BGP Traceback: Um Novo Método para Identificação de Caminhos de Ataques na Internet

Luis Felipe M. de Moraes[1] **, Denilson Vedoveto Martins**[1]

[1]Laboratório de Redes de Alta Velocidade – RAVEL
Programa de Engenharia de Sistemas e Computação – COPPE/UFRJ
Caixa Postal: 68.511 – 21941-972 – Rio de Janeiro, RJ, Brasil

{moraes,denilson}@cos.ufrj.br

Abstract. *This paper presents the proposal of a new method of IP Traceback that introduces the use of the Border Gateway Protocol (BGP) to trace the path of an attack in the Internet. To allow such functionality, new messages were included to the BGP. Due to the problems found in current methods of IP Traceback, modifications are proposed in the packet marking mechanism, allowing only attack packets to be marked. To guarantee the secure communication between BGP Peers, the use of security mechanisms introduced by the proposal of Secure-BGP (S-BGP) will be considered.*

Resumo. *Este artigo apresenta a proposta de um novo método de IP Traceback que introduz a utilização do Border Gateway Protocol (BGP) para rastrear o caminho de um ataque na Internet. Para permitir tal funcionalidade, foram incluídas novas mensagens ao BGP. Devido aos problemas encontrados nos métodos atuais de IP Traceback, são propostas alterações no mecanismo de marcação de pacotes, permitindo que sejam escolhidos apenas aqueles pertencentes a ataques. Para garantir a comunicação segura entre as entidades BGP, será considerado o uso dos mecanismos de segurança introduzidos pela proposta do Secure-BGP (S-BGP).*

1. Introdução

Os principais protocolos da Internet, o TCP e o IP (*Transmission Control Protocol e Internet Protocol*), foram desenvolvidos sem os devidos cuidados relacionados a segurança. Isso permitiu a exploração de falhas como SYN Flood e IP Spoof [CERT 1996], falhas na geração do número inicial do TCP/IP [CERT 2001] e falhas que permitem ataques diretamente à pilha TCP/IP. Essas falhas aliadas aos ataques de *DoS* e *DDoS* dificultam a identificação do endereço de origem do ataque, ou do caminho do ataque na rede. Devido a esses problemas, técnicas de rastreamento tiveram que ser desenvolvidas. Uma dessas técnicas é o *IP Traceback*, que tem por objetivo identificar, ou rastrear, o caminho do ataque na Internet sem levar em consideração o endereço IP de origem dos pacotes de ataque, pois estes geralmente são falsificados [ISS 2000].

Alguns trabalhos encontrados na literatura apontam os problemas mais comuns dos métodos de *IP Traceback*, inclusive problemas ligados à segurança desses métodos [Belenky and Ansari 2003c] [Kuznetsov, V. et al 2002]. Devido a esses problemas, foi proposto um novo método, apresentado neste trabalho, que não apresenta tais problemas de segurança, que efetua marcações de maneira mais eficiente que os demais métodos

de *Probabilistic Packet Marking* (PPM) [Park and Lee 2001], e que introduz uma nova abordagem: o uso do BGP para rastrear caminho de ataques na Internet.

Na seção 2, será apresentada uma análise dos métodos de *IP Traceback* com enfoque em segurança. Na seção 3, será apresentada a proposta deste trabalho, que é um método de *IP Traceback* mais eficiente e seguro, ao qual foi dado o nome de *BGP Traceback*. Na seção 4, serão apresentados os resultados da implementação no simulador NS-2, e a comparação com a proposta de *ICMP Traceback*. Finalmente, na seção 5, serão apresentadas algumas considerações finais e trabalhos futuros.

2. IP Traceback

O *IP Traceback*, ou somente *Traceback*, é definido como um conjunto de mecanismos para identificar o caminho de um ataque na Internet. Em [Savage et al. 2001], a identificação do caminho de um ataque é dividido em 2 problemas. O primeiro, é o problema do *Traceback* exato, que é determinar o caminho completo do ataque e o verdadeiro endereço do *Atacante*. O segundo, é o problema do *Traceback* aproximado, que é encontrar um caminho na rede, mesmo que parcial, para cada candidato a *Atacante* que contém o caminho real de ataque. Em alguns casos, a identificação do caminho completo é impossibilitada devido ao uso de dispositivos de rede que impedem o acesso direto ao *Atacante*, como *Firewall* ou equipamentos que realizam *NAT* (*Network Address Translation*).

Uma premissa utilizada neste trabalho e em outras propostas de métodos de *Traceback*, é que a vítima terá somente uma saída para a rede, que obrigatoriamente irá passar pelo roteador com BGP de seu SA (Sistema Autônomo).

Será utilizada a definição encontrada em [Baba and Matsuda 2002] para classificar os métodos de *IP Traceback*. Nela, os métodos são divididos entre pró-ativos e reativos. Os métodos pró-ativos são aqueles que preparam a informação para o *Traceback* quando os pacotes ainda estão em trânsito na rede, mesmo que um ataque não esteja em andamento, ou mesmo se a ocorrência de um ataque ainda não tenha sido identificada. Já os métodos reativos são aqueles que tentam identificar o caminho do ataque somente após ter sido detectada a ocorrência do ataque.

Diversos métodos de *Traceback* já foram propostos, entretanto, nenhum dos métodos encontrados na literatura é uma solução completa. Nem mesmo algum método foi considerado como um padrão, e tampouco existe um consenso sobre quais são as características mais importantes nos métodos de *Traceback*. Até o momento, somente dois trabalhos publicados compararam os métodos propostos e enumeraram métricas para a avaliação desses métodos. São eles: *On IP Traceback* [Belenky and Ansari 2003c] e *An Evaluation of Different IP Traceback Approaches* [Kuznetsov, V. et al 2002].

