

Marcação Probabilística de Pacotes em um Ambiente sob Ataque de Negação de Serviço

Mateus Mosca Viana, José Neuman de Souza e João César Moura Mota

Resumo—A aplicação de uma contramedida de rastreamento reverso, em um cenário de ataque por Negação-de-Serviço (DoS), requer indícios da trajetória de ataque, que possam ser obtidos dos pacotes que chegam até a vítima. Desde que não é possível identificar toda a trajetória em cada pacote, utiliza-se uma abordagem, que se baseia na Teoria da Amostragem, conhecida como “marcação probabilística de pacotes” (PPM). Este artigo descreve o funcionamento da PPM em ambientes sob ataque DoS, bem como a fundamentação matemática que justifica esse modo de marcação de pacotes, o *Problema do Coletor de Cupons*. Também mostra uma análise teórica sobre a relação entre os parâmetros ambientais, p e d , envolvidos no problema da amostragem de pacotes atacantes.

Palavras-Chave—Rastreamento reverso, Negação-de-Serviço, marcação probabilística de pacotes, problema do coletor de cupons.

Abstract—In a Denial-of-Service attack scenario, a traceback countermeasure employment requires some attack path clues from the packets reaching the victim. Since it is not possible to identify the entire path through only one packet, one uses an alternative approach, whose foundation is Sampling Theory, named “probability packet marking” (PPM). This paper describes the PPM functioning in an environment under DoS attack, along with the PPM mathematical background, the *Coupon Collector’s Problem*. Moreover, it shows a theoretical analysis dealing with the relation among the environment parameters, p and d , related in the attack packets sampling problem.

Keywords—Traceback, Denial-of-Service, probability package marking, coupon collector’s problem.

I. INTRODUÇÃO

A aplicação de uma contramedida de rastreamento reverso, em um cenário de ataque por Negação-de-Serviço (Denial-of-Service), necessita de indícios dos roteadores componentes da trajetória de ataque, obtidos dos pacotes que chegam até a vítima. Uma idéia inicial é forçar cada roteador a gravar uma marca que o identifique, em qualquer pacote trafegando pelo mesmo. Essa abordagem determinística, em princípio, parece a mais indicada, visto que transmite a certeza de que o objetivo do rastreamento reverso será atingido. Por outro lado, torna-se uma ameaça de sobrecarga do tráfego na rede, mesmo em condições normais de operação, quando não se configura um ataque DoS.

Especial atenção tem sido dada a uma abordagem alternativa, de caráter aleatório, para o enfrentamento desse problema. Trata-se de uma na qual o ato de marcação de um pacote por um roteador depende de uma probabilidade, p , desse

Mateus Mosca Viana (mosca@ufc.br), Depto. de Engenharia de Teleinformática/UFC e Instituto Atlântico, José Neuman de Souza (neuman@ufc.br) do Depto. de Computação/UFC e João César Moura Mota (mota@deti.ufc.br) do Depto. de Engenharia de Teleinformática/UFC. Este trabalho foi parcialmente financiado pelo INSTITUTO ATLÂNTICO e pela FUNCAP.

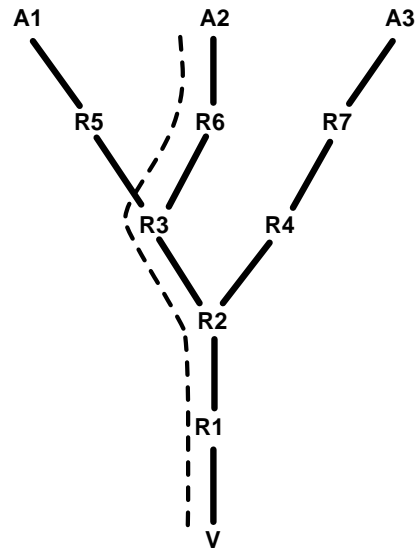


Fig. 1. Ambiente de Ataque

modo recebendo a denominação de *marcação probabilística de pacotes* (Probability Packet Marking, ou PPM).

O uso da PPM faz surgir duas indagações. A primeira se refere ao valor de p que deve ser adotado para a marcação de pacotes. A outra diz respeito à relação entre p e d , este sendo a distância desde um roteador que marcou um pacote até a vítima.

