Uma rede sobreposta no nível de Sistemas Autônomos para rastreamento de tráfego IP

André O. Castelucio[1], Ronaldo M. Salles[1], Artur Ziviani[2]

[1]Instituto Militar de Engenharia - IME
Praça General Tibúrcio, 80 – 22290-270 – Rio de Janeiro – RJ – Brazil

[2]Laboratório Nacional de Computação Científica - LNCC
Av. Getúlio Vargas, 333 – 25651-075 – Petrópolis – RJ – Brazil

{castelucio, salles}@ime.eb.br, ziviani@lncc.br

Abstract. *Distributed Denial of Service (DDoS) attacks currently represent a serious threat to the appropriate operation of Internet services. We propose 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 requires a priori no knowledge of the network topology while allowing single packet traceback and incremental deployment. We also investigate and evaluate the strategic placement of our system, 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.*

Resumo. *Ataques distribuídos de negação de serviço (DDoS) atualmente representam uma grande ameaça à operação adequada de serviços na Internet. Nós propomos um sistema que cria uma rede sobreposta de rastreamento de tráfego IP a ser implementada no nível de Sistemas Autônomos (SAs) para lidar com essa ameaça. Nosso 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. Nós também investigamos e avaliamos a implementação estratégica do sistema proposto, 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.*

1. Introdução

A Internet atual é vulnerável a ataques distribuídos de negação de serviço (DDoS) [CERT 2001, Hussain et al. 2003, Mirkovic e Reiher 2004, Moore et al. 2006]. Ataques desse tipo tem 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 nos dias atuais tipicamente ocorre com múltiplas fontes enviando pacotes para a mesma vítima.

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 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 o rastreamento só será realizado até a borda da rede de onde os pacotes são provenientes.

Todos estes fatos deixam ao atacante 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 – os sistemas de rastreamento de tráfego IP têm esta finalidade – e o desenvolvimento de ferramentas para bloquear os ataques ao menos em alguns pontos estratégicos nesta rota.

É importante deixar claro que em geral a defesa contra ataques possui 3 fases: (i) a detecção da ocorrência de um ataque, que é usualmente feita por sistemas de detecção e prevenção de intrusão [NIST 2007]; (ii) a identificação da origem dos pacotes de ataque, ou seja, o rastreamento dos atacantes; (iii) e a filtragem e bloqueio dos pacotes de ataque. Ressaltamos que o sistema aqui proposto é focado na segunda fase, ou seja, no rastreamento dos pacotes de ataque e consequentemente, na identificação da origem dos atacantes.

Trabalhos relacionados na área de rastreamento de tráfego (discutidos mais profundamente na Seção 2) 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.

Neste artigo é proposta e avaliada uma rede sobreposta para rastreamento de tráfego IP que trabalha no nível de Sistemas Autônomos (SAs) [1] e que pode ser instalada *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, 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 relativamente pequeno de SAs com o sistema instalado – desde que escolhidos estrategicamente – o rastreamento pode ser realizado de forma eficiente em redes de larga escala.

O restante do artigo está organizado da seguinte forma. Na Seção 2, são discutidos os trabalhos relacionados. O sistema proposto é apresentado na Seção 3. Na Seção 4, o problema do posicionamento é abordado através de simulações. Finalmente, na Seção 5 são apresentadas as conclusões e os trabalhos futuros.

[1] A proposta preliminar deste trabalho foi apresentada como poster em [Castelucio et al. 2007].

2. Trabalhos relacionados

Vários sistemas de rastreamento de tráfego IP foram propostos nos últimos anos [Aljifri 2003, Belenky e Ansari 2003]. Savage et al. [Savage et al. 2000] propuseram um sistema baseado em marcação probabilística de pacotes, a medida que estes passam pelos roteadores. Essa 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 é capaz de reconstruir o caminho de ataque. Bellovin et al. [Bellovin et al. 2003] introduziram um outro sistema baseado em marcação probabilística de pacotes. Para cada pacote selecionado, uma mensagem ICMP 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 TTL do pacote. Tal informação é usada pela vítima no momento da reconstrução da rota.

