社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－DPS－134 (12)
2008－CSEC－ 40 (12)
2008／3／6

サンプリング確率を変動させたIPトレースバック方式の考察

唐沢 智之† 双紙 正和‡ 宮地 充子†

†北陸先端科学技術大学院大学 情報科学研究科
923-1292 石川県能美市旭台 1-1
{s0610026, miyaji}@jaist.ac.jp

‡広島市立大学 大学院情報科学研究科
731-3194 広島市安佐南区大塚東三丁目 4 番 1 号
soshi@hiroshima-cu.ac.jp

あらまし ネットワークにおける脅威の一つに，分散サービス不能攻撃 (DDoS 攻撃) が挙げられる．その対策の一つとして IP トレースバックが研究されており，中でも，パケットマーキング法とロギング法を効率的に組み合わせた Li らの方式が有望視されている．本研究では，パケットサンプリングの相関を Li らの方式より向上させた，効率のよいトレースバック方式を提案する．さらに，提案方式の性能を評価するために，詳細な理論的解析を行う．

An Efficient IP Traceback Scheme with Variable Packet Sampling Probabilities

Tomoyuki Karasawa † Masakazu Soshi ‡ Atsuko Miyaji †

†School of Information Science, Japan Advanced Institute of Science and Technology
1-1, Asahi-dai, Nomi-shi, Ishikawa, 923-1292, Japan
{s0610026, miyaji}@jaist.ac.jp

‡School of Information Science, Hiroshima City University
3-4-1 Ozuka-Higashi, Asa-Minami-Ku, Hiroshima, 731-3194, Japan
soshi@hiroshima-cu.ac.jp

Abstract One of serious threats on the Internet is a distributed denial of service (DDoS) attack and IP traceback has been studied as an effective countermeasure against DDoS attacks. In this paper we propose an efficient traceback scheme, which improves correlation of packet sampling in DDoS Attacks.

1 はじめに

近年，インターネットにおけるセキュリティの脅威が増しているが，その中でも特に深刻な被害をもたらす攻撃の一つとして，分散サービス不能攻撃 (Distributed Denial of Service Attack : DDoS 攻撃) が挙げられる．DDoS 攻撃とは，複数の攻撃者 (Attacker) が特定のサーバ (Victim) へ不正なパケットを大量に送りつけることで，通信路やリソースを溢れさせ，サービスを停止させる攻撃である．

現状では DDoS 攻撃に対する有効な対策がいまだ確立していない．これは DDoS 攻撃における攻撃者の数は，数千〜数万と大規模であることに加え，パケットの発信元の IP アドレスを記録するヘッダである “Source IP Address” が攻撃者によって偽造が容易なためである．

現在，DDoS 攻撃の有効な対策法の一つとして “IP トレースバック” が研究されている．IP トレースバックとは，攻撃者と Victim を結ぶ経路上におけるそれぞれのルータが，中継するパケットに対し “痕跡” を残し，Victim とルータがそれらを解析することにより攻撃の発信元を特定する技術である．IP トレースバックは，攻撃者の痕跡を残す “サンプリング” と，痕跡を解析し，攻撃経路を復元する “トレースバック” から構成されている．

本研究では，2004 年に Li らによって提案された複合型 IP トレースバック方式 [1] に着目し，パケットにカウンタ機能を実装することで，Li らの方式の問題点を克服した IP トレースバック方式を提案する．本論文は，CSS2007 [2] にて発表した本方式に，詳細な理論的解析を行ったものである．

2 章では提案方式を説明し，3 章ではエントロピーを用いた理論的評価を行う．4 章にてシミュレーションと考察をし，今後の展望をまとめる．

2 提案方式

2.1 基本的なアイデア

本研究では，パケットサンプリングの相関を Li らの方式より向上させた，効率のよいトレースバック方式を提案する．さらに，提案方式の性能を評価するために，詳細な理論的解析を行う．

For each packet P
with probability $\frac{(P.counter)^{\alpha}+\beta}{M}$
$P.counter \leftarrow P.counter + 1$;
Store digest;

