2007. URL `http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, visitado em Janeiro de 2008`.

PARK, Kihong e LEE, Heejo. **On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack**. Em Proceedings IEEE Infocomm 2001, p. 338–347, April 2001.

PAXSON, Vern. **An analysis of using reflectors for distributed denial-of-service attacks**. SIGCOMM Comput. Commun. Rev., v. 31, n. 3, p. 38–47, 2001. ISSN 0146-4833.

QUOITIN, B. e BONAVENTURE, O. **A survey of the utilization of the BGP community attribute**. IETF Internet Draft, March 2002.

REKHTER, Y. e LI, T. **A border gateway protocol 4 (BGP-4)**. RFC 1771, March 1995.

REKHTER, Y., MOSKOWITZ, B., KARRENBERG, D., DE GROOT, G. J. e LEAR, E. **Address Allocation for Private Internets**. Internet Engineering Task Force. RFC 1918, 1996. URL `http://www.ietf.org/rfc/rfc1918.txt`.

ROSEN, E. e REKHTER, Y. **BGP/MPLS IP Virtual Private Networks (VPNs)**, 2006. URL `http://www.ietf.org/rfc/rfc4364.txt`. Updated by RFCs 4577, 4684.

ROSENBERG, J., SCHULZRINNE, H., CAMARILLO, G., JOHNSTON, A., PETERSON, J., SPARKS, R., HANDLEY, M. e SCHOOLER, E. **SIP: Session Initiation Protocol**. Internet Engineering Task Force. RFC 3261, 2002. URL `http://www.ietf.org/rfc/rfc3261.txt`.

SAVAGE, Stefan, WETHERALL, David, KARLIN, Anna e ANDERSON, Tom. **Practical network support for IP traceback**. Em Proceedings of the 2000 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM), p. 295–306, Stockholm, Sweden, August 2000.

SNOEREN, Alex C., PARTRIDGE, Craig, SANCHEZ, Luis A., JONES, Christine E., TCHAKOUNTIO, Fabrice, SCHWARTZ, Beverly, KENT, Stephen T. e STRAYER, W. Timothy. **Single-packet IP traceback**. IEEE/ACM Trans. Netw., v. 10, n. 6, p. 721–734, December 2002. ISSN 1063-6692.

SONG, Dawn X. e PERRIG, Adrian. **Advanced and authenticated marking schemes for IP traceback**. Em Proceedings IEEE Infocomm 2001, p. 878–886, April 2001.

STONE, Robert. **Centertrack: An IP overlay network for tracking dos floods**. Em Proceedings of the 9th USENIX Security Symposium, p. 119–212, December 2000.

TURK, D. **Configuring BGP to Block Denial-of-Service Attacks**. Internet Engineering Task Force. RFC 3882, 2004. URL `http://www.ietf.org/rfc/rfc3882.txt`.

VIXIE, Paul, SNEERINGER, Gerry e SCHLEIFER, Mark. **Events of 21-oct-2002**. Technical report, 2002. URL `http://www.isc.org/ops/f-root/october21.txt`, `visitado em Janeiro de 2008`.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo