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

2007－DPS－130 (18)
2007－CSEC－ 36 (18)
2007／3／1

DoS攻撃に対する偽造耐性をもつ改良パケットマーキング法の提案と評価

竹本 秀樹† 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

{h-takemo,soshi,miyaji}@jaist.ac.jp

あらまし DDoS攻撃に対する有効な対策の一つに，パケットマーキング法を用いたパケットフィルタリング技術がある．これは，送られてくるIPデータグラムのパケット(以下パケットと呼ぶ)に，ルータのアドレスなどの経路情報に基づいてマーキングを行い，パケットを廃棄する技術である．通常攻撃者は多数存在し，なおかつパケット中のパラメータを偽造して送ってくるので，それぞれのパケットが送られてくる攻撃経路に対して一意なマーキング値を計算することは難しい．そこで筆者らは，上記の偽造に対してより耐性を持つ方式(以下提案方式1と呼ぶ)と，16ホップ以上の経路情報をマーキングする方式(提案方式1+2と呼ぶ)を提案し，実験を定性的に評価した[8]．

本研究は，[8]に示す実験的評価の裏づけとなる理論的根拠を示し，さらに実験を改良することで提案方式1，1+2いずれもPi方式よりもよいマーキングを行うことを示す．

An Approach and evaluation of improved unforgeble packet marking scheme against DoS attacks

Hideki Takemoto† 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
{h-takemo,soshi,miyaji}@jaist.ac.jp

Abstract One of the effective countermeasures against DDoS attacks is packet filtering, which marks routing information on each packet and drops attack packets based on the information. Unfortunately, previous packet filtering schemes have a drawback such that they cannot efficiently deal with the attack packets forged by adversaries. Therefore in order to overcome such difficulties we proposed simple and efficient packet filtering schemes in [8]. We show the proof of experimental evaluation to show in [8] and that our scheme 1, 1+2 is better than a Pi scheme by improving an experiment more.

1 はじめに

インターネットの普及と共に，悪意あるユーザからの攻撃に対するネットワークセキュリティの必要性が高まっている．その中でも，サービス不能攻撃(Denial of Service Attack: 以下DoS攻撃)が脅威となっている．これは，悪意あるユーザが，特定のサーバに対し大量のパケットを送ることで，そのサーバの機能を停止させる攻撃である．さらに近年では，複数の攻撃者がDoS

攻撃を行う分散サービス不能攻撃 (Distributed Denial of Service Attack: 以下 DDoS 攻撃) が大きな問題となっている．DoS 攻撃においては，攻撃者は通常，自らの身元を隠すためにパケット中のパラメータ (例えば，パケットの平均寿命を表す Time To Live (TTL)，距離を表すホップ数，発信元 IP アドレスなど) を偽造する．そのため，DoS 攻撃への防御対策を行う上で，パケットの偽造や複数の攻撃者からの攻撃への耐性が必要となる．

DDoS 攻撃に対する有効な対策の一つに，パケットマーキング法を用いた Pi 方式 [3] がある．この方式では，各ルータが一つのパケットに自らのアドレスに基づくマーキングを施すことにより，各パケットに経路毎の固有の値を割り振る．このスキームは，他のフィルタリング方式と比較するとよい性能を持つことが [5] で実験的に示されている．

しかし，Pi 方式は，TTL の偽造やマーキング値偽造に対してアドホックな対策しかしておらず，統一的な対策が望まれる．そこで筆者らは，上記の偽造に対してにより耐性を持つ方式 (以下提案方式 1 と呼ぶ) と，16 ホップ以上の経路情報をマーキングする方式 (提案方式 1+2 と呼ぶ) を提案し，実験を定性的に評価した [8]．

本研究は，[8] に示す実験的評価の裏づけとなる理論的根拠を示す．また，実験の評価を改良することにより提案方式 1，1+2 いずれも Pi 方式よりもよいマーキングを行うことを示す．