Em [Belenky and Ansari 2003c], os autores enumeram e explicam as características que consideram ser importantes nos métodos de *Traceback*, como: interação com outras redes no processo de identificação, número de pacotes necessários para realizar o *Traceback* com êxito, sobrecarga de processamento nos roteadores, tráfego extra gerado pelo método, facilidade de evasão do método, validade dos resultados caso algum roteador tenha sido invadido, dentre outros. Por fim, é concluído que nenhum método avaliado possui todas as qualidades de um esquema ideal, e que cada método tem suas vantagens e desvantagens, mas com alguns mostrando-se melhores em alguns casos. No entanto, a questão segurança não é abordada em detalhes.

Já em [Kuznetsov, V. et al 2002], os autores estabeleceram as seguintes métricas para comparação: número de pacotes necessários para identificar a origem com sucesso, complexidade do método, eficiência dos resultados e dificuldade de implantação. Os autores consideraram que essas métricas de avaliação estipuladas têm a mesma importância, pois todas terão grande valor caso um desses métodos venha a ser utilizado na prática. Por fim, é concluído que todos os métodos impõem uma sobrecarga muito grande no processamento dos roteadores, ou que se deve passar um longo tempo coletando pacotes, o que torna impraticável a implantação de tais métodos na Internet.

Foi decidido realizar uma análise dos principais métodos encontrados na literatura, pois não existe um trabalho mais detalhado sobre a segurança dos métodos de *IP Traceback*. Com essa análise, pôde-se perceber que todos os métodos citados permitem de alguma forma a evasão por parte do *Atacante*, possuem alguma falha que pode ser utilizada para que o método seja ele próprio uma nova fonte de ataques, ou então, permitem a inserção de dados falsos, o que dificulta o rastreamento do ataque. Essa análise motivou uma pesquisa a fim de encontrar soluções para os pontos fracos dos métodos analisados.

Durante a pesquisa, foi observado que a maioria dos métodos propõem acréscimos ou mudanças no cabeçalho do pacote IP. Uma conclusão encontrada é que o principal motivo desses métodos serem inseguros é justamente por utilizarem o protocolo IP como fonte da solução, pois o IP é um protocolo não orientado a conexão, e não possui mecanismos de segurança ou de autenticação que garantam a identidade da origem dos pacotes.

Outro problema de segurança está presente em alguns métodos, mas desta vez, nos que utilizam a técnica de PPM. Esses métodos inserem uma marcação nos pacotes, e geralmente essa marcação é o próprio IP do roteador. Não existe a autenticação da marcação realizada nos pacotes, e isso permite que o *Atacante* atrapalhe a identificação através da inserção de marcações falsas nos pacotes de ataque. Segundo [Waldvogel 2002], os métodos que utilizam PPM estão vulneráveis a um ataque estatístico, e os autores mostram que um *Atacante* consegue injetar pacotes com marcações falsas na rede de forma mais eficiente do que os roteadores conseguem realizar marcações legítimas.

Também foi identificado um problema relacionado à eficiência dos métodos de PPM. Estes realizam a marcação em um pacote qualquer que passa pelo roteador, independente de ser, ou não, pertencente a um ataque ou direcionado a uma vítima. Desta forma, a chance de um pacote pertencente a um ataque ser marcado e de um outro pacote qualquer é a mesma. Como mostrado por [Mankin, A. et al 2001], a eficiência da marcação cai muito quando a quantidade de tráfego legítimo é muito maior que o tráfego de ataque. Portanto, seria interessante alterar esse mecanismo de marcação para que fossem realizadas marcações somente em pacotes pertencentes a um ataque, não ocorrendo, desta forma, marcações consideradas inúteis.

Com os conhecimentos adquiridos nesta pesquisa, foi proposto um novo método de *Traceback* que não possui os problemas de segurança já citados, e que tem um bom nível de segurança, a ponto de evitar que o atacante insira dados falsos no mecanismo de *Traceback*, ou ainda, que o próprio método seja uma nova fonte para ataques.

3. O BGP Traceback

Após observações nos métodos de *Traceback* existentes, pôde-se perceber que todos realizaram alguma modificação nos roteadores, seja para marcar um pacote IP, para criar

novos pacotes, ou para coletar os pacotes que passam por um roteador. Entretanto, essas alterações são muitas vezes inviáveis devido a problemas como: tráfego extra excessivo na rede, sobrecarga no processamento dos roteadores e até mesmo incompatibilidade com outros protocolos [Belenky and Ansari 2003b] [Belenky and Ansari 2003a].

Foi decidido que para propor o novo método, este deveria funcionar nos mecanismos ou protocolos que fazem parte da infra-estrutura da Internet. Assim, o protocolo BGP [Rekhter and Li 1995] foi o mecanismo escolhido por ter o diferencial de ser o padrão utilizado atualmente para interconectar as diversas redes que compõe a Internet.

O BGP é um protocolo de roteamento cujo principal objetivo é interconectar SAs (Sistemas Autônomos). A função primária de um roteador BGP é de realizar a troca de informações relativas a conectividade de redes com outros sistemas BGP. Isso é feito através do uso das mensagens *OPEN, UPDATE, NOTIFICATION* e *KEEPALIVE*, conforme definidos em [Rekhter and Li 1995]. A mensagem de *OPEN* é a primeira mensagem trocada por dois vizinhos BGP e que possui alguns parâmetros necessários para o estabelecimento da conexão. Uma vez que a mensagem de *OPEN* é aceita, as mensagens de *UPDATE, NOTIFICATION* e *KEEPALIVE* podem ser enviadas. Elas servem respectivamente para transferir informações e atualizações sobre roteamento, indicar a identificação de uma condição de erro, e manter a conexão ativa com seus vizinhos BGP.