Este artigo descreve o funcionamento da PPM em ambientes sob ataque DoS, bem como a fundamentação matemática da teoria que justifica esse modo de marcação de pacotes, o *Problema do Coletor de Cupons* (Coupon Collector’s Problem, ou CCP). Também mostra uma análise teórica sobre a relação entre os parâmetros ambientais envolvidos no problema, p e d . A relação entre esses parâmetros é um importante instrumento, na tarefa de recomposição da trajetória de ataque.

Na seqüência de distribuição dos assuntos, a seção II apresenta os elementos que devem ser considerados no ambiente onde se desenrola o ataque. Os detalhes do CCP são mostrados na seção III. Na seção IV se comentam os aspectos teóricos das relações envolvendo os parâmetros p e d , além de um breve exemplo. Por fim, na seção V se apresentam as conclusões, seguindo-se as referências bibliográficas.

II. DESCRIÇÃO DO AMBIENTE

Quando um ataque do tipo DoS está em curso, a imagem topológica que retrata essa situação, sob o ponto de vista da vítima, [7], se encontra representada na Figura 1. Na estrutura

```

Se "pacote não marcado" então
  Selecionar_pacote(p)
Se "pacote selecionado" então
  Marcar_pacote
Fim_do_se
Fim_do_se

```

Fig. 2. Pseudocódigo

de árvore invertida, a vítima ocupa a posição do nó raiz, enquanto os atacantes se situam nas folhas da árvore.

Os nós intermediários são os roteadores encarregados de fazer progredir os pacotes de mensagens, enquanto a linha interrompida, na Figura 1, mostra uma possível trajetória de ataque. Os pacotes passam por vários roteadores, desde o ponto onde foi originado, até atingir a vítima. Caso recebessem uma marca, como um selo, em cada um dos roteadores por onde passassem, facilmente seria possível reconstituir a sua trajetória de ataque. Contudo, a viabilidade desse procedimento é discutível em virtude de dois fatores principais.

Em primeiro lugar, a marcação de pacotes seria um trabalho adicional que provocaria o imediato aumento da carga de serviço na rede. O outro fator, não menos crítico, diz respeito ao espaço necessário, em um pacote, para a inserção de todas as marcas. Haveria a possibilidade de o tamanho de um pacote se tornar muito grande, e assim surgir o risco de se comprometer o desempenho do funcionamento da rede. A alternativa que se apresenta como mais viável é a marcação de apenas uma parte dos pacotes, de preferência com a menor quantidade possível de sinais.

A. Marcação Probabilística de Pacotes

A idéia da PPM se baseia em dois fundamentos principais. O primeiro diz respeito ao fato de que a marcação de um pacote em um roteador deve estar sujeita a uma distribuição de probabilidade. O outro fundamento estabelece que um pacote somente poderá ser marcado, no máximo, uma única vez. Esses dois fundamentos sugerem que a carga de processamento na rede pode ser reduzida, se comparada com a abordagem determinística citada anteriormente.

A implementação da PPM necessita que, em cada roteador do ambiente, seja incorporado um pequeno módulo de código, capaz de fazer funcionar um procedimento aleatório. Esse procedimento tem a finalidade de selecionar, com probabilidade p estabelecida a priori, um pacote de mensagem a ser marcado. Um pseudocódigo para o referido módulo pode ser visto na Figura 2. Em [7] há uma interessante proposta para a implementação da PPM.

O pseudocódigo mostra que, nem todo pacote chegando a um roteador sofre marcação. Além disso, apenas aqueles que não estão ainda marcados são submetidos à rotina *Selecionar_pacote(p)*. O parâmetro de entrada é a probabilidade p e a saída pode ser um dos valores lógicos V ou F . A marcação acontece somente se o resultado da seleção for V . Qualquer análise destinada ao rastreamento reverso deverá ser realizada apenas no subconjunto de pacotes que chega à vítima e que apresenta marcação. A quantidade de elementos

desse conjunto de pacotes será função da probabilidade p , e naturalmente da quantidade de pacotes atacantes, enviados para a vítima.

A fim de garantir a representatividade do fenômeno em estudo, o subconjunto dos pacotes marcados deve conter indícios de todos os roteadores do ambiente de ataque. Uma vez que a vítima poderá receber distintos pacotes marcados pelo mesmo roteador, fica caracterizado um processo de amostragem com reposição.

