Uma Técnica de Rastreamento sem Estado para Identificar a Origem de Ataques a Partir de um Único Pacote

Marcelo D. D. Moreira[1], **Rafael P. Laufer**[2], **Natalia C. Fernandes**[1] **e Otto Carlos M. B. Duarte**[1]

[1]GTA/PEE/COPPE, Universidade Federal do Rio de Janeiro

[2]University of California at Los Angeles

Abstract. *Anonymity is one of the main motivations for conducting denial-of-service attacks. Currently, there is no mechanism to either identify the true source of an IP packet or to prove its authenticity. In this paper we propose a stateless IP traceback technique that identifies the origin network of each individual packet. We show that the proposed traceback system is the only one that scales with the number of attackers and also satisfies practical requirements, such as no state stored at routers and a header overhead (25 bits) that can be allocated in IPv4 header. The proposed system exploits the customer-provider hierarchy of the Internet at autonomous system (AS) level and introduces the idea of checkpoints, which are the two most important nodes in an AS-level path. Simulation results using a real-world topology trace show that the proposed system narrows the source of an attack packet down to less than two candidate ASes on average. In addition, considering a partial deployment scenario, we show that the proposed system is able to successfully trace more than 90% of the attacks if only 8% of the ASes (i.e., just the core ASes) implement the system. The achieved success rate is quite better than using the classical hop-by-hop path reconstruction.*

Resumo. *O anonimato é uma das principais motivações para a realização de ataques de negação de serviço. Atualmente, não existe um mecanismo capaz de identificar a verdadeira origem de um pacote IP nem de provar sua autenticidade. Propõe-se neste trabalho uma técnica de rastreamento sem estado capaz de identificar a rede de origem de cada pacote individualmente. Mostra-se que o sistema de rastreamento proposto é o único escalável em relação ao número de atacantes e também satisfaz requisitos práticos, como nenhum estado armazenado nos roteadores da rede e uma sobrecarga de cabeçalho (25 bits) que pode ser alocada no cabeçalho IPv4. O sistema proposto explora a hierarquia cliente-provedor da Internet no nível de sistemas autônomos (ASes) e introduz a ideia de pontos de verificação, que são os dois nós mais importantes em um caminho de ASes. Resultados de simulação em uma topologia real mostram que o sistema proposto restringe o resultado da descoberta da origem de um pacote de ataque a menos de dois ASes candidatos na média. Além disso, considerando um cenário de implantação parcial, mostra-se que o sistema proposto é capaz de rastrear mais de 90% dos ataques com somente 8% dos ASes (isto é, só os ASes de núcleo) implementando o sistema. A taxa de sucesso obtida é bem melhor do que usando a clássica reconstrução de rota salto-a-salto.*

1. Introdução

Os ataques de negação de serviço distribuídos (*Distributed Denial-of-Service* - DDoS - *attacks*) são um dos principais desafios de segurança da Internet atualmente

[Laufer et al. 2005, Oliveira et al. 2007]. Os atacantes utilizam redes de ataque, chamadas de *botnets*, compostas por máquinas previamente comprometidas denominadas *bots* ou zumbis. Tipicamente, cada estação de ataque gera certa quantidade de tráfego em direção à vítima e o tráfego agregado é então responsável por exaurir os recursos da vítima, de forma a tornar indisponível o serviço oferecido. Os ataques de DDoS somente ocorrem porque os atacantes são capazes de avariar a vítima e ainda assim permanecer anônimos e, consequentemente, impunes [Ehrenkranz e Li 2009]. O protocolo IP não provê autenticação da origem dos pacotes, e assim pacotes com endereço de origem forjado podem ser injetados na rede. Tal vulnerabilidade é explorada pelos atacantes para garantir seu anonimato através da técnica de falsificação do endereço de origem. Um estudo recente [Ehrenkranz e Li 2009] mostra que aproximadamente 20% das redes da Internet permitem a falsificação do endereço de origem. Dentro de tais redes, uma estação pode forjar até 100% de todos os endereços da Internet. Portanto, não é possível *provar* a participação de uma estação em um ataque, ainda que as estações de ataque usem endereços de origem legítimos. Este trabalho visa preencher essa lacuna da arquitetura da Internet na área de responsabilização da origem [Andersen et al. 2008]. O escopo deste trabalho é a identificação da rede de origem de cada pacote IP recebido por uma estação da Internet.

Uma solução promissora para o problema de identificação da origem dos pacotes IP é tornar a rede capaz de rastrear o caminho seguido pelos pacotes até a estação que os enviou, o que é conhecido como o problema do rastreamento IP [Savage et al. 2001]. As técnicas de rastreamento podem ser divididas em duas classes: técnicas baseadas em marcação de pacotes e técnicas baseadas em auditoria [Laufer et al. 2005]. A ideia básica da marcação de pacotes é fazer com que cada roteador insira informações sobre si mesmo nos pacotes encaminhados. Assim, após receber pacotes suficientes, a vítima pode reconstruir a rota percorrida pelo pacote usando as informações fornecidas pelos roteadores. Já nos esquemas baseados em auditoria, os roteadores armazenam informações sobre os pacotes encaminhados. Dessa forma, a vítima pode consultar os roteadores para verificar se um dado pacote foi encaminhado recentemente pelo roteador consultado. No entanto, até o momento o rastreamento foi pensado somente como um primeiro passo para a defesa contra ataques de DDoS, e não como um mecanismo de identificação da origem de cada pacote. Uma das principais razões para isso é que a maioria dos sistemas de rastreamento requer pelo menos dezenas de pacotes recebidos da mesma origem para poder reconstruir a rota de ataque [Yaar et al. 2005]. Somente os esquemas baseados em auditoria e o esquema de marcação de pacotes proposto por Laufer *et al.* possuem a habilidade de rastrear o atacante a partir de um único pacote [Laufer et al. 2007]. Não obstante, nenhum desses esquemas atende a todos os requisitos que uma solução prática deve satisfazer. Os esquemas baseados em auditoria requerem armazenamento de estado por pacote na infraestrutura de rede, o que não é viável para redes de alta velocidade. Laufer *et al.* deram um passo adiante no desenvolvimento da abordagem de rastreamento por um único pacote ao introduzir o chamado Filtro de Bloom Generalizado (FBG). O FBG permite a reconstrução de rota a partir de um único pacote de forma robusta e eficiente sem armazenar nenhum estado na infraestrutura de rede. Porém, uma sobrecarga de cabeçalho de algumas centenas de bits é necessária para localizar o atacante de forma acurada [Laufer et al. 2007].