A proposta do *BGP Traceback* consiste numa extensão ao protocolo BGP, para que este possa identificar o caminho de ataques na Internet. Para isto, foram criadas duas novas mensagens no protocolo BGP. Estas mensagens são para uso exclusivo do método de *Traceback*, e não serão utilizadas em momento algum para o cálculo de rotas ou para qualquer outra finalidade que não seja a identificação do caminho de ataques. Foram dados os seguintes nomes para essas mensagens: *Traceback Request* e *Traceback Reply*. Utilizando a classificação definida em [Savage et al. 2001], o objetivo desta proposta é a identificação do primeiro roteador da Internet que esteja verificando os pacotes enviados por um *Atacante*, ou seja, o objetivo é atacar o problema do *Traceback* aproximado.

A mensagem de *Traceback Request* é utilizada por um roteador para realizar o pedido de *Traceback* aos outros roteadores. Já a mensagem de *Traceback Reply* é a resposta utilizada pelos roteadores para identificar o caminho do ataque.

Caso um administrador queira identificar o caminho de um ataque direcionado a uma vítima *V* sob seu domínio, ele vai enviar uma nova mensagem de *Traceback Request* aos seus roteadores vizinhos contendo o endereço da vítima *V*. Após receberem o pedido, os roteadores vizinhos irão propagar essa mensagem a outros roteadores até uma distância máxima previamente estipulada. No momento em que os roteadores vizinhos identificarem um pacote com destino à vítima *V*, eles respondem ao roteador que originou o pedido com uma mensagem de *Traceback Reply*. Tal mensagem irá conter os endereços dos roteadores por onde o pacote pertencente ao ataque passou.

Será considerada a situação descrita na Figura 1 para apresentar o funcionamento simplificado do método proposto, onde todos os roteadores possuem o BGP e o *BGP Traceback* implementado.

Nesta situação, o atacante *A* escolhe a vítima *V* para direcionar seu ataque. O administrador da rede da vítima identifica que existe um ataque lançado contra *V*, seja através de um alerta do IDS ou do comportamento anômalo da rede, e decide utilizar o

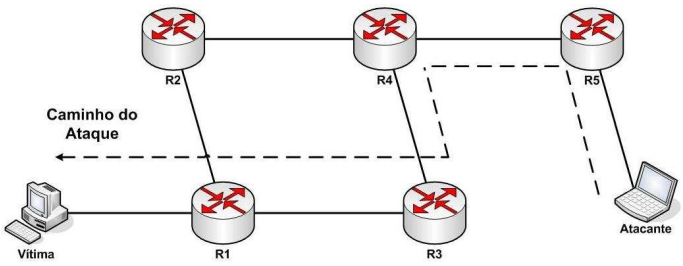

Figura 1. Cenário de exemplo.

BGP Traceback para identificar o caminho do ataque. Para isso, o administrador utiliza o roteador R_1, que está sob seu domínio, para enviar uma mensagem de *Traceback Request* para seus vizinhos, R_2 e R_3.

Os roteadores R_2 e R_3 irão repassar o pedido de *Traceback Request* para seus vizinhos, neste caso enviando para R_4, que enviará o pedido para R_5. Dessa maneira, todos os roteadores terão recebido o pedido de *Traceback Request* gerado por R_1, e estarão aptos a gerar pacotes de *Traceback Reply* quando identificarem pacotes destinados a *V*.

Neste momento, será considerado que o atacante enviou mais um pacote direcionado a *V*. Assim que esse pacote chegar em R_5, esse roteador verificará que existe um pedido para identificar o caminho dos pacotes enviados para *V*, e irá escolher, com uma probabilidade *p*, se irá gerar uma mensagem de *Traceback Reply*, sendo *p* constante e idêntico em todos os roteadores. Neste caso, o roteador R_5 irá criar um novo pacote de *Traceback Reply*, irá acrescentar seu IP no conteúdo desse pacote e o enviará para o próximo roteador no caminho até *V*.

O roteador R_4 irá receber o pacote gerado por R_5, vai verificar que se trata de um *Traceback Reply* e acrescentará seu endereço IP após o endereço já inserido por R_5. Uma vez incluído o endereço IP, R_4 irá encaminhar este pacote ao próximo roteador no caminho até a vítima que é o roteador R_3. Este irá receber o pacote e acrescentar seu endereço IP após o endereço já inserido por R_5 e R_4, e irá encaminhar este pacote ao próximo roteador.

O roteador R_1 irá receber o pacote de R_3, e vai verificar que foi ele, R_1, que gerou o pedido de *Traceback Request* que ocasionou esta resposta. Assim, o BGP vai concluir que este pacote de *Traceback Reply* chegou no seu destino e exibirá para o administrador da rede da vítima o conteúdo R_5-R_4-R_3-R_1, que é o caminho realizado pelo pacote enviado do atacante *A* até vítima *V*.

Foi utilizado como exemplo o pacote gerado por R_5 para mostrar o caminho completo realizado pelo ataque. Os outros roteadores também podem gerar o *Traceback Reply*, quando identificarem pacotes destinados a vítima *V*, mas o resultado será um caminho parcial do ataque. No exemplo, foi simplificado o esquema de funcionamento do *BGP Traceback* e foram omitidos os detalhes da marcação de pacotes. Estes procedimentos de marcação serão descritos a seguir.

O *BGP Traceback* utiliza o conceito de PPM com algumas modificações. Nos demais métodos de PPM os roteadores realizam a marcação diretamente nos pacotes, já no *BGP Traceback* não ocorre a marcação, e sim a geração de um novo pacote. Este novo

```
Procedimento de marcação no roteador R:
      seja p a probabilidade de marcação
      para cada pacote W:
      seja X um número randômico entre [0..1)
      se X < p então
            escreva R em W
            envie W
```

Figura 2. Exemplo de mecanismo de marcação.

```
Procedimento de marcação no roteador R:
      seja p a probabilidade de marcação
      seja T a tabela de IP's a serem rastreados
      para cada pacote W:
      se W.destino está em T então
            seja X um número randômico entre [0..1)
            se X < p então
                  gera mensagem M de Traceback Reply
                  M.caminho = R
                  envie W
                  envie M para nexthop(W)
```

Figura 3. Mecanismo de marcação do *BGP Traceback*.

pacote é uma mensagem de *Traceback Reply*, e todos os dados referentes a identificação do caminho do ataque estão contidos nessa mensagem. Isso permite que o pacote original siga seu caminho sem ser alterado. Apesar dessa mudança, será utilizado o termo "marcação" também para o *BGP Traceback*.