本研究は以下のように構成される．第 2 章では，Pi 方式と筆者らの提案したマーキング方式を示す．さらに，第 3 でスキームの理論的評価とその予想を立て，第 4 章でその予想に対する実験を行う．そして 5 章と，新しく 6 章に示すパラメータを用いて評価した．その実験結果から第 7 章で考察を行い，最後にまとめとする．

2 既存方式

2.1 [YPS03]-Pi 方式

この節では，フィルタリング方式 (マーキング方式) として代表的な，Yaar らによる Pi 方式 [3] を説明する．この方式では，パケットが経由する毎にルータが自らの IP アドレスなどの情報を IP ヘッダ中の identificaion field に書き込む．これにより，$2^{16}(= 65536)$ 個の異なる経路パターンを作ることが可能となる．

ルータが出力するマーキング値 b は，edge marking を用いて，そのルータの IP アドレスと直前のルータの IP アドレスを markingbits 関数に入力した結果となる．markingbits 関数は，MD5 によるハッシュ値を返す．マーキング位置 bitpos は TTL を元に計算される．

2.2 [TSM06]-提案方式 1: 基本マーキングアルゴリズム

Pi 方式では，TTL の値に応じてマーキングを書き込むビット位置が変化していく．そこで，TTL の値を偽造することにより，攻撃者がマーキング値を変えることができるため，その値をフィルタリングに利用することが困難である．

[8] では，Pi 方式と比べ，TTL やマーキング値の偽造に関して強い耐性を持つ方式を提案した．基本的なアイディアとしては，Pi 方式のように以前のマーキングをそのまま用いるのではなく，「圧縮」して用いる．今，攻撃者が攻撃対象に向けてパケットを送り，n 個のルータを経由する場合を考える．そのとき，攻撃者に最も近いルータを R_1，攻撃対象の直前のルータを R_n とすると，$P_n = R_n + aR_{n-1} + \cdots + a^{n-2}R_2 + a^{n-1}R_1$ (ただし，$0 < a < 1$) となる多項式表現できるマーキング値を計算すればよい．本研究で用いるアルゴリズムを図 1 に示す．このアルゴリズムでは，左シフトを行うことで $n = 1$ のとき $a = \frac{1}{2}$，$n = 2$ のとき $a = \frac{1}{4}$ としている．このようにすることで攻撃者の偽造の影響を小さくでき，かつ，より多くのルータの位置情報をマーキングできる．

```
p = mark of the packet
```

```
mark(p, CurrIP, PrevIP, n) {
    b = markingbits (CurrIP, PrevIP);
    return(b || p) ≫ n);
}
```

図 1: 提案方式 1:基本マーキングアルゴリズム

2.3 [TSM06]-提案方式 1+2: ルータの条件付きマーキングアルゴリズム

Pi マーキング方式や提案方式 1 では，攻撃経路の情報を 1 パケットの identification field にマーキングすることを前提としていた．このとき，攻撃対象と攻撃者との距離が遠いほど，攻撃者に近いルータ情報が上書きされてしまい，16 ホップ以上では経路を判別できない．この問題について，以下のような対策を考える．すなわち，攻撃経路のすべての情報を 1 パケットに書き込むのではなく，2 パケットを利用してマーキングすることを考える．こうすることによって，マーキングするルータを選別することができ，より長い攻撃経路でも上書きがおこらないようにすることができる．

```
flag = 1 bit memory of the router

mark2 (p, CurrIP, PrevIP, n) {
 if flag ⊕ markingbits (LSB(CurrIP))
  then mark (p, CurrIP, PrevIP, n)
 flag = ¬ flag }
}
```

図 2: 提案方式 1+2:ルータの条件付きマーキングアルゴリズム

3 スキームの理論的評価

3.1 理論的評価

[8] では，Pi 方式よりも，攻撃者のマーキング値がどこにあるか特定しやすくする方式を提案した．3 章では，提案方式と Pi 方式について定量的に評価を行う．

3.1.1 仮定

パケットがマーキングされる回数を x とし，マーキングビット位置を m $(0 \leq m \leq 15)$ とする．$m = 0$ を MSB (Most Significant Bit)，$m = 15$ を LSB (Least Significant Bit) とする．評価を行うにあたり，以下のように仮定をおく．