Ao que se sabe, o sistema proposto neste trabalho é a primeira proposta que permite a identificação da origem de um ataque a partir de um único pacote e também satisfaz requisitos práticos, como nenhum estado armazenado nos roteadores e uma sobrecarga de cabeçalho (25 bits) pequena o suficiente para poder ser alocada no cabeçalho

IPv4. Para permitir o rastreamento a partir de um único pacote com o pequeno espaço disponível no cabeçalho IP, considera-se o problema do rastreamento no nível de sistemas autônomos (*Autonomous Systems* - ASes). A estrutura hierárquica da Internet no nível de ASes é explorada para localizar o atacante usando a informação inserida pelos ASes atravessados pelo pacote. A novidade da proposta é escolher estrategicamente os ASes que marcam o pacote. Devido à restrição de espaço de cabeçalho, a rota de ataque completa não é transferida à vítima, mas somente a informação de rota que é essencial para localizar o atacante é armazenada no pacote. Dada uma rota em nível de ASes, foram identificados dois ASes, chamados de pontos de verificação (*checkpoints*), que são os mais importantes para reconstruir a rota de forma acurada. Propõe-se um esquema de marcação que privilegia estes dois nós críticos, permitindo rastrear o AS de origem com alta acurácia, a despeito da limitação de espaço para marcação. O sistema proposto é comparado com outros esquemas de marcação de pacotes [Durresi et al. 2009, Song e Perrig 2001, Belenky e Ansari 2007] através de um simulador desenvolvido para este trabalho. Os sistemas são comparados usando uma topologia real da Internet em nível de ASes construída a partir de dados de julho de 2009 da infraestrutura de medição Archipelago (Ark) [Hyun et al. 2009]. O resultado principal é que a taxa de erro do sistema de rastreamento proposto é independente do número de atacantes, o que mostra a escalabilidade da abordagem de rastreamento por um único pacote. Já os outros sistemas comparados, que dependem de múltiplos pacotes para reconstruir a rota de ataque, têm o desempenho bastante degradado com o aumento do número de atacantes, devido a erros de reconstrução que crescem rapidamente com o número de atacantes. Devido ao uso de pontos de verificação, além de constante, a taxa de erro do sistema proposto é bem baixa, pois na média têm-se apenas 0,8 falsos positivos para cada atacante rastreado.

Este artigo está organizado da seguinte forma. Na Seção 2 os trabalhos relacionados são apresentados e comparados com o sistema proposto qualitativamente. A Seção 3 introduz o problema da reconstrução de rota em nível de sistemas autônomos, servindo como base para a solução proposta, descrita na Seção 4. Os resultados de simulação são apresentados na Seção 5. Finalmente, a Seção 6 conclui este trabalho.

2. Trabalhos Relacionados

A solução mais simples para o problema de identificação da origem é evitar que pacotes com endereço de origem forjado atravessem a rede. Isso pode ser feito com técnicas de filtragem de pacotes, como a filtragem de ingresso [Ferguson e Senie 2000]. Essa técnica se baseia no fato de que pacotes com endereço forjado podem ser filtrados pelo roteador próximo à fonte de tráfego, bastando conhecer a faixa de endereços legítimos que podem chegar numa dada interface de rede. Assim, cada provedor de serviço (*Internet Service Provider* - ISP) filtra voluntariamente o tráfego com endereço de origem forjado originado de dentro de sua rede. A filtragem de ingresso, para ser efetiva, requer uma ampla implantação, mas não há nenhum benefício econômico para que um provedor de serviço passe a adotá-la. A adoção da filtragem de ingresso não se traduz em um incremento de segurança imediato para o ISP que a adotou. De fato, se existir um único ISP que não realiza filtragem de ingresso, as estações que pertencem à rede desse ISP podem forjar os endereços de outros ISPs, inclusive daqueles que implementam a filtragem de ingresso. Portanto, técnicas de filtragem são um mecanismo complementar e útil, mas não a solução completa para o problema.

O Passport [Liu et al. 2008] é um trabalho recente que tenta solucionar o problema de identificação da origem de pacotes IP usando autenticação criptográfica. O Passport funciona da seguinte maneira. Quando um pacote deixa o seu sistema autônomo (AS) de

origem, o roteador de borda insere uma lista de códigos de autenticação de mensagem (*Message Authentication Codes* - MACs) no cabeçalho do pacote. Cada MAC da lista é calculado usando uma chave secreta compartilhada entre o AS de origem e cada AS do caminho a ser percorrido pelo pacote. Em seguida, quando o pacote entra em um AS do caminho, o roteador de borda desse AS verifica o MAC correspondente usando a chave secreta compartilhada com o AS de origem. Um MAC correto só pode ser produzido pelo AS de origem, que conhece a chave secreta. Assim, o roteador de borda calcula o MAC e compara-o com o MAC contido no pacote. Se os MACs não forem iguais, é sinal de que o endereço de origem do pacote é forjado e o pacote pode ser descartado. Outra proposta baseada em criptografia é o AIP (*Accountable Internet Protocol*) [Andersen et al. 2008]. Esta é uma proposta de um novo protocolo de rede, em substituição ao IP, no qual os endereços são autocertificados, isto é, são derivados da chave pública da própria estação, podendo ser verificados por qualquer estação sem a necessidade de uma autoridade de certificação global. Apesar de oferecerem um alto grau de segurança, tanto o Passport quanto o AIP possuem limitações práticas que impedem a sua implantação imediata. O Passport possui uma sobrecarga de cabeçalho de 192 bits, que não podem ser alocados no cabeçalho IPv4. Os endereços autocertificados usados pelo AIP são também incompatíveis com a versão atual do IP. Além disso, cálculos de MACs por pacote exigem uma sobrecarga de processamento que limita a capacidade de encaminhamento a, no máximo, poucos gigabits por segundo, considerando o *hardware* dos roteadores atuais [Liu et al. 2008]. Finalmente, adicionar ao núcleo da rede funções restritivas, como a validação/filtragem dos endereços de origem, prejudica mecanismos importantes como a tradução de endereços de rede (*Network Address Translation* - NAT), o *proxying* e o IP móvel, que usam endereços de origem forjados para atividades benignas.

No presente trabalho, ao invés de usar primitivas criptográficas para autenticar o endereço de origem de pacotes IP, propõe-se o uso de um sistema de rastreamento para localizar a origem do pacote. O rastreamento IP possui diversas vantagens em relação à abordagem baseada em criptografia. Em primeiro lugar, a sobrecarga (*overhead*) de processamento e de cabeçalho é significativamente menor. A maioria dos sistemas de rastreamento usa apenas de 16 a 25 bits para armazenar eficientemente a informação de marcação em campos pouco usados do cabeçalho IP[1]. A sobrecarga de processamento dos algoritmos de marcação de pacotes é essencialmente mais simples do que o cálculo de assinaturas digitais ou de MACs. Além disso, os sistemas de rastreamento não desperdiçam o poder de processamento dos roteadores com a validação da origem de tráfegos legítimos,

[1]A informação de marcação poderia ser armazenada no campo de opções do IP, mas isso poderia levar à fragmentação do pacote, além de gerar uma sobrecarga de processamento elevada, visto que a adição de opções ao pacote obriga que o encaminhamento do pacote tenha um processamento mais lento (*slow path*). Outra possibilidade é enviar a informação de marcação em um pacote separado [Bellovin et al. 2003], mas isso adiciona ainda mais sobrecarga de processamento no roteador, reduz a banda disponível na rede e ainda existe o problema de como autenticar esses pacotes adicionais. Portanto, a solução mais eficiente é sobrecarregar campos poucos usados do cabeçalho IP, como o campo (de 16 bits) de identificação de fragmento, o campo (de 8 bits) de tipo de serviço (*Type of Service* - TOS), e o bit de fragmento reservado. Alguns estudos mostram que menos de 0,25% dos pacotes da Internet sofrem fragmentação [Dean et al. 2002]. Assim, o impacto negativo da adoção do sistema de rastreamento é pequeno quando comparado aos benefícios trazidos. Além disso, pode-se manter a compatibilidade com a fragmentação desde que a marcação seja a mesma para todos os fragmentos de um mesmo pacote. Assim, os fragmentos podem ser reagrupados no destino, visto que todos possuem o mesmo valor no campo de identificação de fragmento [Belenky e Ansari 2007]. O campo de tipo de serviço foi projetado para permitir o tratamento especial de tráfego, mas a atribuição de valores arbitrários a esse campo não produz nenhuma diferença na entrega de pacotes mensurável na prática. Sobrecarregar o bit de fragmento reservado também não causa nenhum efeito nas implementações atuais [Dean et al. 2002].

visto que o procedimento de reconstrução de rota é iniciado somente quando necessário.