Em [Mankin, A. et al 2001], é verificado que a quantidade de marcações inúteis é muito maior do que o número de marcações úteis. Com essa informação, foi decidido que o mecanismo de marcação a ser utilizado pelo *BGP Traceback* deveria ser modificado para que se tenha um número maior de marcações úteis. Para isso, foi levado em consideração se o destino do pacote a ser marcado é direcionado a uma vítima.

Nos outros métodos de PPM, a escolha de marcação dos pacotes é totalmente aleatória, ocasionando a marcação de pacotes que não são destinados a uma máquina que está sendo atacada. Essas marcações são consideradas inúteis, e poucos pacotes pertencentes ao ataque são marcados (pacotes úteis) conforme mostrado em [Waldvogel 2002].

Na Figura 2 é possível ver o mecanismo de marcação utilizado em [Savage et al. 2001]. Note que o destino do pacote não é considerado na escolha da marcação, por isso são geradas grandes quantidades de pacotes com marcações inúteis.

No mecanismo de marcação apresentado nesta proposta, primeiro verifica-se se o pacote é destinado a uma vítima para, então, escolher se o pacote será marcado dada a probabilidade p, conforme pode-se ver na Figura 3. A grande vantagem desta modificação no mecanismo proposto sobre os demais é que não são gerados pacotes inúteis, ou seja, não são gerados pacotes para endereços que não solicitaram um pedido de *Traceback*.

3.1. Mensagem de Traceback Request

A mensagem de *Traceback Request* é um pedido enviado aos roteadores vizinhos, para que estes auxiliem a identificar o caminho de um ataque a uma vítima *V*. Os roteadores vizinhos, ao receberem esta mensagem, devem acrescentar o endereço da vítima (contido no pedido) a uma lista local de endereços a serem rastreados, e repassar o pedido aos seus vizinhos, decrementando o campo Distância-Máxima em cada roteador.

Esta lista de endereços será utilizada pelo roteador para verificar se os pacotes que passam por ele são direcionados a alguma vítima. Caso seja, ele irá escolher, com probabilidade p, se será gerada uma mensagem de *Traceback Reply*.

O formato proposto para a mensagem de *Traceback Request* e os campos desta mensagem são ilustrados na Figura 4. A seguir, serão descritos os campos da mensagem e suas respectivas funcionalidades:

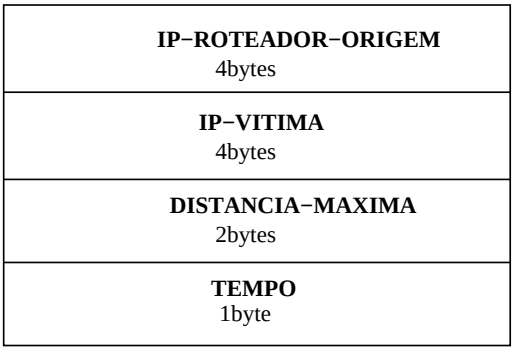

Figura 4. Formato proposto para o *Traceback Request*.

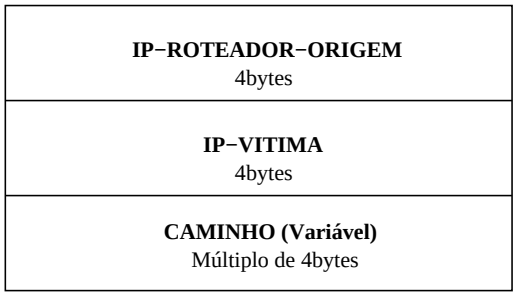

Figura 5. Formato proposto para o *Traceback Reply*.

• Campo IP-Roteador-Origem. Tamanho de 4 bytes. Utilizado para armazenar o IP do roteador que originou o pedido de *Traceback Request*. Este campo não é alterado quando o pacote for repassado de um roteador para outro.

• Campo IP-Vítima. Tamanho de 4 bytes. Utilizado para armazenar o IP da máquina que está sendo atacada (vítima). Este campo não é alterado quando o pacote for repassado de um roteador para outro.

• Campo Distância-Máxima. Tamanho de 2 bytes. O valor do campo Distância-Máxima tem como valor inicial a distância máxima escolhida pelo administrador para que um roteador receba este pedido, e este valor é decrementado a cada roteador pelo qual o pedido passa, até chegar ao valor 0 (zero), quando a mensagem não deve ser mais repassada.

• Campo Tempo. Tamanho de 1 byte. Indica a quantidade de tempo, em segundos, que os roteadores que receberem este pedido devem observar o tráfego destinado a vítima.

A finalidade do campo Distância-Máxima é permitir que o administrador da rede da vítima possa escolher até qual distância, a partir de seu roteador, os outros roteadores irão receber a mensagem de *Traceback Request* e participar do rastreamento. Como o número de roteadores está sendo limitado, a sobrecarga de processamento nos roteadores devido ao procedimento de marcação dos pacotes será limitada somente aos roteadores que receberão a mensagem.

Para os resultados serem mais completos, todos os roteadores deveriam participar da identificação. No entanto, esta restrição deve ser feita para que o *BGP Traceback* não sobrecarregue os roteadores, pois foi verificado que o procedimento de marcação seria muito oneroso em termos de consumo de processamento. Este item será abordado mais adiante.

Para reduzir ainda mais o impacto do *BGP Traceback* no processamento dos roteadores, é estipulado um tempo t de permanência do pedido em um roteador (campo Tempo), para que os roteadores realizem o rastreamento. Esse tempo deve ser contado a partir do momento do recebimento da mensagem de *Traceback Request* para determinada vítima V. Após o término deste tempo t, o pedido para a vítima V deve ser removido da lista de endereços a serem rastreados.

