情報処理学会論文誌　Vol. 52　No. 9　2718–2728 (Sep. 2011)

確率的パケットマーキングにおける最適マーキング確率の推定

岡田雅之[†1,†2]　金岡晃[†3]
勝野恭治[†4]　岡本栄司[†3]

インターネットにおけるサービス不能攻撃の攻撃者を特定する IP トレースバックの 1 つとして，確率的パケットマーキング手法が近年注目されている．確率的パケットマーキング手法は，他の IP トレースバック技術と比較して，ICMP などの能動的なトラフィックを発生させないことや，攻撃対象宛パケットのすべてを収集する必要がないことなどのメリットが知られているが，これまで，ルータにおけるパケットへのマーキング確率は，個別の研究事例ごとに想定するルータ間距離の逆数をマーキング確率とする研究が多く，実際のインターネットにおけるネットワークトポロジを考慮した最適確率については論じられてこなかった．本研究では，確率的パケットマーキング手法において，攻撃経路逆探知に必要な収集パケット数が最小となり，最短時間で攻撃者までの攻撃経路逆探知が可能となるマーキング確率を推定する．

Probability Estimation for Probabilistic Packet Marking

Masayuki Okada,[†1,†2] Akira Kanaoka,[†3]
Yasuharu Katsuno[†4] and Eiji Okamoto[†3]

Recently, much attention has been paid to Probabilistic Packet Marking (PPM), as one of IP traceback techniques which enable to identify the Denial of Services (DoS) attackers on the Internet. This paper proposes optimum marketing probability considering network topology on actual Internet, while many existing PPM studies use marking probability calculated as the reciprocal of distance between routers. We investigated the DoS attack and IP traceback system and some DoS defense mechanism, using Internet topology data and some past PPM mechanisms in order to estimate probability. As the result of experiments, we found the probability that minimizes the number of packet collections is 0.082.

1. はじめに

インターネットが様々な局面で利用され，広く普及するにともない，インターネットの安定性を脅かす事例が複数発生している．特にサービス不能（Denial of Service，DoS）攻撃は大きな脅威となっており，DoS 攻撃に対する分類や対策が複数提案されてきた[1)]．様々な技術がある対策において，本研究では IP トレースバックに注目した．IP トレースバックには複数の方式が提案され細分化しており，IP トレースバックの一方式として，確率的パケットマーキング（Probabilistic Packet Marking，PPM）方式が存在する．PPM では，攻撃者から送出されたパケットがルータで転送され被害者へ到達する過程において，ルータが確率的に攻撃経路逆探知に有用な情報をパケット自身へ書き込むマーキング行為を行う．被害者はマーキングされたパケットを収集し，攻撃経路の逆探知や攻撃元の特定に利用する．

PPM は Savage らによって最初に提案され[2)]，その後，複数の応用や改善の提案[3)–5)]がなされてきた．PPM 方式は他の IP トレースバック方式と比較し，探知のためのパケット増加などがないこと，パケットを記録するための記憶装置が不要であることなど複数の利点がある一方で，確率的にマーキングされているという特徴から攻撃経路逆探知のために多くのパケットを収集する必要があることや，攻撃者が多数となった場合に，攻撃経路を識別するためのハッシュ値の衝突が発生し，逆探知において誤探知の可能性があることが知られている．

従来の PPM 方式では，マーキング確率は想定される攻撃者と攻撃対象者の距離より算出される値で，なるべく小さくすべき[2)]とされ，実際のインターネットトポロジを考慮した議論はされてこなかった．また，PPM 方式の評価においても，攻撃経路逆探知のための必要パケット数の期待値による比較評価がされており，実際のネットワーク環境に適用する場合で必要な逆探知の時間についての評価はなされていなかった．

本研究においては，ルータにおけるマーキング負荷を測定し，インターネットトポロジ分

†1 筑波大学大学院システム情報工学研究科リスク工学専攻
Department of Risk Engineering, Graduate School of Systems and Information Engineering, University of Tsukuba
†2 社団法人日本ネットワークインフォメーションセンター
Japan Network Information Center
†3 筑波大学大学院システム情報工学研究科
Graduate School of Systems and Information Engineering, University of Tsukuba
†4 日本アイ・ビー・エム東京基礎研究所
Tokyo Research Laboratory, IBM Japan Ltd.