Embora o rastreamento de pacotes IP apresente diversas vantagens sobre a abordagem baseada em criptografia, os sistemas de rastreamento propostos não servem como um mecanismo de identificação da origem de cada pacote. Conforme mostrado na Tabela 1, os sistemas existentes possuem uma ou mais das seguintes limitações: (i) exigência de múltiplos pacotes para ser capaz de reconstruir a rota de ataque, (ii) uso de uma sobrecarga de cabeçalho maior do que se pode alocar no cabeçalho IP e (iii) armazenamento de estado nos roteadores. Dentre os sistemas apresentados na tabela, por limitação de espaço, são descritos a seguir somente aqueles que são avaliados neste trabalho.

Tabela 1. Comparação dos sistemas de rastreamento.

	Pacotes exigidos	**Sobrecarga de cabeçalho**	**Estado nos roteadores**
Sistema proposto	1	25 bits	Sem estado
[Laufer et al. 2007]	1	192-256 bits	Sem estado
[Snoeren et al. 2002]	1	Nenhuma	Estado por pacote
[Choi e Dai 2004]	1	16 bits	12,5% dos pacotes
[Gao e Ansari 2007]	6-9	32 bits	Sem estado
[Durresi et al. 2009]	8-10	25 bits	Sem estado
[Belenky e Ansari 2007]	55-130	17 bits	Sem estado
[Bellovin et al. 2003]	Dezenas	Nenhuma	Sem estado
[Yaar et al. 2005]	10-1000	16 bits	Sem estado
[Dean et al. 2002]	Milhares	25 bits	Sem estado
[Song e Perrig 2001]	500-2000	16 bits	Sem estado
[Savage et al. 2001]	1000-8000	16 bits	Sem estado

Song e Perrig propuseram o uso do mapa da topologia para auxiliar o rastreamento. Dessa forma, a rota de ataque é reconstruída a partir de uma busca no grafo que representa a topologia de rede [Song e Perrig 2001]. No esquema de Song e Perrig, a marcação inserida por cada roteador no pacote é o *hash* do endereço IP do roteador. Isto permite compactar os 32 bits do endereço IP em um identificador de tamanho fixo, de 8 bits neste caso. Dessa forma, durante a reconstrução de rota, a marcação inserida no pacote é comparada com o *hash* do endereço IP do roteador que está sob teste. Chama-se de grafo de reconstrução, o grafo resultante da incorporação dos roteadores identificados pelo procedimento de reconstrução de rota. Durante o procedimento de reconstrução de rota, um roteador que não pertence à rota percorrida pelo pacote pode ser incorretamente integrado ao grafo de reconstrução. Esse tipo de erro é chamado de *falso positivo*.

Belenky e Ansari observaram que, sendo o objetivo final a identificação do atacante e não da rota completa de ataque, somente o primeiro roteador da rota de ataque precisa marcar o pacote [Belenky e Ansari 2007]. Assim, a proposta é que o roteador mais próximo do atacante insira no pacote o endereço IP da sua interface de entrada. Como os 32 bits do endereço IP não cabem dentro do espaço disponível para marcação, o endereço IP é dividido em k fragmentos de endereço. Ao marcar o pacote, o roteador escolhe aleatoriamente um dos k fragmentos e o insere no pacote. Após o recebimento de todos os fragmentos, a vítima pode recuperar o endereço do primeiro roteador, bastando agrupar corretamente os fragmentos de endereço recebidos. No restante deste trabalho, considera-se $k = 4$.

Durresi *et al.* propuseram o FAST (*Fast Autonomous System Traceback*), um sistema de rastreamento inter-domínio no qual os 5 primeiros ASes da rota de ataque mar-

cam o pacote [Durresi et al. 2009]. O espaço de marcação é dividido em 5 subcampos para acomodar as 5 marcações permitidas. Um contador também é carregado no pacote para informar qual subcampo um AS deve marcar. A marcação é feita pelo roteador de borda de cada AS. Para notificar a vítima sobre a presença do AS na rota de ataque, é usado o identificador de AS no roteamento inter-domínio, chamado de número de AS (*AS number* - ASN). Ao marcar o pacote, o roteador de borda do AS insere o *hash* do ASN correspondente. Assim como o sistema de Song e Perrig, o FAST realiza uma busca no grafo que representa a topologia de rede para reconstruir a rota de ataque.

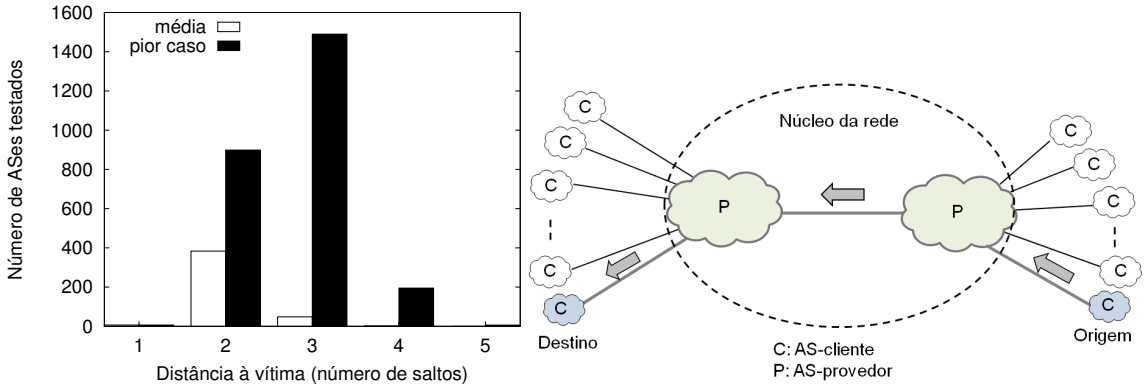
Os sistemas mencionados nesta seção dependem do recebimento de múltiplos pacotes para serem capazes de reconstruir a rota percorrida pelos pacotes. Por essa razão, eles não podem ser usados como um mecanismo de identificação da origem de cada pacote individualmente. Além disso, a distribuição das marcações por múltiplos pacotes implica um rápido crescimento da taxa de falsos positivos conforme o número de atacantes aumenta. Quando há vários atacantes, durante o procedimento de reconstrução de rota, a vítima acredita que pacotes de origens distintas pertencem à mesma rota de ataque, causando imprecisões graves, conforme mostram os resultados da Seção 5. Em comparação, a proposta deste trabalho é capaz de rastrear um número ilimitado de atacantes com menos de um falso positivo por atacante, usando apenas um único pacote recebido.

