日本オペレーションズ・リサーチ学会
2005年春季研究発表会

マーキング方式を利用したIPトレースバックの攻撃パス検出効率

千葉大学　*王恵静　OH Keisei
01207040　千葉大学　塩田茂雄　SHIODA Shigeo

1　はじめに

インターネットの特定のサーバに大量のIPパケットを送信し，そのサーバが正常に機能することを妨害する「サービス妨害攻撃（Denial of Service Attack）」が頻発しており，インターネットの脅威となっている．DoS攻撃の被害を最小限に食い止めるには，早期に攻撃パスと攻撃ノードを特定し，攻撃ノードからのパケットを遮断する方法がもっとも有効であり，このため攻撃パスと攻撃ノードを特定するための技術が検討されている．これを「IPトレースバック」と呼ぶ．

IPトレースバックにはこれまでに，逆探知パケット方式，マーキング方式，ダイジェスト方式など様々な手法が提案されている[4]．本稿ではこのうちマーキング方式に着目し，その攻撃パス検出効率，とりわけ，攻撃パスを検出するまでに被害ノードが受信しなければならない総攻撃パケット数の分布および期待値の表式を導く．さらに，攻撃パスの検出効率を最大化するようなマーキング戦略について考察し，この最適マーキング戦略と従来方式の攻撃パス検出効率を比較する．

以下，本稿の構成を示す．2章では，マーキング手法について説明する．3章では，攻撃パスを特定するまでに，被害ノードが受信しなければならない総攻撃パケット数の分布および期待値の表式を導き，期待値を最小化するような最適マーキング戦略について考察する．4章では，最適マーキング戦略と従来方式の攻撃パス検出効率を数値的に比較する．

2　マーキング方式

マーキング方式とは，リンクを通過するパケットのIPヘッダに，当該リンクの情報（両端ノードのIPアドレス，被害ノードからの距離情報）を一定の確率で書き込む（マーキングする）方式である[2, 3, 1]．書き込みはリンクの両端ノードが行う．あるリンクでマーキングされたパケットが，後方リンクで再度マーキングされる場合は，最初に書き込まれた情報は消去（上書き）される．被害ノードは多数の攻撃パケットの中からリンク情報が書き込まれたパケットを抽出・分析し，攻撃パスを構築する．

一般に，リンク情報を書き込めるヘッダ領域は小さいため，多くの提案では，リンク情報を圧縮，ないしは複数のパケットに分割して書き込むような工夫をこらしている．本研究では，簡単のため，リンクを一意に特定できる情報が1つのパケットのヘッダにマーキング（記載）できることを仮定する．この仮定は現実のマーキング方式には必ずしもあてはまらないが，この仮定のもとでの結果を実際のマーキング方式の場合に拡張することは容易である．

3　攻撃パス検出効率の解析

本章では，攻撃ノードがただ一つの場合を想定し，攻撃ノードと被害ノードを結ぶ経路はn本のリンクから構成されているとする．パケットがリンクを通過する際に，ヘッダにリンク情報が書き込まれる確率は全てpに等しいとする．攻撃ノードに近いリンクから順に「リンク1，リンク2，…」というように番号を付与すると，攻撃パケットがリンクiでマーキングされ，さらにマーキング情報が後方リンクで上書きされずに被害ノードに届く確率p_iは以下で与えられる．

$$p_i = p(1-p)^{n-i}$$

なお，被害ノードが受信するパケットにマーキングが施されている確率p_{all}は$p_1 + \cdots + p_n = 1-(1-p)^n$に等しい．

3.1　構成リンクの検出に要するマーキング攻撃パケット数

リンクiの情報がマーキングされた攻撃パケットを被害ノードが受信したとき，「(被害ノードは) リンクiを検出した」と呼ぶこととする．i個の異なるリンクを検出するまでに被害ノードが受信したマーキング攻撃パケットの総数を$X_m^{(i)}$とし，さらに

$$N_m^{(1)} \stackrel{\text{def}}{=} X_m^{(1)}, \quad N_m^{(i)} \stackrel{\text{def}}{=} X_m^{(i)} - X_m^{(i-1)}, \quad (i \geq 2)$$

を定義する．$N_m^{(i)}$は，$i-1$個のリンクを検出してから，i個目のリンクを検出するまでに，被害ノードが受信したマーキング攻撃パケットの総数に相当する．以下が成立する．

補題 3.1.

$$P[N_m^{(i)} = k] = \underbrace{\sum_{l_1=1}^{n}\sum_{l_2=1}^{n}\cdots\sum_{l_i=1}^{n}}_{l_1\neq l_2\neq\cdots\neq l_i} x_{l_1,\cdots,l_i}(y_{l_1,\cdots,l_{i-1}})^{k-1}(1-y_{l_1,\cdots,l_{i-1}}), \tag{1}$$

$$x_{l_1,\cdots,l_i} \stackrel{\text{def}}{=} \frac{p_{l_1}}{p_{all}}\frac{p_{l_2}}{p_{all}-p_{l_1}}\cdots\frac{p_{l_i}}{p_{all}-p_{l_1}-p_{l_2}-\cdots-p_{l_{i-1}}},$$

$$y_{l_1,\cdots,l_i} \stackrel{\text{def}}{=} \frac{p_{l_1}+\cdots+p_{l_i}}{p_{all}}.$$