Snoeren et al. [Snoeren et al. 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 e Mitzenmacher 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. Laufer et al. [Laufer et al. 2005a] introduziram um outro sistema baseado em Filtros de Bloom. Nesse sistema, quando um pacote atravessa um roteador, é inserida uma marca dentro de um Filtro de Bloom Generalizado (FBG) [Laufer et al. 2005b], 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. 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. Por sua vez, este roteador também verifica o FBG a procura da marca de um de seus vizinhos. 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. De forma similar ao SPIE, este sistema pode rastrear um único pacote.

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 neces-

sidade 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 de 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. Em realidade, se faz necessário apenas identificar alguns pontos críticos no caminho por onde os pacotes de ataque são encaminhados (por exemplo no sistema autônomo 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. Durresi et al. [Durresi et al. 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 número identificador do SA 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. 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. Korkmaz et al. [Korkmaz et al. 2007] propõem o sistema AS-SPT (*AS-level Single Packet Traceback*), em um cenário de instalação parcial. Cada SA possui um ASTS (*Autonomous System Traceback Server*) responsável por monitorar os roteadores de borda e armazenar resumos dos pacotes. O ASTS também serve como ponto principal de contato para as requisições de rastreamento vindas de usuários locais ou remotos. Os autores basicamente definem a arquitetura do sistema sem propor um novo mecanismo de rastreamento para ser usando nos ASTSes – eles sugerem o SPIE como possível candidato dada sua popularidade. Embora a arquitetura proposta permita instalação parcial, ela tem como necessidade o conhecimento prévio da topologia da rede além de ser vulnerável, já que os ASTSes podem ser atacados e se tornarem incapazes de executar o rastreamento.

Em um trabalho anterior [Castelucio et al. 2008], nós avaliamos o desempenho de uma possível instalação parcial de um sistema de rastreamento de tráfego, sem a criação de uma rede sobreposta. A partir dos resultados promissores encontrados nesse trabalho anterior, houve a concepção e a proposição do sistema de rede sobreposta no nível de Sistemas Autônomos para rastreamento de tráfego IP apresentado no presente artigo. Em contraste com os demais trabalhos na literatura sobre rastreamento de tráfego IP, a rede sobreposta no nível de SAs para rastreamento de tráfego IP proposta neste artigo não requer conhecimento prévio da topologia da rede enquanto permite o rastreamento de um único pacote bem como uma instalação parcial e incremental.

3. Rede sobreposta para rastreamento de tráfego IP no nível de SAs

No sistema proposto neste trabalho, a marcação dos pacotes é feita de forma similar ao originalmente proposto por Laufer et al. [Laufer et al. 2005a]. 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. O sistema

aqui proposto, no entanto, utiliza o protocolo de roteamento BGP (*Border Gateway Protocol*) [Rekhter e Li 1995] como veículo de comunicação entre os SAs que possuem o sistema de rastreamento instalado. Essa comunicação 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 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.

Vale ressaltar que a utilização dos Filtros de Bloom em sistemas de rastreamento já foi amplamente discutida em outros artigos e, portanto, preferimos exaltar as diferenças, vantagens e contribuições do nosso sistema quando comparado aos demais. Ao longo desta seção, apresentaremos os mecanismos através dos 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.

3.1. Uso do BGP como veículo de comunicação do sistema proposto

Os roteadores BGP usam a mensagem `Update` para trocar informações de roteamento entre si – os roteadores vizinhos são conhecidos como *peers* BGP. Essa mensagem `Update` possui um atributo chamado `Path Attribute`, que é uma coleção de atributos associados às rotas que podem influenciar no processo de seleção das mesmas. Um desses atributos, chamado `Community Attribute`, definido na RFC 1997 [Chandra et al. 1996], é usado por um grupo de SAs que possuem características comuns [Quoitin e Bonaventure 2002]. Esse atributo mostra-se bastante versátil e pode ser utilizado com diferentes propósitos, tais como roteamento *multi-home* [Chen e Bates 1996], engenharia de tráfego [Huston 2004], suporte para VPNs [Rosen e Rekhter 2006] e sistemas de *honeypot* móveis [Krishnamurthy 2004].