3. Reconstrução de Rota em Nível de Sistemas Autônomos

O rastreamento inter-domínio possui algumas vantagens sobre o rastreamento em nível de roteadores. Os caminhos em nível de ASes são cerca de 5 vezes menores que do em nível de roteadores e o número de ASes (aproximadamente 45 mil) é bem menor do que o número de roteadores (da ordem de dezenas de milhões). Apesar dessas vantagens, o rastreamento inter-domínio apresenta um novo desafio: lidar com uma estrutura altamente hierárquica. Isto leva a pontos de divergência do procedimento de reconstrução de rota, que podem comprometer a acurácia do sistema de rastreamento, conforme mostrado a seguir.

A Fig. 1(a) mostra o número de ASes testados pelo procedimento de reconstrução de rota de acordo com a distância em número de saltos. Nota-se que, dependendo da distância à vítima, o número de ASes que devem ser testados durante o procedimento de reconstrução de rota varia significativamente. Tal comportamento pode ser explicado pela distribuição do número de vizinhos dos ASes, que segue uma lei de potência [Mahadevan et al. 2006]. A maioria dos ASes possui poucos vizinhos e está localizada na borda da rede, enquanto que alguns poucos ASes possuem um elevado número de vizinhos e estão localizados no núcleo da rede. Logo, quando o procedimento de reconstrução de rota é iniciado pela vítima, há poucos vizinhos a serem testados, visto que se está ainda na borda da rede. Quando se aumenta a distância à vítima, avançando em direção ao núcleo da rede, o número de vizinhos testados aumenta. Da mesma forma, caso se continue a aumentar a distância à vítima, a borda da rede é atingida novamente e, consequentemente, o número de ASes testados diminui, conforme ilustrado na Fig. 1(a). Esse comportamento é um reflexo da hierarquia cliente-provedor que existe na topologia da Internet em nível de ASes. A relação cliente-provedor é fruto de relações comerciais entre os ASes: um AS-cliente paga ao seu AS-provedor para que este transporte tráfego de/para o AS-cliente. Em geral, um mesmo AS-provedor possui diversos ASes-clientes, formando o que se chama de hierarquia cliente-provedor. Tal hierarquia é claramente vista nas características dos caminhos em nível de ASes: 62% dos caminhos possuem comprimento de 3 saltos [Mahadevan et al. 2006]. No padrão de caminho mais comum, mostrado na Fig. 1(b), o pacote é originado em um AS-cliente, na borda da rede, sobe para o prove-

dor do AS de origem, entrando no núcleo da rede, depois vai para outro AS-provedor e finalmente chega ao seu destino, geralmente um AS-cliente localizado na borda da rede.



(a) Números de testes na reconstrução de rota. (b) A hierarquia cliente-provedor em nível de ASes.

Figura 1. A reconstrução de rota em nível de ASes.

De acordo com as Figs. 1(a) e 1(b), os passos críticos durante a reconstrução de rota em nível de ASes ocorrem no segundo e terceiro saltos, nos quais devem ser testados até 898 e 1490 ASes, respectivamente. Há muitos ASes a serem testados devido à concentração de caminhos que passam pelos grandes provedores, chamados de ASes de núcleo. Metade dos caminhos da Internet passam pelos 10 ASes com mais de 500 vizinhos [Mahadevan et al. 2006]. Assim, partindo da vítima em direção ao atacante, o procedimento de reconstrução consegue identificar o provedor da vítima, entrando no núcleo da rede sem muitas dificuldades. Porém, para identificar o primeiro sistema autônomo (AS) de núcleo atravessado pelo pacote de ataque, é preciso testar quase mil ASes vizinhos, o que pode resultar em uma elevada taxa de falsos positivos. Por essa razão, o primeiro passo crítico é a identificação do primeiro AS de núcleo da rota de ataque. O segundo passo crítico ocorre quando o procedimento de reconstrução alcança o provedor do AS-atacante e está tentando localizar o AS-atacante. Este é também um passo crítico, porque o atacante deve ser identificado dentre aproximadamente mil ASes.

4. O Sistema Proposto

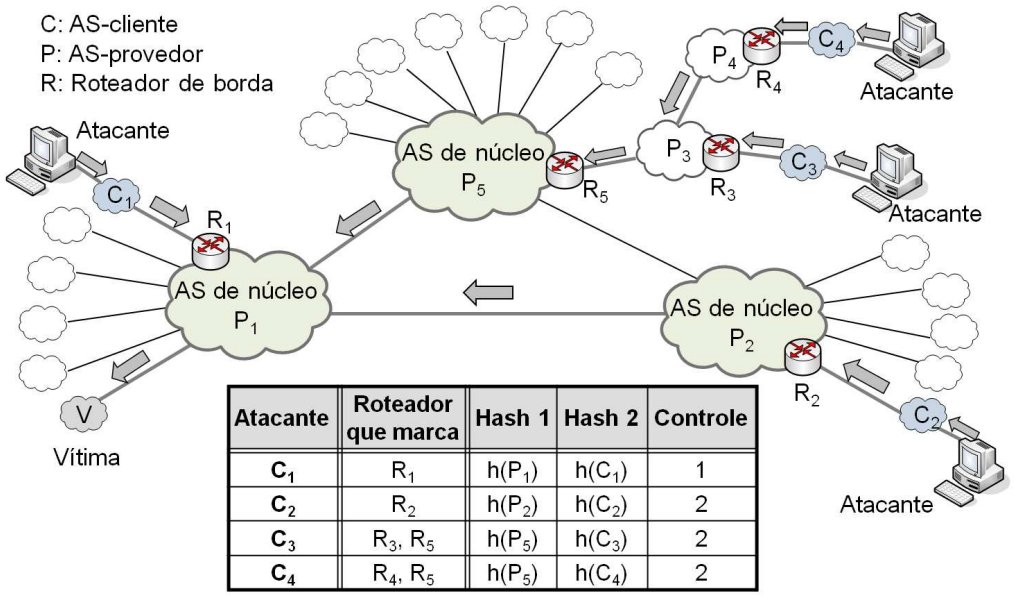
Assim como Castelucio *et al.*, propõe-se o uso do protocolo de roteamento interdomínio BGP (*Border Gateway Protocol*) como o veículo de distribuição da informação de implantação do sistema [Castelucio et al. 2009]. Os ASes cooperativos, isto é, os ASes que têm o sistema implantado, anunciam o suporte ao rastreamento em um atributo do BGP nos anúncios de rota. Assim, é formada uma rede sobreposta composta pelos ASes cooperativos, de forma que um dado AS é capaz de determinar se ele é o primeiro AS cooperativo de um dado caminho ou não[2]. A seguir, são descritos os procedimentos de marcação de pacotes e reconstrução de rota do sistema proposto.

4.1. Procedimento de Marcação de Pacotes

Observando a existência de dois passos críticos durante a reconstrução de rota, propõe-se um novo esquema de marcação de pacotes no qual somente dois ASes marcam

[2]Uma vez que se conhece o primeiro AS cooperativo de um dado caminho, então uma solução simples para identificar a origem dos pacotes seria fazer com que este primeiro AS inserisse o seu ASN (*AS number*) no pacote. Porém, o tamanho dos ASNs aumentou recentemente de 16 para 32 bits [Huston 2009], o que não cabe dentro do espaço disponível para marcação no cabeçalho IPv4.

o pacote. Essas duas marcações são usadas como pontos de verificação (*checkpoints*) para guiar o procedimento de reconstrução de rota. Os pontos de verificação são estrategicamente posicionados no AS-atacante e no primeiro AS de núcleo da rota de ataque. Assim, em vez de representar a rota de ataque completa, propõe-se marcar apenas alguns ASes e, com isto, alocam-se mais bits do cabeçalho IP para os passos críticos, garantindo que os pontos de verificação sejam alcançados com uma baixa taxa de falsos positivos. Para armazenar as marcações, propõe-se sobrecarregar 25 bits do cabeçalho IPv4. Os campos sobrecarregados são subdivididos em três campos. Dois campos, denominados `Hash 1` e `Hash 2`, de 11 e 12 bits, respectivamente, são usados para acomodar as marcações dos dois ASes que marcam o pacote. É usado também um campo `Controle`, de 2 bits, para indicar se algum AS de núcleo já marcou o pacote e também para carregar a distância entre o primeiro AS de núcleo da rota de ataque e a vítima.