Assim, o administrador da rede da vítima deverá receber as mensagens de *Tra-*

ceback Reply por um tempo um pouco superior à *t*, para que tenha tempo suficiente de todas mensagens chegarem até o roteador que gerou o pedido. Após isso, o administrador deverá interpretar essas respostas e verificar se os resultados são aceitáveis. Caso não sejam, ele pode gerar um novo pedido de *Traceback Request*, mas desta vez com o valor do campo Distância-Máxima, ou Tempo, maior que o anterior, a fim de obter resultados mais conclusivos.

3.2. Mensagem de Traceback Reply

Quando um roteador recebe um pacote destinado a um dos endereços que constam na sua lista de endereços a serem rastreados, ele irá escolher com probabilidade *p* se irá gerar um *Traceback Reply* para este pacote. É considerado que a probabilidade *p* é constante e idêntica em todos os roteadores. Se o *Traceback Reply* for gerado, então o roteador irá inserir seu endereço no conteúdo desta mensagem, preencher os campos que indicam qual roteador gerou o pedido e a qual vítima esta mensagem se refere, e irá enviá-la para o próximo roteador no caminho até chegar ao roteador gerador do pedido.

O formato proposto para a mensagem de *Traceback Reply* e os campos desta mensagem são ilustrados na Figura 5. A seguir serão descritos os campos da mensagem e suas respectivas funcionalidades:

• Campo IP-Roteador-Origem. Tamanho de 4 bytes. Utilizado para indicar o IP do roteador que originou o pedido de *Traceback Request*. Este campo não é alterado quando o pacote for repassado de um roteador para outro.

• Campo IP-Vítima. Tamanho de 4 bytes. Utilizado para indicar o IP da máquina que está sendo atacada, ou seja, a vítima *V*. Este campo não é alterado quando o pacote for repassado de um roteador para outro.

• Campo Caminho. Tamanho variável, mas sempre múltiplo de 4 bytes. Cada roteador que receber a mensagem de *Traceback Reply* deve acrescentar seu endereço IP ao final deste campo.

Se o caminho realizado pelo ataque for muito grande, ou seja, se o ataque atravessar muitos roteadores, o campo Caminho pode crescer muito, e suspeitou-se de que não existiria espaço suficiente no pacote para acrescentar tais endereços. Após consulta à RFC1771 [Rekhter and Li 1995], que define o protocolo BGP, foi verificado que o tamanho máximo de uma mensagem BGP é 4096 bytes, e que todas as implementações do BGP devem suportar este tamanho máximo. Como o cabeçalho IP consome apenas 20 bytes, o TCP consome outros 20 bytes, e o cabeçalho BGP consome outros 19 bytes, isso totaliza 59 bytes, e mostra que ainda há espaço suficiente para armazenar 255 endereços, que é o valor máximo para o campo TTL (Time To Live) do protocolo IP.

3.3. Secure BGP

O BGP não é um protocolo seguro, como apresentado em [Murphy 2006]. Por isso, foi realizado um estudo para identificar o estado atual da segurança do BGP, e encontrar propostas na literatura para incorporar segurança a ele. Foi encontrada a proposta do *Secure Border Gateway Protocol (S-BGP)* [Kent et al. 2000], na qual é introduzida uma nova arquitetura que utiliza diversos mecanismos que protegem o protocolo BGP contra grande parte dos ataques aos quais ele está vulnerável atualmente.

Para eliminar as falhas existentes no BGP, a arquitetura S-BGP utiliza três mecanismos de segurança, são eles: PKI (*Public Key Infrastructure*), um novo atributo BGP e o IPSec. Esses componentes são usados pelo BGP para validar a autenticidade e a integridade dos dados de uma mensagem *BGP UPDATE*, para prover privacidade aos dados do *UPDATE* e para verificar a identidade e a autorização [Kent et al. 2000] de quem os enviou.

O uso do IPSec, mais especificamente do ESP (*Encapsulated Security Payload*) e do IKE (*Internet Key Exchange*), fornece serviços de segurança necessários pelo receptor BGP para verificar a integridade e a identidade de quem enviou e recebeu a mensagem. O ESP também provê proteção criptográfica para todo o tráfego BGP, e protege contra ataques de *replay* de mensagens [Haller and Atkinson 1994].

O novo atributo acrescentado ao BGP pelo S-BGP é utilizado para carregar os dados que vão permitir a validação dos endereços e das rotas anunciadas, protegendo o BGP contra vizinhos que distribuíram *UPDATEs* errados, e contra anunciantes BGP que anunciaram endereços ou rotas que não deveriam ser anunciadas. Para uma descrição mais completa dos mecanismos de PKI e de certificados utilizados no S-BGP é sugerida a leitura da proposta original em [Kent et al. 2000].

O maior ganho na utilização do S-BGP é impossibilitar que os atacantes enviem mensagens BGP falsas. Consequentemente impede-se o envio de mensagens falsas do *BGP Traceback*, pois o *BGP Traceback* consiste, basicamente, no acréscimo de 2 novas mensagens ao BGP.

Apesar de ainda não ser uma proposta formal no IETF, os autores tem trabalhado com empenho num protótipo que implementa o S-BGP. Muitos trabalhos acreditam que num futuro breve haverá uma oficialização da proposta no IETF, e que o S-BGP será considerado um padrão para as novas versões do protocolo BGP.

Por acreditar que o S-BGP é uma proposta viável, que será utilizada num futuro breve, e por atender as necessidades de segurança do *BGP Traceback*, será considerado que o *BGP Traceback* só será utilizado quando o S-BGP estiver em uso, e, consequentemente, com todos os benefícios de segurança citados anteriormente. É importante deixar clara essa consideração, pois provavelmente o *BGP Traceback* não será utilizado na versão atual do BGP, mas sim em versões futuras do BGP.