図 1: 提案サンプリングアルゴリズム

提案方式では，Li らが考案した隣接 2 ルータ間の相関ではなく，経路全体で相関を高めることを考える．そのため，Li らの方式で使用された 1bit のマークを，4bit のカウンタへ拡張する．パケット P のカウンタを P.counter とし，初期値は 0 とする[1]．そして，経路上のルータはパケット P を確率的にサンプリングし，もしサンプリングされた場合，P.counter の値を 1 増やす．すなわち，パケット P における P.counter の値は，経路上の複数のルータによって P がサンプリングされた回数を表すことになる．そこで，カウンタの値が大きいパケットほど，経路上の複数のルータに多くの情報が格納されていることになり，トレースバックの際に有用であると考えられる．

以上より，カウンタの値が大きいパケットを優先的に利用することができれば，より効率的なトレースバックが可能となることがいえる．

2.2 サンプリング

カウンタの値が大きいパケットを優先的に利用するためには，直感的にいえば，カウンタの値が大きいパケットをより高い確率でサンプリングし，カウンタの値が小さいパケットはより小さい確率でサンプリングするようにすればよい．このためには，実数 $\alpha \geq 1$, β, M を定数とし，ルータは，カウンタの値 P.counter に依存した確率

$$p = \frac{(P.counter)^{\alpha} + \beta}{M} \tag{1}$$

によってサンプリング動作を行えばよい．パケットがサンプリングされた場合，カウンタを +1 インクリメントする．インクリメント後に，パケット P のダイジェストをルータへ保存する．ダイジェストには，Li らの方式と同様に Bloom Filter というデータ構造を用いる．

以上による，提案アルゴリズムを図 1 に示す．

2.3 トレースバック

Li らの方式と同様に，Victim に到着した攻撃パケットを用いて，トレースバックを行う．トレースバックは，Victim が攻撃を受けたことを感知した瞬間に開始される．提案方式では，攻撃パケット L_v から，カウンタ値 P.counter $\geq$ threshold を満たすパケットを L_v' として，トレースバックに利用する．カウンタの値が大きいパケットはより高い確率でサンプリングされているためである．threshold は，Victim が任意に決めることができるパラメータであり，Li らの方式と比べて，トレースバックに用いるパケット数を格段に少なくすることが可能である．

[1]カウンタのための領域としては，IP Identification Field を用いることが考えられる．

アルゴリズムは，Li らのトレースバック方式と同様に，L_v' を隣接するルータ R_1 へ送信し，もし L_v' の要素が R_1 に含まれていた場合，R_1 を攻撃経路上であると断定し，隣接するルータ R_2 へ L_v' を送信する．Li らとの相違点は，新たに集合 L_{R_1} を作成しない点である．これは提案方式の L_v' が限りなく小さいため，Bloom Filter の false positive (偽陽性) 2^{-k} が無視できるからである．

3 理論的評価

3.1 定数 α, β, M の決定

各ルータのサンプリング確率 p は (式 1) と定義した．シミュレーションによる実験を行うためには，定数 α, β, M の値を定め，サンプリング確率を決定する必要がある．ここでパケット P のカウンタ P.counter が取り得る最大値と最小値を考察する．P.counter の最大値は，攻撃者から発信されたパケット P が，Victim に届くまでに経由した全てのルータでサンプリングされた回数である．つまり，事前にトレースバックを行うホップ数 d が決まっていれば，P.counter の最大値が定まる．ネットワークを流れるパケットが経由する平均ホップ数は 16 [?] であることから，$n = 16$ を仮定する．$n = 16$ のときの確率 p が 1 以下となればよいので，確率 p は，$p = \frac{16^{\alpha}+\beta}{M} \leq 1$ となる．P.counter の最小値は，カウンタの値が 0 のときであり，サンプリングされた回数が 0 回の時の確率である．この確率を初期確率 IPr とすると，$\frac{\beta}{M} = IPr$ と定義できる．

Li らの方式のサンプリング確率 $p = 0.03$ よりも低い確率，$IPr = 0.01$ とし，$\alpha = 2$ の増加関数とすると，定数 β, M はそれぞれ，$\beta = 2.58586$, $M = 258.586$ と求まる．