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 rastreamente de tráfego no nível de SAs. Uma característica importante sobre o `Community Attribute` refere-se a ele ser um atributo BGP opcional e transitivo. Isso significa que se a implementação do BGP operando no roteador de um SA não reconhece um atributo opcional presente na mensagem `Update` recebida, uma verificação se o *flag transitive* está ativado ou não para este atributo é realizada. Em caso positivo, o atributo é repassado nas mensagens `Update` seguintes enviadas pelo roteador do SA para seus *peers*. 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. Ao final de uma seqüência de mensagens `Update`, a rede sobreposta de roteamento, 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.

3.2. Criação da rede sobreposta para rastreamento de tráfego IP

A rede sobreposta permite que o rastreamento de tráfego seja realizado entre os roteadores dela participantes (não necessariamente contíguos no nível de rotamento) 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.

Um exemplo da criação da rede sobreposta pode ser visto na Figura 1. 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. Esse processo se repete por todos os SAs da rede. Uma observação importante 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. 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*. 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 Tabela 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.

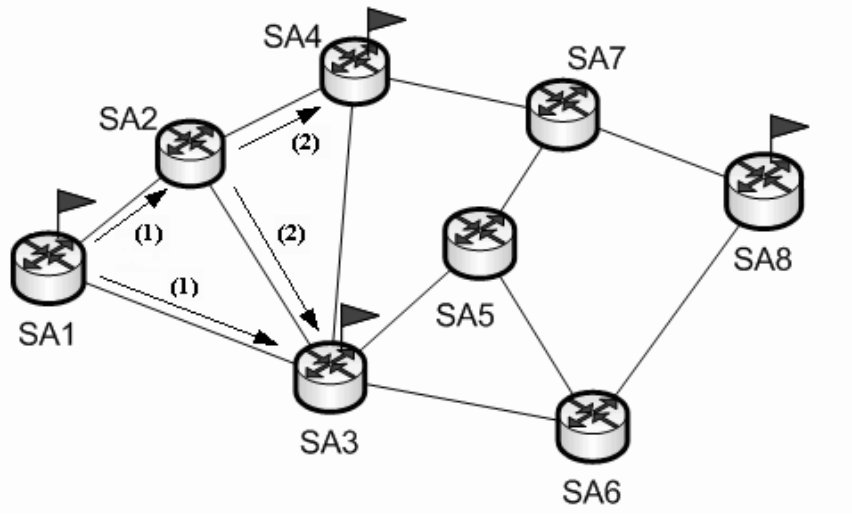

Figura 1. Troca de mensagens Update do BGP.

A rede sobreposta resultante é ilustrada na Figura 2, onde as linhas de maior espessura representam suas conexões.

Tabela 1. Tabela de overlay dos SAs.