Quanto ao desenvolvimento de uma análise, que possibilite construir as trajetórias de ataque, é necessário que a vítima disponha de informação suficiente acerca desse ambiente de ataque. Essa informação deverá ser extraída dos dados sobre os roteadores, representados pelas marcas representadas nos pacotes. Surge, então, a seguinte pergunta: qual é a quantidade mínima de informação necessária para que se possa reconstituir as trajetórias de ataque? Traduzindo noutros termos: qual é a quantidade mínima de pacotes marcados que a vítima deve receber, para que seja possível reconstituir as trajetórias de ataque?

Na seção IV essa questão será abordada com mais detalhes técnicos. Aspectos gerais da reconstituição das trajetórias, serão comentados na próxima sub-seção.

B. Aspectos da Reconstituição de Trajetórias

Uma trajetória de ataque pode ser representada como uma seqüência de roteadores, desde a vítima até o atacante, sendo aquela indicada na Figura 1 por uma linha tracejada representada como (R_1, R_2, R_3, R_6) , na forma vetorial. A relação de ordem implícita entre os elementos estabelece que, quanto mais à esquerda, mais próximo da vítima se encontra o roteador.

Para que se possa reconstituir uma trajetória é preciso que os dados existentes nos pacotes marcados permitam inferir alguma relação de ordem total entre os roteadores. Essa ordem total permitirá estabelecer a distância a que cada roteador se encontra da vítima. A distância entre dois roteadores, R_λ e R_μ é medida em "saltos", que é a quantidade de roteadores existentes na trajetória entre os dois extremos citados, mais um. Segundo a descrição realizada em II-A sobre a PPM, identificam-se as seguintes propriedades:

- 1) Os roteadores são independentes no que concerne ao processo de marcação;
- 2) Cada pacote de mensagem pode ser, ou não, marcado;
- 3) A probabilidade de marcação, p , é a mesma em todo o ambiente de ataque.

Como se pode ver, o processo de marcação de pacotes segue o modelo de um *experimento de Bernoulli* [3]. Então, a probabilidade de a vítima receber um pacote marcado por um roteador, afastado por uma distância d , é dada pela função $f(d) = p(1-p)^{d-1}$, visto que um pacote somente poderá ser marcado no máximo uma única vez e é desconsiderado para marcação nos $d-1$ roteadores restantes da trajetória. Observando a expressão da função $f(d)$ é trivial concluir que a mesma é monótona decrescente [5] e a monotonicidade permite estabelecer uma ordem parcial entre os roteadores. Escalonando de modo decrescente os roteadores por meio

da quantidade de pacotes que é recebida de cada um dos mesmos, obtém-se uma tabela de frequências. E quanto maior a frequência associada a um roteador, mais próximo o mesmo se encontra da vítima. A obtenção de uma trajetória de ataque é consequência da identificação de algum conjunto de roteadores que mantenha uma relação interna de ordem total.

III. O PROBLEMA DO COLETOR DE CUPONS

Uma alegoria do problema do coletor de cupons trata da obtenção de todos os N diferentes cupons de uma coleção, que são distribuídos como brindes no interior de caixas de cereais. Ao adquirir uma caixa, a priori o comprador não se sabe qual cupom da coleção irá encontrar, o que cria a possibilidade de receber um que seja repetido. Esse mecanismo de obtenção dos cupons se comporta como um processo de amostragem com repetição. A pergunta que dá origem ao problema é a seguinte: qual é a quantidade mínima de caixas de cereais que deve ser adquirida, a fim de que se possa obter toda a coleção de N cupons, sabendo que a probabilidade de extrair um cupom é igual a p ? A resposta a essa questão exige algumas considerações de natureza teórica, apresentadas na próxima subseção.