4. Implementação e Resultados

Para entender melhor o comportamento da proposta em relação ao número de pacotes gerados devido a troca de mensagens entre os roteadores, e para poder analisar as características relativas à marcação de pacotes, (como probabilidade de marcação p, tempo t de permanência do pedido nos roteadores e valor da distância máxima do pedido de *Traceback Request*) foi realizada a implementação e também simulações do *BGP Traceback* para observar tais aspectos.

A utilização de um simulador de redes vem a ser uma boa alternativa, visto que é necessário somente uma máquina para realizar as simulações. Entretanto, os simuladores possuem limitações e não conseguem reproduzir todo o ambiente real no ambiente de simulações, como também é mostrado em [Ford and Paxson 2001].

A implementação foi realizada no simulador NS-2 *(Network Simulator 2)*, versão

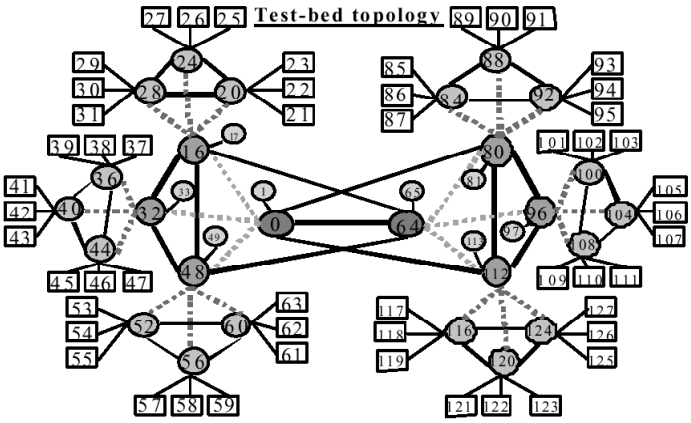

Figura 6. Topologia utilizada no Exemplo 1

2.27, disponibilizado em [VINT Project 2004]. Uma grande quantidade de código foi inserida no simulador, por isso, fica difícil listar as alterações e inclusões realizadas. Os principais pontos em relação a implementação foram:

• Criação de 2 novas mensagens no simulador.

• Alteração do mecanismo de envio de pacotes para suportar as mensagens de *Traceback Request* e *Traceback Reply*.

• Alteração do mecanismo de recebimento de pacotes nos roteadores para, ao receber um pacote, verificar se existe um pedido de *Traceback* para aquele destino.

• Criação do mecanismo de marcação e geração de pacotes nos roteadores.

• Criação e manipulação da lista de endereços a serem rastreados no roteador.

4.1. Exemplo 1

Em [Mankin, A. et al 2001], os autores criaram uma topologia de rede para simular um ataque e verificar o comportamento do *ICMP Traceback* proposto em [Bellovin 2000]. A topologia utilizada pode ser observada na Figura 6. O simulador utilizado pelos autores também foi o NS-2 [VINT Project 2004], e o ambiente de simulação possui diversos roteadores representados por círculos, e computadores representados por retângulos.

Nesta simulação, foi implementado o caso onde há somente um atacante e uma vítima. O atacante está situado no computador representado pelo endereço 25 e a vítima no 125. O caminho do ataque é $25 \rightarrow 24 \rightarrow 16 \rightarrow 0 \rightarrow 112 \rightarrow 124 \rightarrow 125$, e a taxa de ataque é de 50 mil pacotes por segundo. Os computadores representados por retângulos geram tráfego aleatoriamente entre si para simular o tráfego legítimo da rede.

O *ICMP Traceback* utiliza o conceito de PPM e utiliza a probabilidade de marcação de $1/20000$. Os autores de [Mankin, A. et al 2001] efetuaram a simulação e analisaram os pacotes de *ICMP Traceback* gerados pelo roteador 24, que é o roteador conectado diretamente ao atacante 25, conforme pode-se observar na Figura 6. As primeiras 1200 mensagens geradas por este roteador foram analisadas, e a maior parte (99,58%) delas são consideradas inúteis, pois não foram direcionadas a vítima 125. A primeira mensagem útil foi gerada após 292 mensagens inúteis, ou seja, se uma mensagem útil equivale

a 20 mil pacotes que passaram pelo roteador, isso implica que a primeira mensagem foi gerada após o roteador 24 ter encaminhado quase 6 milhões de pacotes.

Foi utilizado o mesmo ambiente e os mesmos parâmetros apresentados em [Mankin, A. et al 2001], para que ocorresse a comparação de forma fiel ao trabalho em questão. Foi utilizado o valor 4 para o campo Distância-Máxima no pedido de *Traceback Request*, pois este valor é suficiente para identificar a origem do ataque neste exemplo. A probabilidade *p* utilizada foi de $1/20000$, e o tempo de simulação utilizado foi o suficiente para que o roteador 24 gerasse 1200 mensagens de *Traceback*.

Devido às modificações propostas ao mecanismo de marcação de pacotes realizadas no *BGP Traceback*, era esperado que não houvessem pacotes de *Traceback* gerados de forma inútil, como é observado no *ICMP Traceback*. Após observar os registros das simulações, essa expectativa foi confirmada e 100% das mensagens de *Traceback Reply* geradas foram direcionadas à vítima 125. Desta maneira, pôde-se mostrar que as modificações propostas ao mecanismo de marcação foram válidas e funcionaram da maneira esperada, ou seja, não gerando pacotes inúteis.

4.2. Exemplo 2

Foi observado que a probabilidade de $1/20000$, definida em [Bellovin 2000], e utilizada na simulação anterior, mostrou-se inadequada, pois devido a grande quantidade de tráfego gerado pelo atacante 25, e pelo tempo de observação de pacotes, foram gerados inúmeros pacotes na rede. Para reduzir esse número de pacotes, é necessária a redução do tempo de observação de pacotes pelos roteadores ou a redução da probabilidade.