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

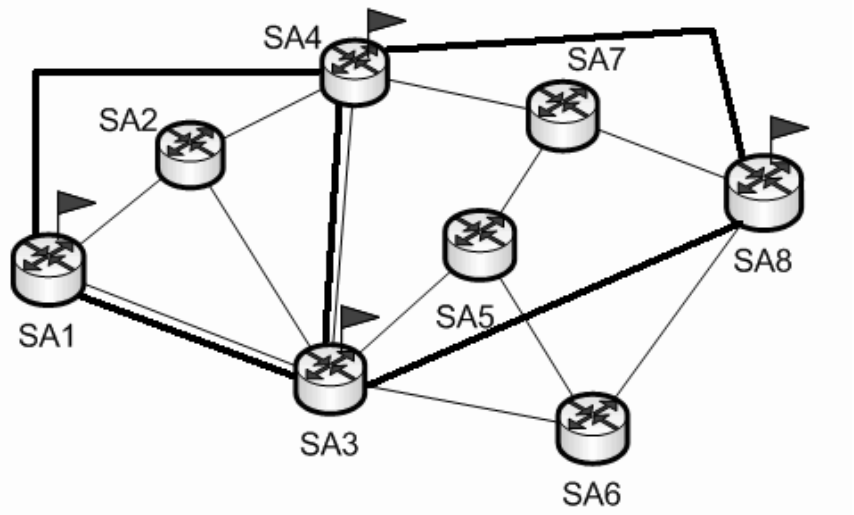

Figura 2. Rede sobreposta resultante da troca de mensagens Update do BGP.

3.3. Marcação de pacotes

O processo de marcação de pacotes proposto originalmente por Laufer et al. [Laufer et al. 2005a] 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 Figura 3 – 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 pode terminar inesperadamente sem que seja completamente realizado ou gerar mensagens repetidas desnecessárias na rede.

No sistema proposto neste artigo, para se evitar problemas como o citado acima, antes do FBG ser preenchido com a marca de um roteador, é proposta uma marcação da seqüência dos roteadores dos SAs. A marcação da seqüência dos roteadores dos SAs 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 (*AS number* – 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 (possível causadora de *loops*) no momento da reconstrução do caminho reverso dos pacotes de ataque como discutido na Seção 3.4 ao descrevermos o processo de rastreamento de tráfego na rede sobreposta.

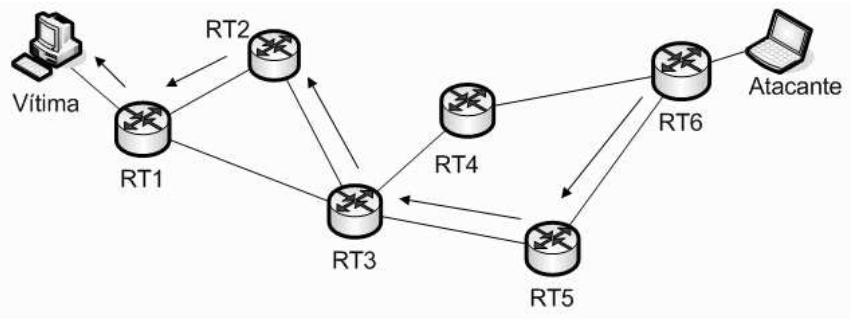

Figura 3. Problema de identificação de duas marcas no FBG.

3.4. Processo de rastreamento de tráfego

Um roteador de borda de um SA com o sistema proposto instalado que deseja realizar o rastreamento deve buscar 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.

O processo de rastreamento é ilustrado na Figura 4. 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* (ver Tabela 1) e assim constata que deve buscar no FGB pelas marcas de SA3 ou SA4, seus vizinhos na rede sobreposta (Figura 2). 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 o pacote de reconstrução de rota para SA4, 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. O mesmo processo é repetido no SA3 e termina quando o pacote de reconstrução de rota chega ao SA1 – neste caso, a origem do ataque está além do SA1. 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, 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 FGB auxilia a indicação da seqüência de roteadores pelos quais os pacotes de ataque passaram.