A. Aspectos Teóricos

Considere-se uma população cujos elementos são de N diferentes tipos e de onde se deseja extrair uma amostra com repetição, que precisa conter r elementos distintos. A questão que se apresenta é a determinação de S_r , que é o tamanho da amostra. Assim, S_r é a variável aleatória que representa a quantidade de extrações necessárias de serem realizadas, até que seja obtido o r -ésimo sucesso, isto é, até existirem r elementos distintos na amostra. Além disso, sendo $X_r = S_{r+1} - S_r$, então $X_r - 1$ é a variável que representa a quantidade de extrações realizadas na população depois de já existirem r elementos distintos, mas antes de existirem $r + 1$ elementos distintos, na amostra [3]. Da definição da variável X_r decorre que

$$S_r = 1 + X_1 + X_2 + \dots + X_{r-1}, \quad (1)$$

pois o primeiro sucesso ocorre com a primeira extração. O objetivo do problema se constitui na obtenção de um estimador para a variável aleatória S_r . Aplicando-se o operador da esperança matemática a ambos os lados de (1), e levando em conta que o mesmo é um operador linear, segue-se a expressão:

$$E[S_r] = 1 + \sum_{k=1}^{r-1} E[X_k]. \quad (2)$$

Conclui-se de (2) que, o estimador da variável aleatória S_r depende apenas da esperança matemática de cada uma das variáveis aleatórias X_k , $k = 1, 2, \dots, r - 1$. Considerando que a variável aleatória $X_k - 1$ representa a quantidade de fracassos precedendo o próximo sucesso em um experimento de Bernoulli, em uma população na qual $N - k$ elementos distintos ainda não foram selecionados, então a expressão da sua probabilidade é dada por $Prob(X_k - 1) = q^\lambda \cdot p$. Trata-se de uma função de massa geométrica, sendo λ a quantidade de

insucessos antecedendo o primeiro sucesso. O parâmetro p é a probabilidade a ocorrência de um sucesso, enquanto $q = 1 - p$. Logo, a expressão para a esperança matemática de $X_k - 1$ será a seguinte:

$$E[X_k - 1] = \sum_{\lambda=0}^{\infty} \lambda \cdot q^\lambda \cdot p. \quad (3)$$

Por outro lado, visto que na população, $N - k$ elementos distintos ainda não foram selecionados, tem-se que $p = (N - k)/N$ é a probabilidade da ocorrência de um sucesso. Segue de (3) que

$$E[X_k - 1] = q \cdot p \cdot \left(\sum_{\lambda=1}^{\infty} \lambda \cdot q^{\lambda-1} \right) = q \cdot p \cdot \frac{d}{dq} \left(\frac{q}{1 - q} \right). \quad (4)$$

Então, de (4) se conclui que $E(X_k - 1) = q/p$. Logo, $E(X_k) = 1 + q/p$, ou seja,

$$E[X_k] = \left(\frac{N}{N - k} \right). \quad (5)$$

O resultado de (5) substituído em (2), resulta na expressão abaixo:

$$E[S_r] = 1 + \sum_{k=1}^{r-1} \frac{N}{N - k} = N \cdot \sum_{k=0}^{r-1} \frac{1}{N - k}. \quad (6)$$

Apesar de o raciocínio utilizado para se deduzir a expressão (6) ser baseado no fato de que a variável X_k se comporta de acordo com uma distribuição geométrica, essa premissa não é indispensável para encontrar o resultado, pois o problema em questão é de contagem. A fim de se obter uma aproximação de (6), cada uma das parcelas pode ser vista como sendo a área de um retângulo com base é unitária e centro no ponto $N - k$, e a altura é o valor $(N - k)^{-1}$, que é a ordenada nesse ponto central da base do retângulo. Decorre dessa interpretação que, a soma das áreas desses retângulos se torna uma aproximação da integral definida da função $f(x) = x^{-1}$ no intervalo fechado $[N - r + \frac{1}{2}, N + \frac{1}{2}]$, seguindo-se a expressão abaixo, conforme [2]:

$$E[S_r] \approx N \int_{N-r-1/2}^{N+1/2} x^{-1} dx = N \cdot \ln \left(\frac{N + 1/2}{N - r + 1/2} \right). \quad (7)$$

Uma conclusão imediata decorrente de (7) é que, no cálculo do valor esperado da variável S_r , a quantidade de extrações necessárias de serem realizadas até que seja incluído o r -ésimo sucesso, tem complexidade $O(n \log n)$. No caso particular em que se tem $r = N$, a expressão (7) toma a forma

$$E[S_N] = N \cdot \sum_{k=0}^{N-1} \frac{1}{N - k}. \quad (8)$$

Levando em conta a interpretação de que os termos do somatório representam áreas de retângulos com base unitária e altura $(N - k)^{-1}$, então têm-se as seguintes relações [2]:

$$\int_1^N \frac{1}{x+1} dx \leq \left(\sum_{k=0}^{N-1} \frac{1}{N - k} \right) - 1 \leq \int_1^N \frac{1}{x} dx. \quad (9)$$