1. 攻撃パケットが各ホップ数の攻撃者から均等に送られてくる．
2. 攻撃パケットの TTL はランダムの値かつ一様分布の値をとる．
3. 攻撃者の位置は，マーキングビット数 $n = 1$ のとき 16 ホップ以内 $n = 2$ のとき 8 ホップ以内 (攻撃者のマーキングが残る状態) である．

仮定 2 は，Pi 方式では，マーキング開始位置が均等に分布することを示す．

このとき，各方式について $n = 2$ の場合，攻撃者のマーキングが，マーキング回数 x $(1 \leq m \leq 8)$ でマーキングビット位置 m $(0 \leq m \leq 15)$ に残る確率を考える．

3.1.2 Pi 方式の評価

Pi 方式において，ホップ数 x に対する各ビット毎の偽造されている確率 (攻撃者のマーキングが残る確率) を考える．表 1 は，TTL によりマーキングビット位置が 6–7 から開始された一例を示す．

表 1: Pi 方式において $n = 2$ の場合のマーキングフィールド中にマーキングビット位置 m とホップ数 x (各ビット毎の偽造されている確率の一例: 偶数で区切った場合かつマーキングビット位置が 6–7 から始まったとき)

	x							
m	1	2	3	4	5	6	7	8
0–1	1	1	1	1	1	0	0	0
2–3	1	1	1	1	1	1	0	0
4–5	1	1	1	1	1	1	1	0
6–7	0	0	0	0	0	0	0	0
8–9	1	0	0	0	0	0	0	0
10–11	1	1	0	0	0	0	0	0
12–13	1	1	1	0	0	0	0	0
14–15	1	1	1	1	0	0	0	0

3.1.3 提案方式 1 の評価

提案方式において，マーキング回数 x (攻撃者からのホップ数) に対する各ビットの偽造されている確率は表 2 のようになる．

表 2: 提案方式において $n=2$ の場合のマーキングビット位置 m とホップ数 x

	x							
m	1	2	3	4	5	6	7	8
0–1	0	0	0	0	0	0	0	0
2–3	1	0	0	0	0	0	0	0
4–5	1	1	0	0	0	0	0	0
6–7	1	1	1	0	0	0	0	0
8–9	1	1	1	1	0	0	0	0
10–11	1	1	1	1	1	0	0	0
12–13	1	1	1	1	1	1	0	0
14–15	1	1	1	1	1	1	1	0

表 2 より，上位 2bit つまりマーキングビット位置が 0–1 の時でフィルタリングすると 0 になる．また，マーキングビット位置が 2–3 の時でフィルタリングすると $\frac{1}{8}$，全 16 ビットでフィルタリングした場合，その値が偽造されている確率は $\frac{7}{8}$ となる．

3.1.4 提案方式 1+2 の評価

表 3: 提案方式 1+2 において $n=2$ の場合のマーキングビット位置 m とホップ数 x

	x							
m	1	2	3	4	5	6	7	8
0–1	$\frac{1}{2}$	0	0	0	0	0	0	0
2–3	1	1	$\frac{1}{2}$	0	0	0	0	0
4–5	1	1	1	1	$\frac{1}{2}$	0	0	0
6–7	1	1	1	1	1	$\frac{1}{2}$	0	0
8–9	1	1	1	1	1	1	$\frac{1}{2}$	0
10–11	1	1	1	1	1	1	1	$\frac{1}{2}$
12–13	1	1	1	1	1	1	1	1
14–15	1	1	1	1	1	1	1	1

同様に，表 3 から，各ビットが攻撃者の影響を受けている確率を考える．上位 2bit つまりマーキングビット位置が 0–1 の時でフィルタリングすると $\frac{1}{16}$ になる．また，マーキングビット位置が 2–3 の時でフィルタリングすると $\frac{5}{16}$，全 16 ビットでフィルタリングした場合，その値が偽造されている確率は 1 になる．提案方式 1+2 がマーキングする回数は，提案方式のそれに比べて $\frac{1}{2}$ としているので，その分攻撃者のマーキングが残る．