3.2 ルータ i におけるサンプリング確率とカウンタ値

ルータ i におけるサンプリング確率 p は，式 (1) から，カウンタ値に依存していた．カウンタ値によるサンプリング確率の挙動を，ルータごとのサンプリング確率を確率変数 X_{p_i} を用いて求めた．

仮定するネットワーク

- 攻撃者と Victim を結ぶ一直線の経路を考える．攻撃者と隣接するルータを R_1 とし，以下 R_2, $R_3, \cdots$, R_{n-1}, R_n, Victim と隣接するルータを R_n とする．n は Victim と攻撃者の間のルータの数である．

ネットワークを流れるあるパケット P を考え，P に対する確率変数 X_{p_i} を以下のように定義する．

$$X_{p_i} = \begin{cases} 1 & \text{ルータ } R_i \text{ で P がサンプリング} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

パケット P がルータ R_i に到着し，ルータに参照されたときの P のカウンタ値を表す確率変数 X_{c_i} によって，X_{p_i} は以下のように求められる．

$$\Pr(X_{p_i} = 1 | X_{c_i} = l) = \frac{l^{\alpha} + \beta}{M}$$

よって，

$$\Pr(X_{p_i}=1)=\sum_{l=0}^{i-1}\frac{l^{\alpha}+\beta}{M}\cdot\Pr(X_{c_i}=l) \qquad (3)$$

次に，$\Pr(X_{c_i}=l)$ について考える．R_1 におけるカウンタ値の初期値は 0 であるから，

$$\Pr(X_{c_1}=l)=\begin{cases}1 & l=0 \text{ のとき}\\ 0 & \text{otherwise}\end{cases}$$

$$\Pr(X_{c_2}=l)=\begin{cases}\frac{\beta}{M} & l=1 \text{ のとき}\\ 1-\frac{\beta}{M} & l=0 \text{ のとき}\\ 0 & \text{otherwise}\end{cases}$$

である．

一般的には，

$$\begin{aligned}\Pr(X_{c_i}=l) &= \Pr(X_{c_i}=l|X_{c_{i-1}}=l-1)\times\\ &\quad \Pr(X_{c_{i-1}}=l-1)+\\ &\quad \Pr(X_{c_i}=l|X_{c_{i-1}}=l)\cdot\Pr(X_{c_{i-1}}=l)\\ &= \frac{(l-1)^{\alpha}+\beta}{M}\cdot\Pr(X_{c_{i-1}}=l-1)+\\ &\quad \left(1-\frac{l^{\alpha}+\beta}{M}\right)\cdot\Pr(X_{c_{i-1}}=l) \qquad (4)\end{aligned}$$

である．以下，$\Pr(X_{c_i}=l)$ は，再帰的に求めることができる．ただし，R_i においてとりうるカウンタ値の最大値は，$i-1$ であり，また最小値は 0 であり，非負である．よって，$l<0$ または $i-1<l$ のとき，$\Pr(X_{c_i}=l)=0$ である．

以上から，式 (2) を求めることができる．式 (2) を用いたルータ $R_i(1\le i\le 16)$ によるサンプリング確率は，図 2 における “理論値” の通りである．

3.3 エントロピーによる評価

ルータ R_i から R_{i-1} へのトレースバックを考える．R_{i-1} が攻撃経路上のルータであるかは，R_i のログの，少なくとも 1 つ以上が R_{i-1} のログと一致するかによる．ここでは，R_{i-1} が R_i のログを少なくとも 1 つ以上持つかどうかを，エントロピーを用いて評価する．

3.3.1 モデリング

はじめに，以下の記法を定義する．

記法

- N_p : Victim がトレースバックに用いる攻撃パケット群
- $d_i=d$:
  ルータ R_i を通過した攻撃パケットの割合．後述するが，全ての d_i は同一の値をとるため，簡略化して以後 d と表す．
- k : Bloom filter に用いるハッシュ関数の数
- $f=2^{-k}$: Bloom filter の False positive の確率

確率変数

- X_{t_i} : R_i にサンプリングされた攻撃パケットの数
- X_{f_i} : $Binom(N_p-X_{t_i},f)$: N_p を R_i の Bloom filter に通したときに発生する false positive の数
- Y_{t_i} : R_{i-1} へトレースバックする際に使用される攻撃パケットの数
  すなわち，R_i と R_{i-1} において，共通してサンプリングされたパケットの数である．
- Y_{f_i} : $Binom(X_{t_i}+X_{f_i}-Y_{t-1},f)$: $X_{t_i}+X_{f_i}$ を R_{i-1} の Bloom filter に通したときに発生する false positive の数