布[16] を考慮した攻撃経路逆探知のための必要パケット数期待値の算出を行う．そして算出したパケット数期待値を基に，攻撃経路逆探知時間を評価指標として最適マーキング確率を推定する．最適なマーキング確率を推定するにあたり Savage らの方式，Goodrich らの方式，金岡らの方式の 3 方式を選択した．これらの 3 方式は，利用する IP ヘッダのフィールド種別において他の通信には影響を与えない方式であり，かつ既存方式の中でも効率的な方式であるためである．

これらの 3 方式について，前述のマーキング負荷，トポロジ分布と合わせて推測を行い，逆探知時間が最短となるマーキング確率は 0.082 であるという結果を得た．さらに，本研究では，推定した確率に基づきマーキング機能と攻撃経路逆探知機能に関する実装評価実験を行い，Linux ルータ環境下において，最適確率 0.082 でのマーキング処理の負荷を測定した．その結果，従来のマーキング確率での処理負荷と比較し差がなく，実験環境では短時間でのトレースバックが可能であることを示した．最後に，日本国内での PPM 展開に必要な，IP トレースバックを行う際の通信の秘匿性に関する検討を行った．

本論文の構成は，関連する研究について，2 章において IP トレースバックと PPM 方式について，3 章において，インターネットの接続構成に関する特徴についてそれぞれ解説する．4 章では，PPM 方式のマーキング，攻撃経路再構築機能の実装と評価を行い，それをふまえ 5 章において最適なマーキング確率の算出を提案し，実際の DoS 攻撃時の状況をあてはめたシミュレーションを，6 章で PPM 方式の法的側面を交えた考察を行う．最後に 7 章において本論文の内容について総括し，まとめとした．

2. 関 連 研 究

2.1 DoS 攻撃と IP トレースバック

DoS 攻撃においては，攻撃者は送信元ソース IP アドレスを偽装していることが多く，偽装パケットの送信元を追跡する技術として IP トレースバックが研究されている．IP トレースバックには，リンク追跡型[1),13)]，探知 Internet Control Message Protocol（ICMP）パケット型，メッセージダイジェスト型，そしてパケットマーキング型が知られている．リンク追跡型は，IP トレースバックの初期から存在する方式で，攻撃目標となったノードを始点とし，トラフィック流入量などの変化からルータのインタフェースごとにたどり攻撃元を特定する．探知 ICMP パケット型は，ICMP トレースバック方式とも呼ばれ，経路途中のルータが一定の確率で，攻撃目標となったノードへ探知 ICMP パケットを送る．攻撃目標となったノードはこの ICMP 探知パケットをたどることにより攻撃元へ到達する．メッセージダイジェスト型[14),15)] は，ルータ外部またはルータ上で IP ヘッダの特定部位の値を入力値としてハッシュを生成し記録することで，攻撃元までの経路を攻撃目標となったノードが知ることができるとされる．パケットマーキング型は，攻撃元から攻撃目標への途中経路のルータにおいて，IP ヘッダの特定部位を使い，確率的に通過ルータの情報を書き込む（**図 1**）．確率的パケットマーキング型については次項で詳細を説明する．

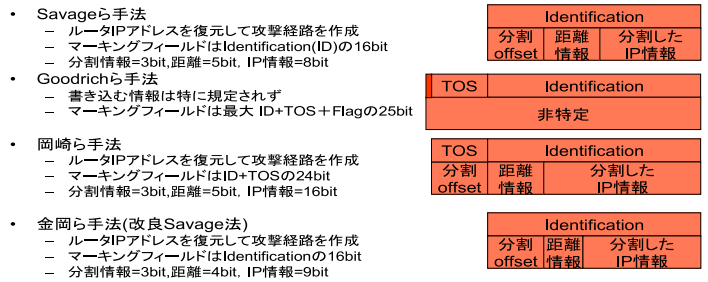

図 1　代表的な確率的パケットマーキング方式の IP ヘッダフィールド利用法
Fig. 1　IP header field usage for typical PPM methods.