上記のことから，送られてきたパケットの各ビットが偽造されている割合を考える．Pi 方式では，等確率なので判断できない．しかし，提案方式 1 は上位ビットほど，攻撃者のマーキング値への影響が少なく，下位ビットほどマーキング値の影響が大きい．このことから，提案方式 1，1+2 では，Pi 方式よりも高い確率で判別できる．

この評価が，マーキング値に影響すると考えられる．そこで 3.2 節で，ホップ数を変化させた場合の変動係数を考える．

3.2 変動係数の理論的評価

変動係数は，平均の異なるデータ間のばらつきを比較するのに使う指標を表し，ばらつきが多ければ値は高くなり，少なければ低い．つまり，マーキング値に偏りがあるほど，変動係数が低くなり，フィルタリングしやすくなる．

3.2.1 ホップ数を変化させた場合

$n=1$ でホップ数を変化させた場合の場合を考える．ここで，それぞれパケットが通るルータが，初期値 0 で送られる場合の，マーキング値の取り幅は，表 4 のようになる．表 4 から，提案方式 1 と Pi 方式では，値の取り幅が 16 倍になっていることがわかる．

表 4: 各方式において $n=1$ の場合のマーキング値の取り得る幅 y とホップ数 x

	x		
y	1	2	3
Pi scheme	$2^1 \cdot 16$	$2^2 \cdot 16$	$2^3 \cdot 16$
our scheme 1	2	2^2	2^3
our scheme 1+2	2	2	2^2

3.2.2 初期値を変化させた場合

$n=1$ でホップ数が 6 の場合を考える．ここで，それぞれパケットが通るルータが，書き込

むマーキング値は固定とする．

表 5: 各方式において $n=1$ の場合のマーキング値の取り得る幅とホップ数 x

	x
y	6

Pi scheme	$2^{10} \cdot 16$
our scheme 1	2^{10}
our scheme 1+2	2^{13}

Pi 方式では，16 ビット中 6bit がルータによって上書きされるから，攻撃者のマーキングは 10 ビット残るので，2^{10} 通りあり，なお TTL によってホップ数が 16 通りある．よって，$2^{10} \cdot 16$ 通り考えられる．

提案方式 1 では，16 ビット中 6bit がルータによって上書きされるから，攻撃者のマーキングは 10 ビット残るので，2^{10} 通りある．しかし，提案方式は TTL によってホップ数が変わらないので 2^{10} 通り考えられる．よってマーキング値の範囲は Pi 方式の $\frac{1}{16}$ 倍となる．

提案方式 1+2 では，16 ビット中 3bit がルータによって上書きされるから，攻撃者のマーキングは 10 ビット残るので，2^{13} 通りある．よってマーキング値の範囲は Pi 方式の $\frac{1}{8}$ 倍となり．上記の結果を考慮すると，変動係数の比が Pi : 提案方式 1 : 提案方式 1+2 $= 1 : \frac{1}{16} : \frac{1}{8}$ になると予想できる．この結果を踏まえた上で，第 4 章で実験を行う．

4 実験

4.1 DDoS 攻撃モデル

4.1 節では，[3, 2] のモデルを使用する．つまり，DDoS 攻撃の手順を学習段階と攻撃段階の 2 つに分ける．学習段階では，packet identification function[1] で攻撃者リストが得られていることと仮定し，攻撃段階でそのリストを用いてフィルタリングを行う．本研究では，攻撃段階に焦点をあて，なおかつ各ノードが攻撃者か正規ユーザか決めずに，各方式について取り得るマーキング値の評価，解析を行った．