Atacante	Roteador que marca	Hash 1	Hash 2	Controle
C_1	R_1	$h(P_1)$	$h(C_1)$	1
C_2	R_2	$h(P_2)$	$h(C_2)$	2
C_3	R_3, R_5	$h(P_5)$	$h(C_3)$	2
C_4	R_4, R_5	$h(P_5)$	$h(C_4)$	2

Figura 2. Procedimento de marcação dos pacotes de ataque originados nos ASes-clientes C_1, C_2, C_3, e C_4.

A Fig. 2 ilustra o funcionamento do procedimento de marcação. A figura apresenta quatro exemplos de ataque, com diferentes tamanhos de rota. Em todos os exemplos, foi considerado que os ASes-clientes não são cooperativos, a fim de mostrar que o procedimento proposto não precisa que o AS-cliente e o seu provedor sejam ambos cooperativos. A rota de ataque mais curta é (C_1, P_1, V). Neste exemplo, o pacote de ataque é originado no AS-cliente C_1, sobe para o AS-provedor P_1, que é um AS de núcleo, e então alcança a vítima V. O procedimento de marcação determina, em primeiro lugar, que o roteador de borda do primeiro AS cooperativo da rota de ataque, R_1 neste exemplo, zere todos os campos de marcação a fim de evitar qualquer interferência da condição inicial do pacote, determinada pelo atacante, durante a reconstrução de rota. Em seguida, R_1 deve inserir o *hash* de $ASN_{AS\,origem}$, que neste caso é $h(C_1)$, no campo `Hash 2`. A segunda marcação é feita pelo primeiro AS de núcleo atravessado pelo pacote, que neste exemplo também é P_1. Por essa razão, R_1 insere $h(P_1)$ no campo `Hash 1`. R_1 também insere a distância de P_1 até a vítima V, que é 1 salto neste exemplo, no campo `Controle`[3]. Outro exem-

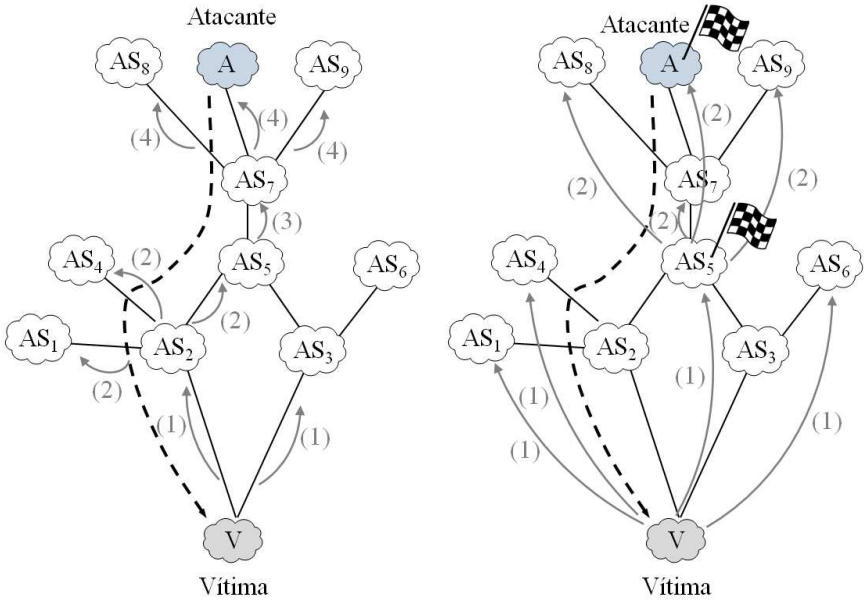
[3]A distância até a vítima pode ser calculada contando o número de elementos do atributo do BGP chamado AS_PATH [Gao e Ansari 2007], que fornece a lista de ASes que precisam ser atravessados para chegar a um dado destino.

plo de rota de ataque é (C_2, P_2, P_1, V). Novamente, o primeiro AS cooperativo, P_2, é também o primeiro AS de núcleo da rota de ataque. Portanto, o roteador de borda de P_2, R_2, insere $h(P_2)$ e $h(C_2)$ nos campos `Hash 1` e `Hash 2`, respectivamente. O valor 2 é inserido no campo `Controle`, pois a distância entre P_2 e V é de 2 saltos. Após deixar P_2, o pacote chega a P_1, que também é um AS de núcleo. Assim, P_1 analisa o valor do campo `Controle`. P_1 então verifica que este valor é diferente de 0 e conclui que algum AS de núcleo já marcou o pacote. Por isso, P_1 simplesmente encaminha o pacote até a vítima, sem fazer nenhuma modificação. O terceiro exemplo de rota de ataque é (C_3, P_3, P_5, P_1, V). Neste caso, o primeiro AS cooperativo é P_3. Logo, R_3 insere $h(C_3)$ no campo `Hash 2`. Em seguida, o pacote chega ao primeiro AS de núcleo, P_5. Assim, o roteador de borda de P_5, R_5, marca o pacote com $h(P_5)$, inserindo este valor no campo `Hash 1`, e atualiza o campo `Controle` com a sua distância até V, que é 2 neste caso. O pacote é então encaminhado ao AS de núcleo P_1, que não faz nada, visto que o valor do campo `Controle` é diferente de 0. Finalmente, o pacote chega à vítima. O último exemplo é de uma rota de ataque de 5 saltos: $(C_4, P_4, P_3, P_5, P_1, V)$. Nesse caso, o primeiro AS cooperativo é P_4. Dessa forma, R_4 insere $h(C_4)$ no campo `Hash 2`. O pacote é então encaminhado para P_3, que não é o primeiro AS cooperativo nem o primeiro AS de núcleo desse caminho. Portanto, P_3 não insere marcação alguma. A seguir, o pacote chega ao primeiro AS de núcleo, que é P_5. Assim, o roteador de borda R_5 marca o pacote com $h(P_5)$ e atualiza o campo `Controle` com sua distância até V, que é 2. O pacote segue então para P_1, que simplesmente o encaminha para a vítima.