Segue de (9) que

$$\ln(N + 1) - \ln 2 \leq \left(\sum_{k=0}^{N-1} \frac{1}{N - k} \right) - 1 \leq \ln N. \quad (10)$$

De (10) resulta uma limitação para a magnitude do valor esperado para a variável S_N .

$$E[S_N] = N \cdot \left(\sum_{k=0}^{N-1} \frac{1}{N-k} \right) \leq N \cdot (\ln N + 1). \quad (11)$$

Após o estabelecimento dos aspectos de análise do problema estatístico do coletor de cupons, na seção seguinte será mostrado como utilizar a sua relação com a PPM.

IV. A AMOSTRAGEM DE PACOTES

Nesta seção será mostrado como a abordagem da PPM, pode ser modelada de acordo com a metodologia do problema do coletor de cupons. Considerar-se-á a alegoria seguinte para representar o cenário do ataque. Trata-se de um dispositivo formado por uma mesa possuindo diversos buracos no seu tampo, tendo um saco sob cada um, com o qual se pode praticar um jogo de atirar bolas para acertar os buracos. Deve-se estimar a quantidade de bolas a ser arremessada, de modo que todos os buracos sejam atingidos pelo menos por uma bola. Não há limite estabelecido para a quantidade disponível de bolas a serem atiradas.

Aplicando a alegoria do arremesso das bolas nos buracos, ao cenário de um ataque do tipo DoS, podem-se fazer corresponder os pacotes de mensagens às bolas e os roteadores aos buracos. Quando uma bola é arremessada ela poderá, ou não, cair em um buraco, tal qual um pacote pode, ou não, ser marcado em um roteador. As bolas fora dos buracos correspondem aos pacotes não marcados.

A. Aspectos do Modelo

O movimento de um pacote em uma trajetória contendo d roteadores, juntamente com o eventual registro da sua marcação, pode ser representado por uma seqüência, formada pelos símbolos extraídos do conjunto $\{F, S\}$. Cada símbolo é utilizado para representar fracasso (F), ou sucesso (S), com probabilidade p , de um pacote ser marcado em um determinado roteador. Os símbolos são posicionados de modo que representem a ordem crescente da distância à vítima, a partir da extremidade esquerda da seqüência.

Devido à natureza do experimento, qualquer seqüência poderá conter, no máximo, uma ocorrência do símbolo S . Nesse caso, a posição do sucesso entre os elementos da seqüência indica a distância, em saltos, a que o roteador que marcou o pacote se encontra da vítima.

Dessa forma, esse processo de marcação de pacotes se caracteriza como um subconjunto de um experimento de Bernoulli, no qual ocorre um sucesso e $d - 1$ fracassos. Isso significa que no conjunto Ω , dos pacotes que chega até a vítima, identifica-se uma partição $\{\Omega_F, \Omega_S\}$, formada pelos pacotes sem marcação e por aqueles com uma única marcação, respectivamente. Considerando todas as possíveis seqüências oriundas do experimento de Bernoulli com d elementos, sabe-se que a probabilidade de ocorrerem as seqüências com apenas um sucesso é dada por $d \cdot p \cdot (1 - p)^{d-1}$, segundo [5]. Essa é a probabilidade de os d roteadores da trajetória de ataque poderem ser escolhidos para a marcação.

Considere-se a variável aleatória $X : \Omega \rightarrow \mathbb{N}$, que associa a cada pacote recebido a quantidade de experimentos de Bernoulli necessárias para a obtenção de um sucesso [6]. Pela própria definição pode-se ver que $X(\omega) \in \mathbb{N}$, para $\omega \in \Omega$, o que caracteriza X como uma variável aleatória discreta e não-negativa, com valores inteiros.

Sendo $k = X(\omega)$, a expressão da função de massa de probabilidade de X é dada por $p_X(k) = p \cdot (1 - p)^{k-1}$, pois a variável aleatória se comporta de acordo com a distribuição geométrica. O parâmetro da distribuição, p , é a probabilidade de que ocorra um sucesso em um experimento de Bernoulli, isto é, a marcação de um pacote por um roteador. Além disso, convém notar que o valor de X estabelece a que distância o roteador que marcou o pacote se encontra da vítima.