以上のパラメータを用いて，さらに以下の確率変数を考える．

- $X=X_{t_i}+X_{f_i}=L_{R_i}$: R_{i-1} へのトレースバックに使用するパケットの数
  R_i にサンプリングされた攻撃パケットと，N_p を R_i の Bloom filter に通したときに発生した false positive の数の和．R_i の本来のログであるパケットの集合 (総数 X_{t_i}) と，本来のログでないが，Bloom filter によって本来のログと誤って判定されたログ (総数 X_{f_i}) を合わせたもの．
- $Y=Y_{t_i}+Y_{f_i}$: 上記の L_{R_i} と，R_{i-1} の Bloom filter が一致した攻撃パケットの数の和．

victim によるトレースバックに使用される攻撃パケットのうち，少なくとも一つのパケットが R_{i-1} によってサンプリングされることを意味する確率変数 Z を以下のように定義する．

$$Z=\begin{cases}1 & \text{if } X_{t_{i-1}}>0\\ 0 & \text{otherwise}\end{cases} \qquad (5)$$

3.3.2 各確率変数の導出

R_i にサンプリングされた攻撃パケットの数 :
パケットにおけるサンプリングは，パケットごとに独立に行われる．よって，全てのパケットにおいて X_{p_i}，X_{c_i} の確率分布は等しくなる．そこで，$\Pr(X_{t_i}=k)$ は，

$$\begin{aligned}\Pr(X_{t_i}=k) &= \binom{N_p d_i}{k}\Pr(X_{p_i}=1)^k\times\\ &\quad (1-\Pr(X_{p_i}=1))^{N_p d_i-k} \qquad (6)\end{aligned}$$

N_p を R_i の Bloom filter に通したときの false positive の数 :
Victim は攻撃パケットの集合 L_v を用いて R_i から R_{i-1} へトレースバックを行う．X_{f_i} は，R_i の Bloom Filter へ L_v を通したときの false positive の数を表す

$$\begin{aligned}&\Pr(X_{f_i}=k)= \qquad (7)\\ &\sum_{n=0}^{N_p d_i}\Pr(X_{t_i}=n)\binom{N_p-n}{k}f^k(1-f)^{N_p-n-k}\end{aligned}$$

R_{i-1} へ送る攻撃パケットの数 ：

N_p と，R_i のログの中身と一致したパケット数を表す確率変数を X とする．R_{i-1} の Bloom filter へ通すために送る攻撃パケットの数 X の確率変数は以下の様になる．

$$\Pr(X=k)=\sum_{n=0}^{\min(k,N_p d_i)}\Pr(X_{t_i}=n)\cdot\Pr(X_{f_i}=k-n) \tag{8}$$

R_i と R_{i-1} のログに共通するパケットの数 ：

R_i と R_{i-1} のログに共通するパケットの数である Y_{t_i} について考察する．R_{i-1} が受け取ったパケットのカウンタの値が l であるとき，そのパケットを R_{i-1} と R_i が順にサンプリングする確率は，以下のように表せる：

$$\Pr(X_{p_i}=1,X_{p_{i-1}}=1|X_{c_{i-1}}=l)=\frac{(l+1)^\alpha+\beta}{M}\cdot\frac{l^\alpha+\beta}{M}$$

これから，

$$\Pr(X_{p_i}=1,X_{p_{i-1}}=1)=\sum_{l=0}^{i-2}\frac{(l+1)^\alpha+\beta}{M}\cdot\frac{l^\alpha+\beta}{M}\cdot\Pr(X_{c_{i-1}}=l)$$