4.2. Procedimento de Reconstrução de Rota

Após o recebimento do pacote contendo as marcações, a vítima pode iniciar o procedimento de reconstrução de rota. O procedimento proposto se difere do procedimento clássico de reconstrução salto-a-salto, conforme mostrado na Fig. 3. A figura mostra um exemplo de reconstrução da rota, considerando a rota de ataque (A, AS_7, AS_5, AS_2, V). No procedimento clássico de reconstrução de rota salto-a-salto, conforme ilustrado na Fig. 3(a), a vítima testa em primeiro lugar os ASes que estão a um salto de distância (AS_2 e AS_3). No exemplo, considerando que o AS_3 não é um falso positivo, então somente o AS_2 é reconhecido. No próximo passo do procedimento, os ASes do segundo salto, AS_1, AS_4 e AS_5, são testados. Somente o AS_5 é identificado. A seguir, os ASes do terceiro salto são testados. No exemplo, o AS_7 é testado e em seguida integrado ao grafo de reconstrução. Apesar de o AS_3 ser vizinho do AS_5, o AS_3 não é testado, pois a sua distância à vítima (1 salto) é menor ou igual à distância do AS_5. É usado o algoritmo de busca em largura para a reconstrução de rota. Finalmente, os ASes do quarto salto, AS_8, A e AS_9, são testados e o atacante A é então encontrado. Por outro lado, o procedimento proposto (Figura 3(b)) pula alguns passos do procedimento clássico e realiza testes somente em pontos estratégicos, onde estão posicionados os pontos de verificação. Assim, o procedimento proposto pula o primeiro salto e testa diretamente os ASes localizados a d (no exemplo, $d = 2$) saltos da vítima, onde d, a distância da vítima até o último AS que marcou o pacote, é o conteúdo do campo `Controle` do pacote recebido pela vítima. No exemplo, os ASes testados no primeiro passo são AS_1, AS_4, AS_5 e AS_6. Nesse momento, o ponto de verificação, que nada mais é do que a marcação contida no pacote recebido pela vítima, é usado para identificar o AS correto, AS_5, com alta acurácia. No passo seguinte do procedimento proposto, todos os ASes ascendentes do AS_5 (AS_7, AS_8, A e AS_9) são testados. Após o teste do segundo ponto de verificação, o atacante A é finalmente encontrado. Nota-se que o procedimento de reconstrução sempre encontra o AS-atacante, desde que sua marcação conste no pacote recebido. De acordo com o procedimento de marcação proposto, esta condição é satisfeita se o AS-atacante ou seu

provedor for cooperativo.



(a) Procedimento salto-a-salto. (b) Procedimento proposto.

Figura 3. Reconstrução da rota de ataque (A, AS_7, AS_5, AS_2, V)**.**

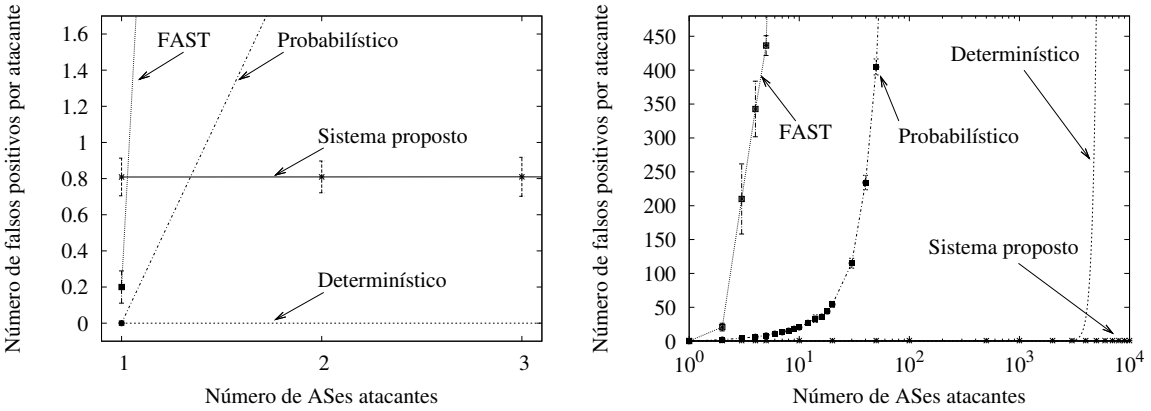
5. Resultados de Simulação

Foi desenvolvido um simulador próprio para analisar o desempenho do sistema proposto. Foi usada uma topologia real da Internet em nível de ASes, obtida em julho de 2009 a partir de dados de medição do projeto Ark (*Archipelago*) [Hyun et al. 2009], composta por 16.352 ASes e 39.346 enlaces[4]. O ataque de negação de serviço distribuído, a marcação de pacotes e a reconstrução de rota são simulados da seguinte maneira. Em primeiro lugar, escolhe-se aleatoriamente a vítima a partir do conjunto de nós da topologia. Em seguida, são definidas as rotas de ataque, que são caminhos sem ciclos que terminam na vítima escolhida. A transmissão dos pacotes de ataque é simulada inserindo-se as marcações apropriadas nos campos de marcação de acordo com os ASes que compõem cada rota de ataque. Uma vez que os pacotes são marcados, o procedimento de reconstrução é iniciado a partir da vítima. Para cada resultado medido, foi calculado um intervalo de confiança de 95%, representado nos gráficos por barras de erro verticais.

Foram implementados no simulador o sistema inter-domínio FAST e o sistema probabilístico de Song e Perrig. Além disso, a fim de comparar também com um sistema determinístico, é apresentada no gráfico a expressão analítica do número esperado de falsos positivos do sistema de Belenky e Ansari. Ao contrário do sistema proposto, esses sistemas não seguem a abordagem de rastreamento por um único pacote. Dessa forma, os ataques simulados foram compostos por um número suficiente de pacotes para cada sistema funcionar adequadamente, isto é, 10 pacotes para o FAST [Durresi et al. 2009], 55 para o sistema determinístico [Belenky e Ansari 2007] e 1.000 para o sistema probabilístico [Song e Perrig 2001]. Com isso, a vítima recebe todas as possíveis marcações

[4]As medições do projeto Ark são feitas através de *traceroutes* sucessivos e, portanto, são capturados os caminhos realmente utilizados, o que explica o fato de o número de ASes da topologia obtida ser menor do que o total de ASNs registrados (aproximadamente 45 mil) [Huston 2009].

de cada roteador das rotas de ataque. Isto representa o melhor cenário possível para os sistemas comparados em termos de número de falsos positivos obtidos.



(a) Acurácia com poucos atacantes. (b) Acurácia com diversos atacantes.

Figura 4. Acurácia dos sistemas avaliados, medida em número de falsos positivos por atacante, em função do número de ASes-atacantes.

Os resultados de simulação da acurácia em função do número de atacantes são mostrados na Fig. 4. A acurácia é medida em termos do número de falsos positivos. Um sistema de rastreamento ideal encontra o AS-atacante sem nenhum falso positivo durante a reconstrução de rota. Assim, quanto menor o número de falsos positivos, melhor a acurácia com que o AS-atacante é identificado. O gráfico da Fig. 4(a) mostra a acurácia medida em um cenário com poucos ASes-atacantes. Observa-se que, quando há apenas um AS-atacante, todos os sistemas comparados obtêm um número de falsos positivos menor do que o do sistema proposto. Isto era de se esperar, visto que o FAST, o sistema probabilístico e o sistema determinístico tiram proveito dos múltiplos pacotes de ataque, enquanto que o sistema proposto só pode contar com a informação de um único pacote de ataque. Porém, mesmo com um pequeno aumento do número de ASes-atacantes, os sistemas FAST e probabilístico já ultrapassam o sistema proposto no número de falsos positivos. Com mais de um AS-atacante, tais sistemas começam a ter problemas com erros de reconstrução devido à combinação incorreta das marcações recebidas por diferentes caminhos de ataque. Este problema se agrava com o aumento do número de ASes-atacantes, conforme fica claro no gráfico da Fig. 4(b). Mesmo o sistema determinístico, que com poucos atacantes mantinha uma taxa de falsos positivos baixa, passa a ter o número de falsos positivos crescendo rapidamente com o número de ASes-atacantes a partir da ordem de milhares de ASes-atacantes. O sistema proposto, por outro lado, só depende de um único pacote para rastrear cada AS-atacante e, consequentemente, não possui o problema da combinação incorreta das marcações recebidas por diferentes caminhos de ataque. Este fato fica evidente no gráfico, que mostra que o sistema proposto é escalável com relação ao número de ASes-atacantes, pois a acurácia obtida é constante em relação ao número de atacantes. Além disso, observa-se que o número de falsos positivos é de fato bem pequeno, apenas 0,8 falsos positivos por atacante.