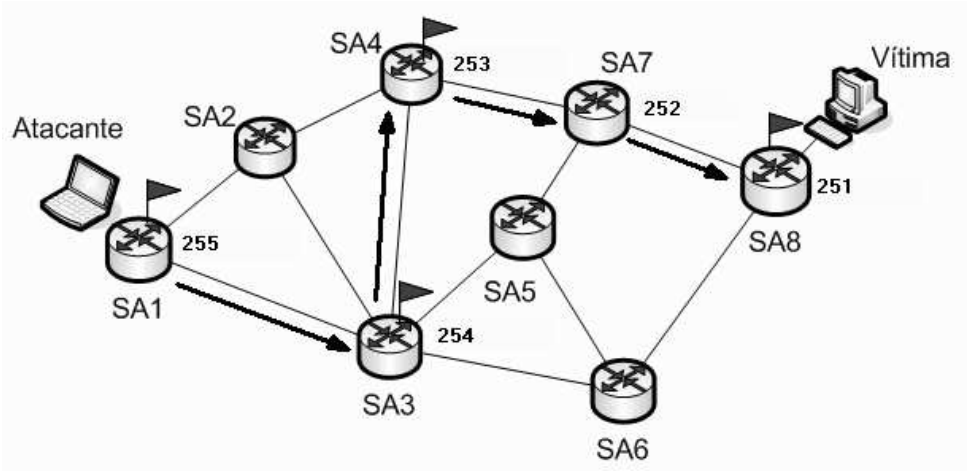

Figura 4. Funcionamento do processo de rastreamento.

Ao final do processo de rastreamento, os roteadores 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.

4. Avaliação da implementação parcial

Nesta seção, 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 et al. 1999, Medina et al. 2000], que mostram 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.

4.1. Configuração da simulação

Para executar as simulações, foi usado o gerador de topologia Nem [Magoni 2002] com o modelo Barabási-Albert [Albert e Barabasi 2000] e o simulador de rede NS-2 [Network Simulator 2 1995] modificado pelo módulo de simulação BGP++ [Dimitropoulos et al. 2006] (uma implementação do Zebra bgdp, que é uma implementação o protocolo de roteamento BGP para plataformas Unix).

Apresentamos neste artigo resultados para topologias de redes no nível de SAs contendo 900 SAs (resultados similares foram observados para topologias com 300 e 600 SAs). Para cada amostra, foram simulados sete diferentes topologias de rede com cinco conjuntos aleatórios de atacantes (10% de SAs, ou seja, 90 SAs no caso da topologia com 900 SAs) enviando tráfego para uma vítima. O propósito das simulações é analisar o desempenho da implementação parcial (e incremental) do sistema proposto. Em outras palavras, a intenção é avaliar a relação 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 implementação do sistema na rede. Os resultados das simulações representam valores médios, de $\pm 1.5\%$ para o posicionamento estratégico e $\pm 3.2\%$ para o posicionamento aleatório, com um intervalo de confiança de 99%. Como o intervalo de confiança observado foi bem pequeno, eles foram omitidos das figuras.

4.2. Resultados

Na Figura 5 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 usando o posicionamento estratégico, são descobertos quase 100% do caminho reverso dos ataques no nível de SAs com aproximadamente 70% dos SAs da rede com o sistema instalado. Por outro lado, para alcançar os mesmos resultados usando o posicionamento aleatório, o sistema deve estar instalado em quase 100% dos SAs da rede. 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 Figura 6 é observado que usando o posicionamento estratégico, para que o sistema descubra quase 100% dos SAs a 1 salto de distância do atacante, é necessário instalá-lo em aproximadamente 65% dos SAs da rede. Para conseguir estes resultados utilizando o posicionamento aleatório, aproximadamente 95% dos SAs devem ter o sistema de rastreamento instalado.

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.