Foi decidido analisar o mesmo cenário, mas com outros parâmetros. Neste caso, foi utilizada a probabilidade *p* de $1/100000$ e o tempo *t* de permanência de pedidos nos roteadores de 30 segundos. Com estes valores, o número médio esperado de mensagens de *Traceback Reply* gerado por cada roteador no caminho do ataque é de 15 mensagens, como é possível conferir a seguir. É considerado *A* como o número de pacotes de ataque observados em um roteador no tempo *t*, e *G* como o número de mensagens de Traceback Reply geradas por cada roteador.

$$p = 1/100000 \qquad t = 30\ segundos$$

$$\lambda = \textit{número médio de pacotes de ataque por segundo} = 50000$$

então,

$$A = \lambda * t = 50000 * 30 = 1500000$$

$$G = \lambda * t * p = A * p = 1500000 * 1/100000 = 15$$

Como existem 4 roteadores no caminho do ataque, excluindo o roteador 124 que é o roteador onde o administrador da rede da vítima está gerando os pedidos de *Traceback Request*, então o número médio de mensagens de *Traceback Reply* geradas é $G * 4 = 60$.

Conferindo os parâmetros e observando os registros das simulações, é possível verificar que o número gerado pelas simulações é compatível com o valor encontrado pela análise anterior. Foram executadas 20 simulações e calculadas algumas métricas. Foi encontrada a média de 15,45 pacotes gerados por roteador, que está muito próximo da média esperada de 15 pacotes. Segundo a *Distribuição t de Student*, foi obtido o nível de

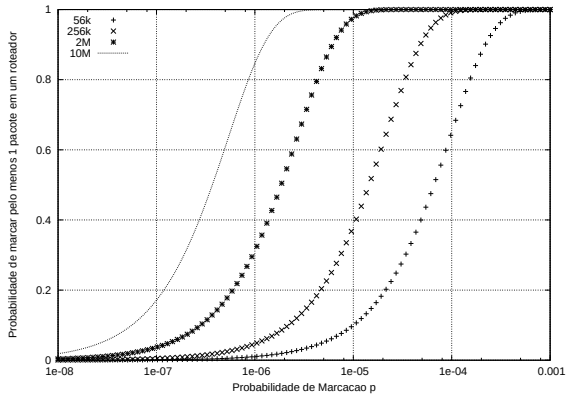

Figura 7. Probabilidade de gerar pelo menos 1 pacote em um roteador. Tempo t fixo em 60 segundos.

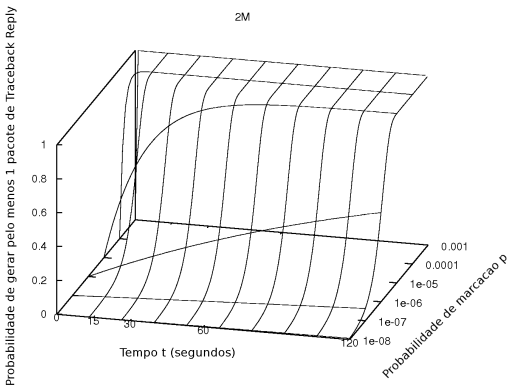

Figura 8. Influência do tempo t na probabilidade de gerar pelo menos 1 pacote.

confiança de 95% da média estar no intervalo $[13,5 < \overline{x} < 17,39]$, o que vem a validar o resultado da simulação.

Diversas simulações em diversos cenários foram executadas, e foi verificado que os resultados obtidos estiveram sempre próximos dos resultados esperados através do estudo analítico. Com estes resultados, foi possível validar a implementação da proposta, tornando possível concentrar os estudos na análise dos melhores valores a serem utilizados pelos parâmetros *p* e *t*.

4.3. Modelo analítico

Após o estudo de comportamento do método, foi possível desenvolver um modelo analítico para encontrar a probabilidade de se gerar pelo menos 1 pacote de *Traceback Reply* em um roteador, dados os parâmetros que influenciam essa geração. A fórmula é:

$$P(Gerar\ pelo\ menos\ 1\ pacote) = 1 - (1-p)^{A*t}$$

Onde *p* é a probabilidade de marcação nos roteadores, *t* é o tempo de permanência dos pedidos nos roteadores e A é a taxa de envio de pacotes do *Atacante*. Através dessa fórmula, foi traçado o gráfico apresentado na Figura 7, onde o parâmetro *t* foi fixado em 60 segundos, o parâmetro *p* variou de 10^{-8} até 10^{-3}, e o tráfego A gerado pelo *Atacante* foi de 56Kbps, 256Kbps, 2Mbps e 10Mbps. O tamanho dos pacotes foi de 40 bytes, que é o tamanho de um pacote TCP SYN utilizado em ataques de SYN Flood.

Através desse gráfico, pode-se perceber que quanto maior a taxa de pacotes enviados pelo *Atacante*, maior é a probabilidade do roteador gerar um pacote. Desta forma, é introduzido um problema ao *Atacante*, pois quanto mais pacotes ele enviar de uma única origem, mais certa será a identificação pelo método proposto. Para reduzir as chances de ser rastreado, ele terá que reduzir o número de pacotes enviados por cada origem, além de ter que aumentar o número de máquinas que participam do ataque para manter o mesmo número de pacotes de ataque que chegam até a vítima.

Através da fórmula citada, pode-se traçar alguns gráficos e avaliar o relacionamento dos parâmetros λ, *t* e *p*. Na Figura 8, é possível visualizar o compromisso entre essas variáveis. O *link* do *Atacante* é de 2Mbps e está sendo utilizado em sua capacidade

máxima. É possível perceber que para determinadas probabilidades p, pode-se escolher valores menores do tempo t, e mesmo assim garantir uma alta probabilidade de conseguir gerar pelo menos 1 pacote de *Traceback Reply*.

5. Considerações Finais e Trabalhos Futuros

Neste artigo foi apresentado o *BGP Traceback*, que utiliza uma abordagem inédita, até o momento, em um método de *Traceback*: a utilização da infra-estrutura de roteamento para a identificação do caminho de um ataque na Internet.