Foi também avaliado o efeito do tamanho da rota de ataque e da topologia na acurácia do sistema proposto, conforme mostrado na Fig. 5. A Fig. 5(a) mostra o comportamento da acurácia do sistema proposto em relação ao tamanho da rota de ataque. Observa-se no gráfico que o número de falsos positivos é maior para rotas de ataques maiores. Isto ocorre porque, para uma rota maior, mais ASes devem ser testados pelo procedimento de reconstrução de rota, especialmente no segundo passo do algoritmo, no

qual são testados todos os ASes ascendentes do AS identificado no primeiro passo. No entanto, mesmo o valor máximo obtido, 1,8 falsos positivos por atacante, é considerado baixo quando comparado ao número de falsos positivos obtidos pelos outros sistemas de rastreamento. Além disso, esse valor máximo não deve aumentar com o crescimento da topologia em nível de ASes. Apesar de o número de ASes aumentar no futuro, não é esperado um aumento significativo no diâmetro da rede e no tamanho das rotas em nível de ASes com o passar do tempo [Andersen et al. 2008]. Os resultados da Fig. 5(b) confirmam esta previsão. A Fig. 5(b) mostra o número de falsos positivos em função do tamanho da topologia, medido pelo número total de nós da topologia. Observa-se que o FAST é o sistema menos escalável com relação ao tamanho da topologia, mesmo considerando um percentual ASes-atacantes de apenas $\alpha = 0,01\%$. Para este mesmo percentual, o sistema probilístico escala quase que tão bem como o sistema proposto. Porém, pela curva com 0,05% de ASes-atacantes, percebe-se que o sistema probabilístico já não escala tão bem, pois a faixa de atacantes passou de [2,10] para [10,50], o que já implica um elevado número de falsos positivos. Em comparação, o sistema proposto se mostra escalável quanto ao número de nós da topologia e esta propriedade é independente do percentual de ASes-atacantes. A razão para a escalabilidade em relação ao número de nós da topologia é que o sistema proposto explora a hierarquia cliente-provedor, o que não é feito pelos demais sistemas da literatura. Essa propriedade é importante, pois os estudos mostram um crescimento exponencial do número de ASes. É esperado que se atinja o número de 100 mil ASNs alocados em 2015 [Huston 2009].

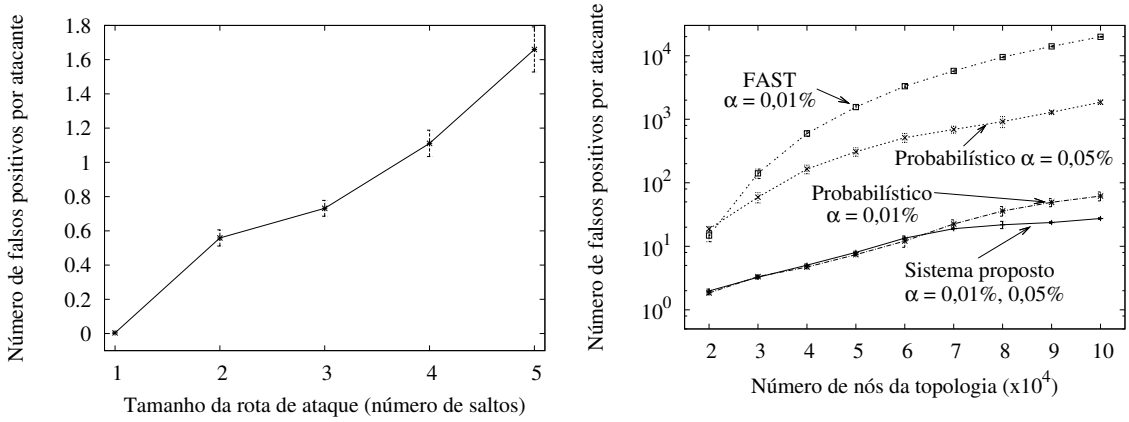
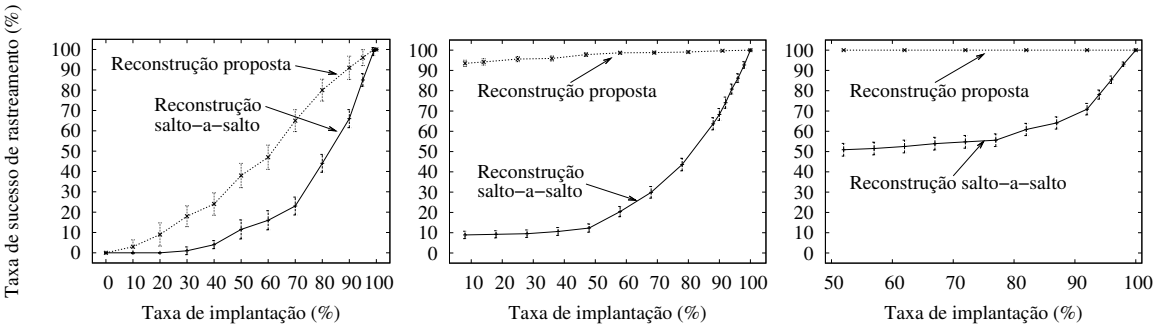


Figura 5. Acurácia em função do tamanho da rota e da topologia. O comportamento do sistema proposto independe do percentual de ASes-atacantes (α).

Foi avaliada também a taxa de sucesso de rastreamento, definida como o percentual de casos nos quais o atacante é encontrado, em função da taxa de implantação do sistema, conforme mostra a Fig. 6. Na Fig. 6(a), considera-se uma distribuição aleatória dos ASes cooperativos. Observa-se neste caso que o procedimento de reconstrução de rota proposto obtém uma taxa de sucesso sempre melhor do que o procedimento de reconstrução salto-a-salto. O fato de o procedimento proposto pular alguns passos da reconstrução salto-a-salto torna o procedimento proposto capaz de encontrar o atacante mesmo que algum AS da rota de ataque não seja cooperativo. Por outro lado, a reconstrução salto-a-salto é interrompida logo no primeiro AS não cooperativo encontrado durante o procedimento de reconstrução. Nota-se que a curva da reconstrução proposta se aproxima da função identidade, o que mostra que o procedimento proposto consegue aproveitar ao máximo os ASes que são cooperativos, encontrando-os quase todos. Na Fig. 6(b) foi simulado um cenário no qual os ASes de núcleo são cooperativos e os demais ASes seguem uma distribuição aleatória de implantação. Como ASes de núcleo foram considerados os