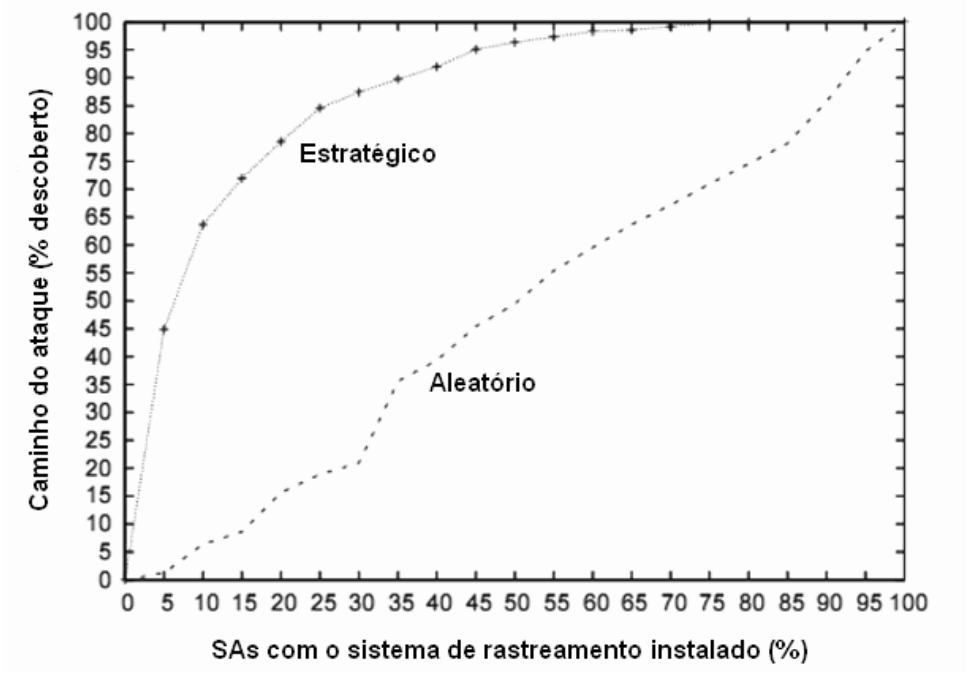

Figura 5. Descoberta do caminho de ataque.

Os resultados sugerem que se o sistema proposto for instalado estrategicamente em aproximadamente 40% 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 de similar a esta, o sistema de rastreamento proposto descobre aproximadamente 95% dos SAs a um salto do SA do atacante. Além disto, mesmo que uma quantidade pequena de SAs tenham o sistema instalado – em torno de 20% – o processo de rastreamento pode ainda sinalizar mais de 80% do caminho reverso do ataque, permitindo que medidas eficientes sejam tomadas de forma distribuída.

5. Conclusão

Neste artigo 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. Estas características permitem que o sistema seja instalado parcialmente e incrementalmente na rede, de forma independente da topologia, eliminando a necessidade da sua instalação em todos os roteadores da rede e o problema da exposição da topologia interna dos SAs, que fazem parte das desvantagens de outros sistemas de rastreamento.

O sistema de rastreamento de tráfego proposto neste artigo, 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, o que constitui um grande desafio para sua utilização em redes de larga escala como a Internet. Nos sistemas tradicionais, se os pacotes atravessam diferentes SAs, a origem do ataque dificilmente será encontrada pois