Para determinar quantos pacotes precisam ser utilizados na reconstituição da trajetória de ataque, será considerada a parte da trajetória que vai até o k -ésimo roteador. Naturalmente, para a reconstituição parcial é necessário que se possa obter exemplares dos pacotes atacantes com marcações distintas, correspondendo a cada um dos roteadores que compõem essa parte da trajetória.

O cenário equivale ao do problema da realização de experimentos de Bernoulli até que sejam incluídos todos os k distintos sucessos. Essa exigência sugere a definição de uma outra variável aleatória, S_k , que representa a quantidade de experimentos de Bernoulli necessárias para que se obtenham todos os sucessos até o k -ésimo, inclusive. De acordo com (2), essa variável aleatória pode ser definida como

$$S_k = X_1 + X_2 + X_3 + \dots + X_r, \quad (12)$$

A variável S_k também pode ser interpretada como a quantidade de pacotes necessários de serem obtidos, para que seja representada a trajetória que vai até o k -ésimo roteador. Uma vez que se considere toda a trajetória, que tem comprimento d , sabe-se de (11) que o valor esperado para S_d satisfaz a expressão:

$$E[S_d] \leq d \cdot (\ln d + O(1)). \quad (13)$$

Durante o período do ataque, a vítima recebe uma determinada quantidade de pacotes, representada por $Y : \Omega \rightarrow \mathbb{N}$, uma variável aleatória discreta. A definição que S_d , permite escrever

$$E[S_d] = d \cdot p \cdot (1 - p)^{d-1} \cdot E[Y]. \quad (14)$$

Substituindo (13) em (14), obtém-se a importante relação abaixo, prognosticada em [7]:

$$E[Y] \leq \frac{\ln d}{p \cdot (1 - p)^{d-1}}. \quad (15)$$

A relação em (15) é um limite superior para a quantidade de pacotes que deve ser recebida, a fim de garantir a representatividade da amostra, na reconstrução da trajetória de ataque. A tabela 1 mostra exemplos para essa razão limitante, considerando três valores distintos da probabilidade p e trajetórias tendo comprimentos de até dez saltos.

Tabela 1 - Razão Limitante

d	$p = 0,020$	$p = 0,100$	$p = 0,300$
1	0,0	0,0	0,0
2	35,4	7,7	3,3
3	57,2	13,6	7,5
4	73,6	19,0	13,5
5	87,2	24,5	22,3
6	99,1	30,0	35,5
7	109,8	43,5	84,2
8	119,8	43,5	84,2
9	129,1	51,0	127,0
10	138,1	59,4	190,2

B. Considerações Teóricas

O comportamento da fração em (15) depende da relação entre os elementos p e d . Definindo-se a função real $\xi : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$, dada pela expressão $\xi(x, y) = (\ln(x)/y) \cdot (1 - y)^{x-1}$, para cada valor tomado para y , podem-se enunciar os resultados a seguir.

Lema 1: Sendo $x \in \mathbb{R} - \{0\}$ e $y \in (0, 1)$, então a função $\xi(x, y) = (\ln(x)/y) \cdot (1 - y)^{x-1}$ é monótona crescente.

Demonstração: Considerando $x_1, x_2 \in \mathbb{R} - \{0\}$, tal que $x_1 < x_2$, sabe-se que $\ln x_1 < \ln x_2$. Por outro lado, $(1 - y)^{x_1-1} > (1 - y)^{x_2-1}$, pois $(1 - y) < 1$. Então, é fácil concluir que $\frac{\ln x_1}{(1 - y)^{x_1-1}} < \frac{\ln x_2}{(1 - y)^{x_2-1}}$, ou seja $\xi(x_1, y) < \xi(x_2, y)$. ■

Lema 2: A função $\xi(x, y) = (\ln(x)/y) \cdot (1 - y)^{x-1}$ tem a declividade positiva para todo $x \in \mathbb{R}$, tal que $x > 1$ e $y \in (0, 1)$.