5 章と新しく 6 章に示すパラメータを用いて実験を行い，評価した．実験対象のネットワークは木構造である．このネットワークは，複数のポータルサイトから深さ優先探索でリンクからノードを辿っていき，そのノードが葉ノードであればそのリンク先 URL とホップ数を計算し，記憶する．そして，一つ前のリンクに戻るということを繰り返し行い，ネットワークを構築した．変動係数，誤判定共に 300 個の葉ノードを用いた．そしてそれぞれ同経路が存在すると仮定し，その 300 葉ノードのホップ数と初期値を変えて攻撃パケットを送った場合の，各方式のマーキング値を解析した．

4.2 評価パラメータ:変動係数

各方式においてマーキング値の偏りを評価するために変動係数 (Coefficient of Variation) に対してホップ数と初期値を変化させた．(変動係数については 3.2 章を参照)．

ホップ数を変化させた場合，初期値を 0 で固定し (パケットは Non-spoofed を示す)，マーキングビット数 $n=1,2$ のときノードの位置を 1 から 21 ホップまで変化させた．Pi 方式は TTL を 255, 127, 63 と変化させた．初期値を変化させた場合，攻撃者のホップ数を 6 とし，変動係数では初期値をランダムに 13000 回変化させた (パケットは Spoofed を示す)．Pi 方式は TTL を 255 とした．

5 実験による変動係数の評価

5.1 ホップ数を変化させた場合

このときの変動係数の値を図 3，図 4 に示す．それぞれの実験において，提案方式 1，1+2 よりも低い値をとることはなかった．また，Pi 方式と提案方式 1，1+2 を比較すると，変動係数の差が 3 倍以上であった．これは，3.2 節の変動係数の理論評価の場合，TTL を固定していないからだと考えられる．TTL を可変にすることで，変動係数が理論値に近づくと考えられる．

5.2 初期値を変化させた場合

実験結果を，図 5，図 6 に示す．初期値を変化させたときでも，値の偏りが Pi 方式よりも少ないことがいえる．すなわち，初期値に対す

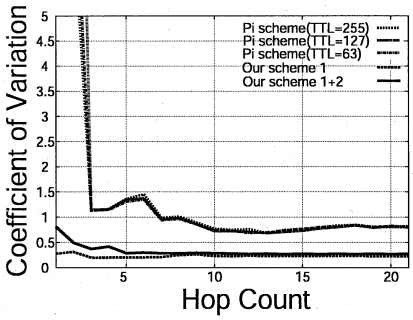

図 3: 距離と変動係数の評価: $n = 1$ (Non-spoofed)

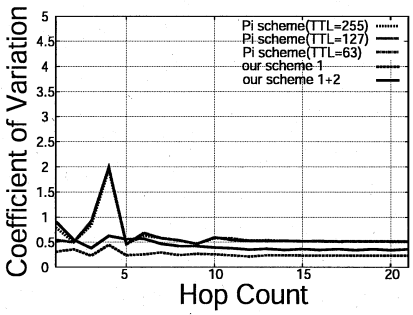

図 4: 距離と変動係数の評価: $n = 2$ (Non-spoofed)

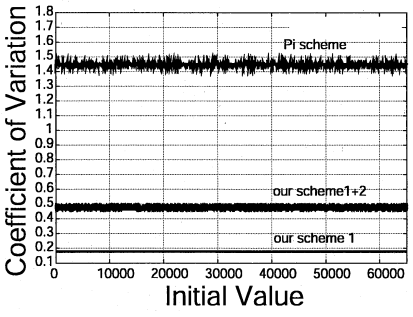

図 5: 初期値と変動係数の評価: $n = 1$ (Spoofed)

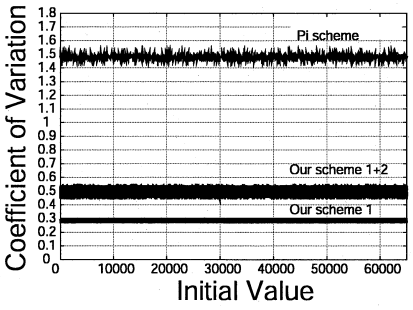

図 6: 初期値と変動係数の評価: $n = 2$ (Spoofed)