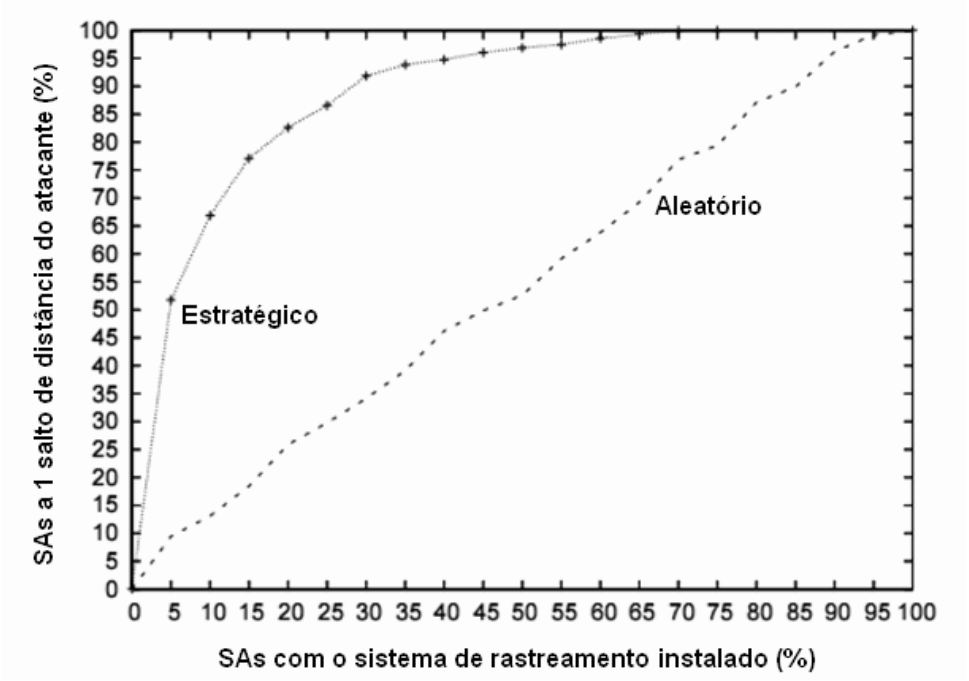

Figura 6. Descoberta do caminho de ataque – até um salto do SA do atacante.

o sistema deve ser instalado em todos os roteadores de todos os SAs por onde o pacote passa. Tipicamente, os operadores dos SAs não estão dispostos a aceitar a exposição da topologia interna da rede (mesmo que parcialmente) para outros SAs. Este problema é eliminado no sistema proposto, já que não existe a necessidade de fazer o rastreamento dentro da rede do SA. 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 para que tome providêncicas 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. Os resultados das simulações também 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.

6. Agradecimentos

Os autores gostariam de agradecer a Timothy G. Griffin (Universidade de Cambridge, Reino Unido), co-autor de [Agarwal e Griffin 2004], e Xenofontas Dimitropoulos (GeorgiaTech, EUA), autor de [Dimitropoulos et al. 2006], por fornecerem explicações detalhadas repectivamente sobre a operação do `Community Attribute` do BGP e a utilização do módulo de simulação BGP++. Este trabalho foi parcialmente financiado pela CAPES, CNPq e FAPERJ.

Referências

Agarwal, S. e Griffin, T. G. (2004). *BGP Proxy Community Community*. IETF Internet Draft.

Albert, R. e Barabasi, A.-L. (2000). Topology of evolving networks: local events and universality. *Physical Review Letters*, 85:5234.

Aljifri, H. (2003). IP traceback: A new denial-of-service deterrent? *IEEE Security and Privacy*, 1(3):24–31.

Belenky, A. e Ansari, N. (2003). On IP traceback. *IEEE Communications Magazine*, 41(7).

Bellovin, S., Leech, M., e Taylor, T. (2003). *ICMP Traceback messages*. IETF Internet Draft.

Bloom, B. (1970). Space/time tradeoffs in hash coding with allowable errors. *Communications of the ACM*, 13(7):422–426.

Broder, A. e Mitzenmacher, M. (2004). Network applications of Bloom filters: A survey. *Internet Mathematics*, 1(4):485–509.

Castelucio, A. O., Salles, R. M., e Ziviani, A. (2007). An AS-level IP traceback system. In *Proceedings of the 3rd International Conference on emerging Networking EXperiments and Technologies - CoNEXT'07*, New York, NY, USA. Poster.

Castelucio, A. O., Salles, R. M., e Ziviani, A. (2008). Evaluating the partial deployment of an AS-level IP traceback system. In *Proceedings of the ACM Symposium on Applied Computing – ACM SAC'08*, Fortaleza, Brasil.

CERT (1996). CERT Advisory CA-1996-21 TCP SYN flooding and IP spoofing attacks. Technical report, CERT- Computer Emergency Response Team.

CERT (2001). Denial of service attacks. Technical report, CERT- Computer Emergency Response Team.

Chandra, R., Traina, P., e Li, T. (1996). *BGP Communities Attribute*. Internet Engineering Task Force. RFC 1997.

Chen, E. e Bates, T. (1996). *An Application of the BGP Community Attribute in Multihome Routing*. Internet Engineering Task Force. RFC 1998.