とできる．

そこで，Li らの解析と同様に，Y_{t_i} は二項分布

$$Binom(X_{t_{i-1}},\Pr(X_{p_i}=1,X_{p_{i-1}}=1)) \tag{9}$$

に従っているとすることができる．

3.3.3 Z のエントロピーの導出

以上で定義した確率変数を用いて，条件付きエントロピーの定義より，Z は以下のように計算できる．

$$\begin{aligned}H(Z|X,Y)=&-\sum_{m=0}\sum_{j=0}\Pr(X=m,Y=j,Z=1)\times\log_2\frac{\Pr(X=m,Y=j,Z=1)}{\Pr(X=m,Y=j)}\\&-\sum_{m=0}\sum_{j=0}\Pr(X=m,Y=j,Z=0)\times\log_2\frac{\Pr(X=m,Y=j,Z=0)}{\Pr(X=m,Y=j)}\end{aligned} \tag{10}$$

$H(Z|X,Y)$ が低い値ほど，トレースバックの成功確率が高くなる．また，

$$\Pr(X=m,Y=j,Z=a)=\Pr(X=m,Y=j|Z=a)\Pr(Z=a) \tag{11}$$

である．

今，Z の取り得る値は，$Z=\{0,1\}$ であるので，それぞれ以下のように求めることができる．

$Z=1$ のとき ：

$Z=1$ のとき，式 (11) の右辺第一項はさらに，

$$\begin{aligned}&\Pr(X=j,Y=m|Z=1)\\&=\Pr(X=j|Z=1)\Pr(Y=m|X=j,Z=1)\end{aligned} \tag{12}$$

となる．また，式 (12) 右辺第二項は，

$$\begin{aligned}&\Pr(Y_{t_i}+Y_{f_i}=m|X=j,Z=1)\\&=\sum_{k=0}^{\min(m,N_p d_i)}\Pr(Y_{t_i}=k|X=j,Z=1)\times\\&\quad\Pr(Y_{f_i}=m-k|X=j,Y_{t_i}=k,Z=1)\end{aligned} \tag{13}$$

特に，

$$\Pr(Y_{f_i}=m-k|X=j,Y_{t_i}=k,Z=1)=\binom{j-k}{m-k}f^{m-k}(1-f)^{j-m} \tag{14}$$

さらに，式 (12) 右辺第一項を求めたい．今，確率変数 $X(=X_{t_i}+X_{f_i})$ と Y_{t_i} について，次の条件を満たす確率変数 W_i を考える．

$$X_{t_i}=Y_{t_i}+W_i \tag{15}$$

Y_{t_i} は，R_{i-1}，R_i の両方にサンプリングされたパケットの数を表すので，W_i は，R_i でサンプリングされたが，R_{i-1} でサンプルされなかった攻撃パケットの数に他ならない．W_i は以下のように表せる：

$$\Pr(X_{p_i}=1,X_{p_{i-1}}=0|X_{c_{i-1}}=l)=\frac{l^\alpha+\beta}{M}\cdot\left(1-\frac{l^\alpha+\beta}{M}\right)$$

これから，

$$\Pr(X_{p_i}=1,X_{p_{i-1}}=0)=\sum_{l=0}^{i-2}\Pr(X_{p_i}=1,X_{p_{i-1}}=0|X_{c_{i-1}}=l)\cdot\Pr(X_{c_{i-1}}=l)$$

とできる．

よって，先ほど求めた Y_{t_i} と同様に，W_i もまた二項分布

$$Binom(M_p d_i-X_{t_{i-1}},\Pr(X_{p_i}=1,X_{p_{i-1}}=0))$$

に従っているということができる．

よって式 (15) を利用して，(13) 右辺第一項を求める．

$$\begin{aligned}&\Pr(Y_{t_i}=k|X=j,Z=1)\\&=\sum_{l=0}^{j}\Pr(X_{f_i}=l)\times\\&\quad\Pr(Y_{t_i}=k|X_{t_i}=j-l,X_{f_i}=l,Z=1)\end{aligned}$$