るマーキング値への影響が，Pi 方式より提案方式のほうが少ないことがわかった．先ほどと同様，特に $n = 1$ のときに，Pi 方式では顕著に出たものの，提案方式1，1+2 ともに Pi 方式より影響が少なかった．

また，提案方式1と1+2を比較すると，3.1節のスキームの理論的評価の通り，提案方式1+2の方が攻撃者のマーキングが残り，変動係数が高くなった．

6 実験による誤判定の評価

6.1 評価パラメータ:誤判定

本研究では，誤判定という評価を新しく用いる．なぜなら，攻撃者とは関係なく，異なる経路において同じ値を持つ場合が考えられるからである．ここでは，[?] に基づくフォルスポジティブやフォルスネガティブも含んだ誤判定という指標を用いる．誤判定は，複数の経路が同じマーキング値を持つ場合，誤判定をしたとみなす．誤判定が少ないほど，各経路が固有な値を持つ．ここで，300 経路中同じマーキング値を持つ経路の最大の数の割合をこの場合の誤判定として評価を行った．

ホップ数を変化させた場合，初期値を 0 で固定し，マーキングビット数 $n = 1, 2$ のときノードの位置を 1 から 21 ホップまで変化させた．Pi 方式は TTL を 255, 127, 63 と変化させた．

初期値を変化させた場合，攻撃者のホップ数を 6 とし，誤判定では 3500 回変化させた．Pi 方式は TTL を 255 とした．

6.2 ホップ数を変化させた場合

このときの実験結果を図 7，図 8 に示す．$n = 1$ より $n = 2$ の方が全体的に大きい．これは，マーキング値が 2^{16} 通りから 2^8 通りののバリ

エーションに減ったと考えられる．また，提案方式1は，特にホップ数が小さい時Pi方式よりも大きな値を取る．これは，Pi方式がTTLにより書き込む開始位置を変えていることにより，マーキング値のバリエーションが提案方式1より多いことが考えられる．また，提案方式1+2はPi方式と比べ誤判定が少ないことがわかった．

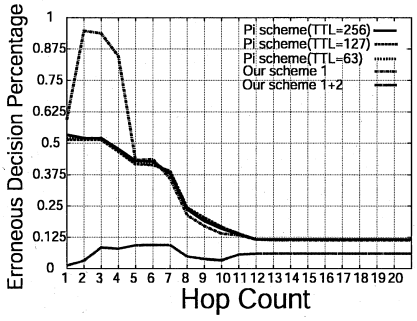

図 7: 距離と誤判定の評価: $n = 1$ (Non-spoofed)

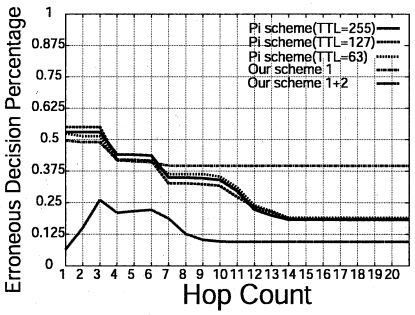

図 8: 距離と誤判定の評価: $n = 2$ (Non-spoofed)

6.3 初期値を変化させた場合

実験結果を，図5，図6に示す．提案方式1+2は，提案方式1やPi方式と比べ，誤判定が少なかった．これは，単純に有効となるマーキングフィールドを増やすことにより，マーキング値が重なる割合が小さくなったことが考えられる．

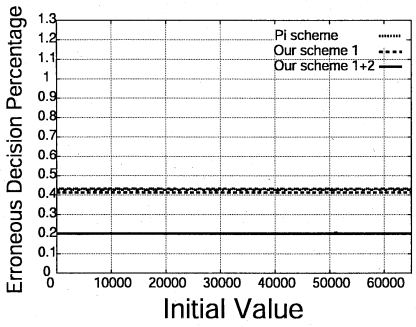

図 9: 初期値と誤判定の評価: $n = 1$ (Spoofed)