Dimitropoulos, X., Verkaik, P., e Riley, G. (2006). BGP++ *http://www.ece.gatech.edu/research/labs/MANIACS/ BGP++* .

Durresi, A., Paruchuri, V., Barolli, L., Kannan, R., e Iyengar, S. S. (2004). Efficient and secure autonomous system based traceback. *Journal of Interconnection Networks*, 5(2):151–164.

Faloutsos, M., Faloutsos, P., e Faloutsos, C. (1999). On power-law relationships of the internet topology. In *SIGCOMM '99: Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication*, pág. 251–262, New York, NY, USA. ACM Press.

Hussain, A., Heidemann, J., e Papadopoulos, C. (2003). A framework for classifying denial of service attacks. In *SIGCOMM '03: Proceedings of the 2003 conference on*

Applications, technologies, architectures, and protocols for computer communications, pág. 99–110, New York, NY, USA. ACM Press.

Huston, G. (2004). *NOPEER Community for Border Gateway Protocol (BGP) Route Scope Control*. Internet Engineering Task Force. RFC 3765.

ISS (2000). Distributed denial of service attack tools. Technical report, ISS- Internet Security Systems.

Korkmaz, T., Gong, C., Sarac, K., e Dykes, S. (2007). Single packet IP traceback in AS-level partial deployment scenario. *International Journal of Security and Networks*, 2(1/2):95–108.

Krishnamurthy, B. (2004). Mohonk: mobile honeypots to trace unwanted traffic early. In *NetT '04: Proceedings of the ACM SIGCOMM workshop on Network troubleshooting*, pág. 277–282, New York, NY, USA. ACM Press.

Laufer, R. P., Velloso, P. B., de O. Cunha, D., Moraes, I. M., Bicudo, M. D. D., e Duarte, O. C. M. B. (2005a). A new IP traceback system against denial-of-service attacks. In *12th International Conference on Telecommunications - ICT'2005*, Capetown, South Africa.

Laufer, R. P., Velloso, P. B., e Duarte, O. C. M. B. (2005b). Generalized bloom filters, gta-05-43. Technical report, COPPE/UFRJ.

Magoni, D. (2002). Network manipulator. *https://dpt-info.u-strasbg.fr/ magoni/nem*.

Medina, A., Matta, I., e Byers, J. (2000). On the origin of power laws in internet topologies. *SIGCOMM Comput. Commun. Rev.*, 30(2):18–28.

Mirkovic, J. e Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *SIGCOMM Comput. Commun. Rev.*, 34(2):39–53.

Moore, D., Shannon, C., Brown, D. J., Voelker, G. M., e Savage, S. (2006). Inferring internet denial-of-service activity. *ACM Trans. Comput. Syst.*, 24(2):115–139.

Network Simulator 2 (1995). http://www.isi.edu/nsnam/ns.

NIST (2007). Guide to Intrusion Detection and Prevention Systems - (IDPS). Technical report, NIST- National Institute of Standards and Technology.

Quoitin, B. e Bonaventure, O. (2002). *A survey of the utilization of the BGP community attribute*. IETF Internet Draft.

Rekhter, Y. e Li, T. (1995). A border gateway protocol 4 (BGP-4). *RFC 1771*.

Rosen, E. e Rekhter, Y. (2006). *BGP/MPLS IP Virtual Private Networks (VPNs)*. Updated by RFCs 4577, 4684.

Savage, S., Wetherall, D., Karlin, A., e Anderson, T. (2000). Practical network support for IP traceback. In *Proceedings of the 2000 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM)*, pág. 295–306, Stockholm, Sweden.

Snoeren, A. C., Partridge, C., Sanchez, L. A., Jones, C. E., Tchakountio, F., Schwartz, B., Kent, S. T., e Strayer, W. T. (2002). Single-packet IP traceback. *IEEE/ACM Trans. Netw.*, 10(6):721–734.