よって，

$$
\begin{aligned}
&\Pr(Y_{t_i}=k|X_{t_1}=j-l, X_{f_i}=l, Z=1)\\
&= \sum_{g=k}^{N_p d_i} \Pr(X_{t_{i-1}}=g)\\
&\quad \times \Pr(Y_{t_i}=k, W_i=j-l-k|X_{t_i}=j-l,\\
&\quad X_{f_i}=l, X_{t_{i-1}}=g, Z=1)\\
&= \sum_{g=k}^{N_p d_i} \binom{N_p d_i}{g} \Pr(X_{p_{i-1}}=1)^g \cdot\\
&\quad (1-\Pr(X_{p_{i-1}}=1))^{(N_p d_i-g)}\\
&\quad \times \binom{g}{k} \Pr(X_{p_i}=1, X_{p_{i-1}}=1)^k \cdot\\
&\quad (1-\Pr(X_{p_i}=1, X_{p_{i-1}}=1))^{g-k})\\
&\quad \times \binom{N_p d_i-g}{j-l-k} \Pr(X_{p_i}=1, X_{p_{i-1}}=0)^{j-l-k} \cdot\\
&\quad (1-\Pr(X_{p_i}=1, X_{p_{i-1}}=0))^{N_p d_i-g-j+l+k}
\end{aligned}
$$

となる．

$Z=0$ のとき ：

$$
\begin{aligned}
&\Pr(X=m, Y=j|Z=0)\\
&= \Pr(X=m)\binom{m}{j} f^j (1-f)^{i-j}
\end{aligned}
$$

$$
\begin{aligned}
&\Pr(X=m, Y=j)\\
&= \Pr(X_{t_{i-1}}=0)\Pr(X=m, Y=j|Z=0) +\\
&\quad \Pr(X_{t_{i-1}}>0)\Pr(X=m, Y=j|Z=1)
\end{aligned}
$$

エントロピーの値

$i=3, N_p=100, d=\frac{1}{10}$ のとき，式 (10) によって得られるルータ R_i におけるエントロピーの値は，0.45 となった．これは，Li らの方式で示された 0.65 [2] よりも低い値であり，本方式のトレースバックの成功確率が高いことが分かる．

4 シミュレーションによる評価

4.1 攻撃のモデル

この節では，提案方式をシミュレーションによって評価する．4.2 節と同様のネットワークのモデルを考える．攻撃パケット数 $n=100,000$，ホップ数 $i=16$，カウンタ値 $P.\mathrm{counter}=0$ のときの初期確率 $IPr=0.01$ とし，確率 p を決定するための定数はそれぞれ $\alpha=2$，$\beta=2.58586$，$M=258.586$ である．

4.2 ルータごとのサンプリング確率の変化

攻撃のモデルにおけるシミュレーションによって，サンプリング確率を求めた．4 章にて理論的に求めたルータごとのサンプリング確率と，実験から得られたデータを比較した表が図 2 である．

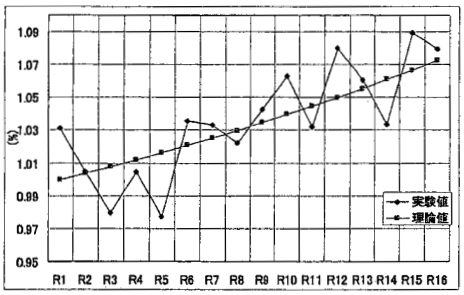

図 2: サンプリング確率の期待値と実験値の比較．

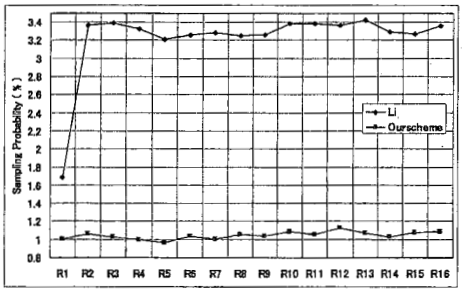

図 3: ルータごとのサンプリング確率．提案方式と Li らの方式との比較

理論値は緩やかに増加しているのに対し，実験値は振幅が大きいが，これは，乱数による偏りによると思われる．しかし概ね理論値に従った値であると言える．

図 3 は，ルータごとの Li らの方式と，提案方式のサンプリング確率である．Li らの方式は，推奨値である $p=3.3\%$ を用いて実装し，提案方式は初期確率 $IPr=1.0\%$ を用いて実装した．提案方式は，Victim に近くなるほどカウンタ値が大きくなり，サンプリング確率がより高い値を返すことが予想されたが，実験したところでは，各ルータがほぼ同確率でサンプリングされている．Victim に近いルータ群の方が若干割合が多くなるが，予想したほど大きい値にはならなかった．