この結果より，以下のように$N_m^{(i)}$の期待値が得られる．

$$E[N_m^{(i)}] = \underbrace{\sum_{l_1=1}^{n}\sum_{l_2=1}^{n}\cdots\sum_{l_i=1}^{n}}_{l_1\neq l_2\neq\cdots\neq l_i} x_{l_1,\cdots,l_i}\frac{1}{1-y_{l_1,\cdots,l_{i-1}}}$$

$$= \underbrace{\sum_{l_1=1}^{n}\sum_{l_2=1}^{n}\cdots\sum_{l_{i-1}=1}^{n}}_{l_1\neq l_2\neq\cdots\neq l_{i-1}} \frac{p_{l_1}}{p_{all}-p_{l_1}}\frac{p_{l_2}}{p_{all}-p_{l_1}-p_{l_2}}\times$$
$$\cdots\times\frac{p_{l_{i-1}}}{p_{all}-p_{l_1}-p_{l_2}-\cdots-p_{l_{i-1}}} \quad (2)$$

3.2 攻撃パスの検出に要する総攻撃パケット数

攻撃パスを検出するまでに被害ノードが受信する総攻撃パケット数を X とする．以下のように，X の分布は $X_m^{(n)}$ の分布を用いて表すことができる．

補題 3.2.

$$P[X=k] = \sum_{l=1}^{k}\binom{k-1}{l-1}p_{all}^{l}(1-p_{all})^{k-l}P[X_m^{(n)}=l]$$
$$= \sum_{l=1}^{k}\binom{k-1}{l-1}p_{all}^{l}(1-p_{all})^{k-l}P[N_m^{(1)}+\cdots+N_m^{(n)}=l]$$

この結果と式 (1) を組み合わせれば，(n 回の畳み込み演算を行うことにより) X の分布を計算可能である．また，補題 3.2 より，次が直ちに得られる．

$$E[X] = \frac{1}{p_{all}}E[X_m^{(n)}] = \frac{1}{p_{all}}\sum_{i=1}^{n}E\left[N_m^{(i)}\right] \quad (3)$$

従って，式 (2) と (3) を組み合わせることで，$E[X]$ が計算できる．

3.3 検出効率を最大化するマーキング戦略

攻撃元を検出するまでに受信する攻撃パケット数の期待値 $E[X]$ はマーキング確率 $\{p_1, p_2, \cdots, p_n\}$ に依存する．通常は，マーキング確率を任意に制御することはできないが，本章では，この条件を緩め，マーキング確率 $\{p_1, p_2, \cdots, p_n\}$ が任意に制御可能であるとして，$E[X]$ を最小化する $\boldsymbol{p} = \{p_1, p_2, \cdots, p_n\}$ を見つける問題，つまり最適マーキング戦略について考察する．次が得られる．

補題 3.3. $E[X]$ は $\boldsymbol{p} = \{1/n, 1/n, \cdots, 1/n\}$ のとき最小値

$$n(1+\frac{1}{2}+\cdots+\frac{1}{n})$$

を取る．

補題 3.3 で与えられたマーキング戦略では，被害ノードが受信するパケットにマーキングが施されている確率 p_{all} は 1 に等しく，被害ノードは全ての受信パケットの解析を行わなければならない．より現実的な戦略として，確率 p_{all} を 1 より充分小さい値に固定したときの最適マーキング戦略を考えることもでき，その解は $\boldsymbol{p} = \{p_{all}/n, p_{all}/n, \cdots, p_{all}/n\}$ となる．これらは攻撃経路の経路長 (n) が予めわかっている場合にのみ有効な方式であり，現実には実施不可能である．しかし，マーキング方式の検出効率限界を与えていることから，現方式の有効性を見るための比較対象として考察する意義はある．

4 数値例

数値例として，攻撃元を検出するまでに受信する攻撃パケット数の期待値 $E[X]$ を 3.3 章で述べた最適マーキング戦略，現マーキング方式を計算し，表 1 に掲載した．さらに，参考のために Savage[2] が提案した (現マーキング方式での) $E[X]$ の近似評価式

$$E[X] \approx \frac{1}{p(1-p)^{n-1}}(\log n + 0.577215\cdots)$$

も表 1 に示した．なお，$p = 0.025$ とした．$p = 0.025$ は攻撃パスの経路長が 25 ホップ (現在のインターネットにおける End-to-End のホップ数は大半が 25 以下である [2]) のとき，現マーキング方式において $E[X]$ をほぼ最小化するようなマーキング確率に相当する．最適マーキング戦略では，攻撃パスの経路長は既知で，かつ $p_{all} = 1-(1-p)^n$ とした．Savage による近似評価式の誤差は大きい．また，現方式と最適マーキング戦略との差は極めて小さく，現方式の有効性が確認できる．

経路長	最適マーキング戦略	現マーキング方式	
		厳密解	Savage
2	38.3	38.3	33.1
4	55.3	55.5	55.5
6	67.7	68.2	72.6
8	78.0	79.2	88.4
10	87.4	89.6	104.0
12	96.2	99.8	119.9
14	104.6	110.1	136.7

表 1 攻撃パスを検出するまでに被害ノードが受信しなければならない攻撃パケット数の期待値

参考文献

[1] T. Ogawa, F. Nakamura, and Y. Wakahara. Branch label based probabilistic packet marking for counteracting DDoS attacks. *IEICE Trans. Commun.*, E87-B(7):1900–1909, 2004.

[2] A. Savage, D. Wetherall, A. Karlin, and T. Anderson. Network support for IP traceback. *IEEE/ACM Trans. Networking*, 9(3):226–237, 2001.

[3] D. Song and A. Perrig. Advanced and authenticated techniques for IP traceback. *IEEE INFOCOM*, 2001.

[4] 大江将史, 門林雄基, 山口英. 階層型 IP トレースバック機構の提案. **電子情報通信学会論文誌**, J85-B(8):1313–1322, 2002.