Demonstração: A primeira derivada de $\xi(x, y)$ é dada pela expressão

$$\frac{\partial \xi}{\partial x} = \frac{(1/x) - (\ln(x)) \cdot (\ln(1 - y))}{y \cdot (1 - y)^{x-1}}, \tag{16}$$

cujos denominador $y \cdot (1 - y)^{x-1}$ é sempre positivo. Resta determinar o sinal do numerador $(1/x) - (\ln(x)) \cdot (\ln(1 - y))$. Porém desde que $\ln(1 - y) < 0$, pois $y \in (0, 1)$, conclui-se que o numerador é positivo. Logo, segue o resultado proposto. ■

Lema 3: Sendo $d \in \mathbb{R}$, fixo, e $y \in (0, 1)$, então a função $\xi(d, y) = (\ln(d)/y) \cdot (1 - y)^{d-1}$ atinge o mínimo quando $y = 1/d$.

Demonstração: Considere-se a função auxiliar $f : (0, 1) \rightarrow \mathbb{R}$, dada por $f(y) = y \cdot (1 - y)^{d-1}$, cuja derivada tem por expressão $f'(y) = (1 - yd) \cdot (1 - y)^{d-2}$. É fácil ver que essa derivada se anula em $y = 1/d$. Por outro lado, também se constata que, nesse ponto, a segunda derivada da função, cuja expressão é dada por $f''(y) = (-1) \cdot (1 - yd)^{d-3} \cdot [d \cdot (1 - y) + (d - 2) \cdot (1 - yd)]$, assume um valor negativo. Logo, a função auxiliar atinge um valor máximo em $y = 1/d$ e, em consequência, a função original $\xi(d, y)$ alcança um valor mínimo no mesmo ponto. ■

Os lemas 1 e 2 mostram que não há valor global para a probabilidade p que resulte em uma quantidade mínima de pacotes a ser usado na reconstrução da trajetória de ataque. Por outro lado, a partir da tabela 1 é possível constatar que, localmente, podem ser identificadas condições que minimizam

a quantidade de pacotes necessária à reconstrução da trajetória de ataque. Esse fato é mostrado através do lema 3, através de uma interessante e simples relação entre y , representando um valor de probabilidade, e d .

V. CONCLUSÃO E TRABALHOS FUTUROS

Um importante passo no sentido de estabelecer um rigor matemático no problema de marcação probabilística de pacotes reside no estudo da desigualdade (15). O limite superior mostrado pela mesma representa uma referência, na tarefa de recomposição de uma trajetória de ataque.

Quanto à função $\xi(x, y) = (\ln(x)/y) \cdot (1 - y)^{x-1}$, que se baseia no lado direito da desigualdade (15), a análise teórica da mesma mostra que a relação entre as variáveis x e y , representando respectivamente d e p , não apresenta pontos críticos globais. Em decorrência desse fato, não existem, a priori, valores para essas variáveis que possam ser estabelecidos como ótimos, quando se trata da tarefa de recomposição de uma trajetória de ataque.

Em algumas situações particulares, contudo, é possível obter alguma vantagem da relação entre as mesma, como mostra a tabela 1. O aprofundamento no trato desse problema de amostragem pode motivar trabalhos futuros, com respeito ao valor da probabilidade p . Com efeito, uma associação do resultado do lema 3, com a possibilidade de utilizar valores variáveis para p nos roteadores, poderá vir a ser um importante argumento para aumentar a eficiência do processo, através da redução da quantidade de pacotes necessários para a marcação.

REFERÊNCIAS

- [1] Micah Adler. Tradeoffs in probabilistic packet marking for ip traceback. *ACM Symposium Theory of Computing (STOC)*, pages 19–21, 2002.
- [2] Richard Burden e J. Douglas Faires. *Análise Numérica*. Thomson, S. Paulo, 2003.
- [3] William Feller. *An Introduction to Probability Theory and its Applications - Volume I; Third Edition*. John Wiley Sons, New York, 1968.
- [4] M. T. Goodrich. Efficient packet marking for large-scale ip traceback. *CCS'02*, 2002.
- [5] Darrel Hankerso, Greg A. Harris, and Peter D. Johnson Jr. *Introduction to Information Theory and Data Compression*. CRC Press, New York, 1998.
- [6] Jean Jacod and Philip Protter. *Probability Essentials*. Springer, Berlin, 2000.
- [7] S. Savage, D. Wetherall, A. Karlin, and T. Anderson. Pratical network support for ip traceback. *Proceedings of ACM SIGCOMM 2000*, pages 295–306, 2000.