4.3 α の評価

ルータは α に依存した式を用いてサンプリング確率を導出している．α によって，サンプリング確率と，カウンタ値が変化する様子を実験により求め，グラフを用いて表現した．

図 4 は，$0.1<\alpha<2$ を満たす α について，ルータごとに記憶されたログの量を示している．縦軸がログの量（パケットの個数）で，横軸がルータである．R_1 は攻撃者と隣接するルータであり，R_{16} は Victim と隣接するルータである．

全ての α について，ログの総量は，Victim に近づく

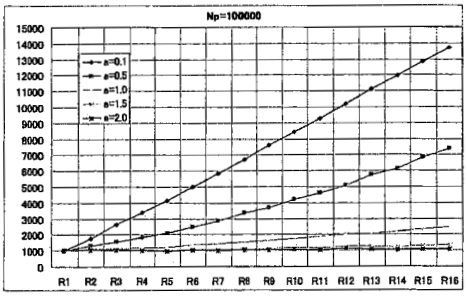

図 4: α の違いによるログの変動

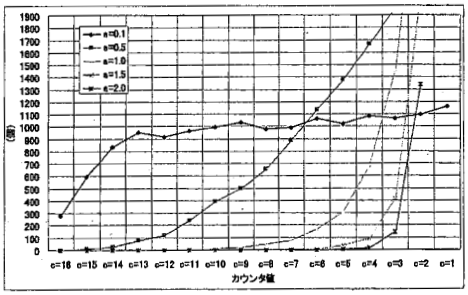

図 5: α の違いによるカウンタ値の変動

に従って増している．これはパケットのカウンタ値が高くなるためである．

図 5 は，Victim が受信した攻撃パケットのカウンタ値別の内訳である．縦軸がパケットの個数，横軸がカウンタ値である．

4.4 経路の復元率

図 6 は，カウンタの値ごとの経路の復元率である．この値が 100%のとき，トレースバックによって経路が復元されたことを意味する．この図により，カウンタ値が 4 以上 (threshold = 4) のパケットは 28 個存在し，その 28 個を用いてトレースバックを行ったとき復元率が 100%となっていることがわかる．すなわち，今回の実験では，threshold = 4 が最適値と言える．

また，図 7 では，Li らの方式の復元率を求めた．Li らの方式では，カウンタを用いるように，特定のパケットを選ぶことができない．そこで，乱数を用いて無作為に 10, 20, ... , 100 個の攻撃パケットを選び，個数毎にそれぞれ 100 回，経路の復元を行い平均を求めた．提案方式では，Threshold = 4 のを満たすパケットは，28 個存在し，その時の復元率は 100%であったが，Li らの方式では，無作為に選んだ 30 個をトレースバックに使用した場合の平均の復元率は，わずか 60%であった．

カウンタ値	復元率	パケット数
6以上	0	0
5以上	81.13%	5
4以上	100%	28
3以上	100%	161
2以上	100%	1405
1以上	100%	14806

図 6: 提案方式：カウンタ値以上のパケットによる復元率

パケット数	復元率(%)
10	27.68
20	48.06
30	61.56
40	69.5
50	80.25
60	85.43
70	88.62
80	91.12
90	93.93
100	94.5

図 7: Li らの方式：復元率

5 まとめと今後の課題

[2] では，パケットサンプリングの相関を Li らの方式より向上させた，効率のよいトレースバック方式を提案した．本論文では，さらに，提案方式の性能を評価するために，詳細な理論的解析を行った．

今後の課題は，シミュレーション環境を DoS 環境から DDoS 環境へ拡張し，有効性を確かめることである．また，カウンタのビット数に応じた定数 α, β, M の最適値を理論的に求めることが必要である．

参考文献

[1] J. Li, M. Sung, J. Xu and L. Li, "Large-Scale IP Traceback in High-Speed Internet: Pratical Techniques and Theoretical Foundation", IEEE Symposium on *Security and Privacy, 2004*, pp. 115–129, May 2004.

[2] T. Karasawa, M. Soshi, and A. Miyaji, "Consideration for an IP traceback method with counters", *Computer Security Symposium*, pp. 453–458, Nov 2007.