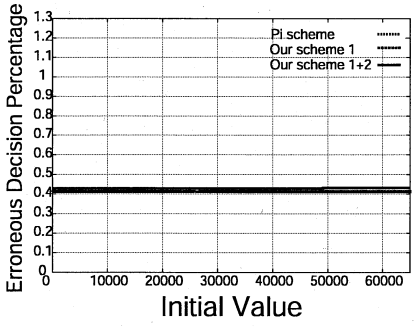

図 10: 初期値と誤判定の評価: $n = 2$ (Spoofed)

7 考察

3章の理論的評価から，各ビットの確率は下位ビットであればあるほど偽造されている確率は高くなる．つまり，上位ビットほど，攻撃者のマーキング値への影響が少なく，下位ビットほど値の影響が大きい．このことから，マーキング値の揺らぎ，つまり変動係数が小さいことになる．逆に，Pi方式では，上位ビットも下位ビットも同等に攻撃者のマーキング値への影響が残る．このことから，上位ビットが偽造されている場合マーキング値の揺らぎが大きくなり，結果変動係数が大きくなる．しかし誤判定では，同じ経路を通っていたとしてもPi方式では攻撃者のマーキング値が残っている可能性が各提案方式よりもある．よって，マーキング値の取り得る範囲が広く，結果誤判定をする確率は低いと考えられる．

今回の実験ではTTLを255，127，63と固定

した．しかし，理論的評価では仮定2をおく事で評価を行った結果を導出している．さらに理論値に近い差が出ると考えられる．

8 まとめ

本研究では，[8]に示す実験的評価の裏づけとなる理論的根拠を示し，さらに実験を改良することで提案方式1，1+2いずれもPi方式よりもよいマーキングを行うことが示された．

今後の課題としては，既存方式と提案方式の理論的比較と，今回の誤判定の結果に基づいた理論的評価を行う．また，ネットワークシミュレータ[9]を使い，攻撃者を設定することでDDoS攻撃のシミュレーションを行い，どの程度フィルタリングできるのか評価する．特に，誤判定を細分化してフォルスポジティブ，フォルスネガティブ[5]による評価を行う．

謝辞

本研究成果は，文部科学省科学技術振興調整費による．

参考文献

[1] J. Ioannidis, and S. M. Bellovin, "Implementing Pushback: Router-based defence against DDoS attacks," in *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2002),* pages 93-107, Feb. 2002.

[2] A. Yaar, A. Perrig, and D. Song, "StackPi: A new defensive mechanism against IP spoofing and DDoS attacks. Path Identification Mechanism to Defend against DDoS Attacks," Technical Report CMU-CS-02-208, Carnegie Mellon Univercity,Feb. 2003.

[3] A. Yaar, A. Perrig, and D. Song, "Pi: A Path Identification Mechanism to Defend against DDoS Attacks," in *Proceedings of IEEE Symposium on Security and Privacy,* pages 93-107, May 2003.

[4] A. Yaar, A. Perrig, and D. Song, "SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks," in *Proceedings of IEEE Symposium on Security and Privacy,* pages 1-14, May 2004.

[5] M. Collins and M. K. Reiter, "An Empirical Analysis of Target-Resident DoS Filters," in *Proceedings of IEEE Symposium on Security and Privacy,* pages 103-114, May 2004.

[6] Y Xiang, W Zhou, M Chowdhury, "A Survey of Active and Passive Defence Mechanisms against DDoS Attacks," Technical Report, TR C04/02, School of Information Technology, Deakin University, Australia, pages 1-40, 2004.

[7] X. Yang, D. Wetherall, T. Anderson, "A DoS-limiting Network Architecture," in *SIGCOMM'05,* pages 242-251, August 2005.

[8] 竹本 秀樹, 双紙 正和, 宮地 充子, "DoS攻撃に対するフィルタリング方式の検討," in *Computer Security Symposium,* pages 149-154, Oct, 2006.

[9] The Network Simulator – ns-2 http://www.isi.edu/nsnam/ns/.