ASes que possuem 7 ou mais vizinhos, o que representa cerca de 8% dos ASes da topologia utilizada. É interessante observar que o procedimento de reconstrução proposto consegue rastrear mais de 90% dos ASes, com apenas 8% de taxa de implantação. Além disso, com 60% de implantação, a reconstrução proposta encontra 100% dos atacantes. A explicação para isso é que, uma vez encontrado o primeiro AS de núcleo da rota de ataque, basta que o AS-atacante ou o seu provedor seja cooperativo que o procedimento de reconstrução obtém sucesso. Em contrapartida, o procedimento salto-a-salto, para taxas de implantação de 10 a 50%, encontra somente cerca de 10% dos atacantes, pois este procedimento só obtém sucesso no rastreamento quando as rotas são compostas exclusivamente por ASes cooperativos. Por fim, o gráfico da Fig. 6(c) mostra o caso no qual todos os ASes não-clientes são cooperativos e os ASes clientes seguem uma distribuição aleatória de implantação. Com ASes não-clientes foram considerados os ASes que possuem 2 ou mais vizinhos, o que representa cerca de 52% dos ASes da topologia utilizada. Neste cenário, a reconstrução proposta sempre encontra o AS-atacante, independentemente da taxa de implantação dos ASes-clientes, desempenhando novamente bem melhor do que a reconstrução salto-a-salto, que é a mais comum na literatura.



(a) Distribuição aleatória. (b) ASes de núcleo + aleatória. (c) ASes não-clientes + aleatória.

Figura 6. Taxa de sucesso de rastreamento em função do percentual de ASes cooperativos para diferentes distribuições de implantação.

6. Conclusões

Mostra-se nesse trabalho que a abordagem de rastreamento por um único pacote permite a identificação da origem de cada pacote IP individualmente, sem armazenar estado na infraestrutura de rede. Para superar o desafio de armazenar a rota completa de ataque no espaço disponível no cabeçalho de um único pacote, propõe-se explorar a estrutura hierárquica da Internet no nível de sistemas autônomos (ASes). É analisado o problema da reconstrução de rotas na Internet no nível de ASes e são obtidas duas descobertas principais: (i) é mostrado que a hierarquia cliente-provedor implica a existência de dois passos críticos durante o procedimento de reconstrução de rota; e (ii) nota-se que o AS de origem pode ser sempre encontrado, mesmo que alguns ASes não participem da marcação de pacotes. Baseando-se nessas duas observações, propõe-se um novo esquema de rastreamento que privilegia os passos críticos da reconstrução de rota e dispensa os ASes-clientes da tarefa de marcar pacotes. O resultado é que, com somente duas marcações, o AS de origem é encontrado com alta acurácia, a despeito da limitação de espaço disponível para marcação no cabeçalho IPv4. O desempenho do sistema proposto é avaliado numa topologia real e os resultados de simulação confirmam a alta escalabilidade e excelente acurácia do sistema proposto. O sistema é capaz de rastrear um número ilimitado de atacantes com menos de 1 falso positivo por atacante. O procedimento de reconstrução proposto consegue rastrear mais de 90% dos ASes, considerando o caso no

qual apenas os ASes de núcleo participam da marcação, o que equivale a cerca de 8% de taxa de implantação do sistema no cenário de simulação considerado.

Agradecimentos

Este trabalho foi financiado com recursos do CNPq, CAPES, FINEP, FUNTTEL e FAPERJ.

Referências

Andersen, D. G., Balakrishnan, H., Feamster, N., Koponen, T., Moon, D. e Shenker, S. (2008). Accountable Internet protocol (AIP). Em *ACM Special Interest Group on Data Communication*, páginas 339–350.

Belenky, A. e Ansari, N. (2007). On Deterministic Packet Marking. *Computer Networks*, 51(10):2677–2700.

Bellovin, S. M., Leech, M. D. e Taylor, T. (2003). ICMP Traceback Messages. *Internet Draft: draft-ietf-itrace-04.txt*.

Castelucio, A., Ziviani, A. e Salles, R. M. (2009). An AS-level Overlay Network for IP Traceback. *IEEE Network*, 23(1):36–41.

Choi, K. H. e Dai, H. K. (2004). A Marking Scheme Using Huffman Codes for IP Traceback. *IEEE ISPAN*, 00:421–428.

Dean, D., Franklin, M. e Stubblefield, A. (2002). An Algebraic Approach to IP Traceback. *ACM Transactions on Information and System Security*, 5(2):119–137.

Durresi, A., Paruchuri, V. e Barolli, L. (2009). Fast Autonomous System Traceback. *Journal of Network and Computer Applications*, 32(2):448 – 454.

Ehrenkranz, T. e Li, J. (2009). On the State of IP Spoofing Defense. *ACM Transactions on Internet Technology*, 9(2):1–29.

Ferguson, P. e Senie, D. (2000). RFC 2827: Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing.

Gao, Z. e Ansari, N. (2007). A Practical and Robust Inter-Domain Marking Scheme for IP Traceback. *Computer Networks*, 51(3):732–750.

Huston, G. (2009). *32-bit Autonomous System Number Report*. http://www.potaroo.net/tools/asn32/.

Hyun, Y., Huffaker, B., Andersen, D., Aben, E., Luckie, M., Claffy, K. e Shannon, C. (2009). The IPv4 Routed /24 AS Links Dataset. http://www.caida.org/data/active/ipv4_routed_topology_aslinks_dataset.xml.

Laufer, R. P., Moraes, I. M., Velloso, P. B., Bicudo, M. D. D., Campista, M. E. M., de O. Cunha, D., Costa, L. H. M. K. e Duarte, O. C. M. B. (2005). Negação de Serviço: Ataques e Contramedidas. Em *Minicursos do V Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg'2005*, capítulo 1, páginas 1–63.

Laufer, R. P., Velloso, P. B., de O. Cunha, D., Moraes, I. M., Bicudo, M. D. D., Moreira, M. D. D. e Duarte, O. C. M. B. (2007). Towards Stateless Single-Packet IP Traceback. Em *IEEE Conference on Local Computer Networks*, páginas 548–555.

Liu, X., Li, A., Yang, X. e Wetherall, D. (2008). Passport: Secure and Adoptable Source Authentication. Em *USENIX Symposium on Network Systems Design and Implementation*.

Mahadevan, P., Krioukov, D., Fomenkov, M., Dimitropoulos, X., Claffy, K. C. e Vahdat, A. (2006). The Internet AS-level Topology: Three Data Sources and One Definitive Metric. *ACM SIGCOMM Computer Communication Review*, 36(1):17–26.

Oliveira, L., Aschoff, R., Lins, B., Feitosa, E. e Sadok, D. (2007). Avaliação de Proteção Contra Ataques de Negação de Serviço Distribuídos (DDoS) Utilizando Lista de IPs Confiáveis. Em *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg'2007*, Rio de Janeiro, RJ, Brasil.

Savage, S., Wetherall, D., Karlin, A. e Anderson, T. (2001). Network Support for IP Traceback. *IEEE/ACM Transactions on Networking*, 9(3):226–237.

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 Transactions on Networking*, 10(6):721–734.

Song, D. X. e Perrig, A. (2001). Advanced and Authenticated Marking Schemes for IP Traceback. *IEEE International Conference on Computer Communications*, 2:878–886.

Yaar, A., Perrig, A. e Song, D. (2005). FIT: Fast Internet Traceback. *IEEE International Conference on Computer Communications*, 2:1395–1406.