Por ser considerado como o futuro padrão de segurança do protocolo BGP, o S-BGP é considerado uma parte fundamental para a concretização do *BGP Traceback*, e este funcionará somente nas versões do BGP que tiverem o S-BGP implementado.

A possibilidade de se injetar dados falsos no S-BGP e no *BGP Traceback* são praticamente inexistentes, conforme as análises realizadas em [Kent et al. 2000] [Kent, S. et al 2000] [Kent 2003]. Assim, a segurança se caracteriza como o grande diferencial desta proposta em relação aos demais métodos.

As alterações realizadas no mecanismo de PPM do *BGP Traceback* e no mecanismo de recebimento de pacotes pelos roteadores, faz com que o endereço de destino do pacote encaminhado seja verificado em uma lista de endereços para os quais foram realizados pedidos, garantindo que não serão gerados pacotes inúteis.

A proposta apresentada tem como objetivo analisar o tráfego que atravessa diversas redes, por isso a escolha de ser implementada em um mecanismo que estivesse presente nos *backbones*. O método não irá identificar ataques dentro de um mesmo SA, a menos que o protocolo intra-SA seja o iBGP. Ataques dentro de um mesmo SA não são frequentes, e mesmo que ocorram, a solução pode ser local, conforme apresentada na RFC 3882 [Turk 2004] que define um procedimento para bloquear ataques *DoS* dentro de um mesmo SA. Um trabalho futuro é expandir a proposta para outros protocolos de roteamento. Uma boa característica para um método reativo, como o *BGP Traceback*, é que o método suporte mudança de rotas, e, como estará implementado diretamente em um protocolo de roteamento presente nos principais *backbones*, ele terá este suporte.

Após analisar o mecanismo de funcionamento do *BGP Traceback* e apresentar seus resultados, este demonstrou ser mais seguro que os demais métodos, mais eficaz para a identificação do caminho de ataques, mais eficaz na criação de mensagens úteis do que os mecanismos propostos em [Bellovin 2000] e [Mankin, A. et al 2001], e, por fim, mostrou ser um método adequado para uso quando o S-BGP estiver implementado.

O estudo da sobrecarga de processamento nos roteadores pelo uso do S-BGP ainda é uma questão em aberto, pois não foi possível analisar tal métrica nos simuladores existentes, como também foi notado em [Ford and Paxson 2001]. No entanto, é possível notar que a alteração realizada no mecanismo de marcação e de recebimento de pacotes, e a utilização dos mecanismos de segurança do S-BGP causarão uma redução significativa no desempenho dos roteadores. Essa queda no desempenho será causada pois os roteadores atuais possuem otimizações para conseguir encaminhar quantidades de giga-pacotes por segundo, e essas alterações, que obrigam que o roteador verifique se há um pedido de *Traceback* associado ao destino do pacote, reduzirá a eficiência dessas otimizações.

Referências

Baba, T. and Matsuda, S. (2002). Tracing Network Attacks to Their Sources. *IEEE Internet Computing*, 6(2):20–26.

Belenky, A. and Ansari, N. (2003a). Accommodating Fragmentation in Deterministic Packet Marking for IP Traceback. In *GLOBECOM 2003*, pages 1374–1378. IEEE.

Belenky, A. and Ansari, N. (2003b). IP Traceback With Deterministic Packet Marking. *IEEE Communications Letters*, 7(4):162–164.

Belenky, A. and Ansari, N. (2003c). On IP traceback. *IEEE Comm. Mag.*, 41(7):142–153.

Bellovin, S. M. (2000). ICMP Traceback Messages. IETF Draft.

CERT (1996). CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks. Technical report, http://www.cert.org/advisories/CA-1996-21.html.

CERT (2001). CERT Advisory CA-2001-09 Statistical Weaknesses in TCP/IP Initial Sequence Number. Technical report, http://www.cert.org/advisories/CA-2001-09.html.

Ford, S. and Paxson, V. (2001). Difficulties in simulating the internet. *IEEE/ACM Transactions on Networking*, 9(4):392–403.

Haller, N. and Atkinson, R. (1994). RFC1704 On Internet Authentication. IETF.

ISS, I. S. S. (2000). Distributed Denial of Service Attack Tools. Technical report, http://www.iss.net.

Kent, S. (2003). Securing the Border Gateway Protocol: A Status Update. In *7th IFIP Conference on Communications and Multimedia Security*.

Kent, S., Lynn, C., and Seo, K. (2000). Secure Border Gateway Protocol (S-BGP). In *IEEE JSAC*, volume 18, pages 582–592. IEEE.

Kent, S. et al (2000). Design and Analysis of the Secure Border Gateway Protocol (S-BGP). In *Proc. of DARPA DISCEX 2000*, volume 1, pages 18–33. IEEE.

Kuznetsov, V. et al (2002). An Evaluation of Different IP Traceback Approaches. In *4th Int. Conf. on Information and Communications Security*, pages 37–48.

Mankin, A. et al (2001). On Design and Evaluation of Intention-Driven ICMP Traceback. In *IEEE Int. Conf. Computer Comm. and Networks*, pages 159–165. IEEE.

Murphy, S. (2006). RFC4272 BGP Security Vulnerabilities Analysis. IETF.

Park, K. and Lee, H. (2001). On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack. In *20th INFOCOM*, pages 338–347. IEEE.

Rekhter, Y. and Li, T. (1995). RFC1771 A Border Gateway Protocol 4 (BGP-4). IETF.

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

Turk, D. (2004). RFC3882 Configuring BGP to Block Denial-of-Service Attacks. IETF.

VINT Project (2004). Network Simulator 2. http://www.isi.edu/nsnam/.

Waldvogel, M. (2002). GOSSIB vs. IP Traceback Rumors. In *Proc. of 18th Annual Computer Security Applications Conference*. IEEE.