2.1.1 確率的パケットマーキングの基本概念

確率的パケットマーキング（PPM）では，パケットが通過するルータなどにおいて，確率的にトレースバックに必要な情報を書き込む．通過するすべてのルータでつねに書き込みを行う場合，攻撃目標となったノードは隣接ノードの情報しか得ることができないが，隣接ノード以遠の情報をパケットに埋め込むために，PPM においては，書き込み頻度を確率的に決定することで，攻撃目標となったノードは，遠位のルータ情報を復元することが可能となっている．PPM 方式は，最初に Savage らによって提案された．Savage らの方式では，ルータの IP アドレスをマーキング情報として書き込む．Savage らの方式は，PPM 方式の基本的な方式であるため，次項で詳細に解説する．

Savage らの方式以後，PPM 方式の改良が複数提案されている．Song ら[18)] の方式では，Savage らの方式と比較して，IP アドレス情報をそのままマーキング情報とするのではなく，IP アドレスの何らかのハッシュ値を書き込むこととした．ハッシュ値だけを書き込むことからマーキング情報が小さくなり，攻撃経路逆探知に必要なパケット数を少なくできるとした．しかしながら，IP アドレスの情報はマーキング情報に含まれないため，攻撃経路の逆探知には，ルータトポロジを事前に把握しておく必要がある．

Law ら[13)] の方式では，各ルータに流れるトラフィック量をマーキング情報とし，被害者

側ネットワークでは，ルータのトラフィック量の変化を調べることで攻撃元を特定する．この方式では，攻撃経路の逆探知を目的とせず，攻撃を受けたルータの特定が可能となっている．

Goodrich[5] の方式では，マーキング情報を特定せず，用途によってマーキング情報を柔軟に変えることができるとした．Goodrich の方式は，これまでの PPM 方式では方式ごとにマーキング情報が指定されていたが，IP アドレスやトラフィック情報，ハッシュ情報に特化せずに，必要な情報を書き込むことができる．Goodrich の方式は，PPM 方式の一般化といえる．

PPM 方式は，逆探知や攻撃元の特定を行う際，確率的にマーキングを行うため，収集するパケット数が多くなることが問題とされている．収集パケット数を少なくする方式として，岡崎ら[4] は，Identification フィールドのほかに Type of Service（ToS）フィールド（8 ビット）を使いマーキング領域を 24 ビットとしてマーキング情報を増やすことにより，攻撃経路復元に必要な収集パケット数を少なくすることが可能であるとした．しかしながら，ToS フィールドは，パケットが運ぶデータによって，転送優先順位付けを行う Quality of Service や DiffServ（Differentiated Services）[19] などに用いられることから現実的ではない．金岡ら[3] の方式では，インターネットトポロジの特性から距離情報を 4 ビットとし，捻出された 1 ビットを使いマーキング領域を増やし，Identification フィールドのみをマーキング領域として，攻撃経路復元に必要なパケット数を削減した．

2.1.2　Savage らの方式

Savage らの方式（**図 2**）では，IP パケット上の Identification フィールド（16 ビット）をマーキング領域とし，32 ビットの IP アドレスとそのハッシュ値 32 ビットの合計 64 ビットを 8 分割し，補足情報とあわせてマーキングする．

Identification フィールドでは，16 ビットのフィールドを，3 ビットのアドレス情報オフセット，5 ビットの距離情報，8 ビットの IP アドレスとハッシュの分割情報に区分し書き込みを行う（**図 3**）．

隣接ノードの IP アドレスと排他的論理和（XOR）の値を書き込む情報とすることで，隣接ルータのアドレスから，繰り返し XOR を計算することで，攻撃経路の復元が可能となっている．さらに，復元した IP アドレス情報の正確さを検証するため，IP アドレスのハッシュ値も同時に書き込む．攻撃目標となったノードは，必要な PPM 情報が書き込まれたパケットを収集し，既知の隣接ルータの IP アドレス情報を始点としてマークされた情報の XOR から攻撃経路を再帰的に復元する．復元した IP アドレスのハッシュ値から，マークされた情報の正当性を確認する．

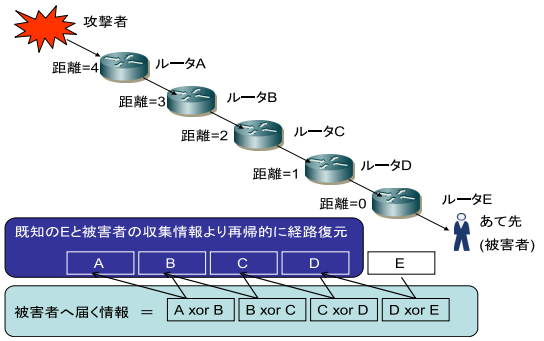

図 2　Savage らの方式における確率的パケットマーキング方式の概念
Fig. 2　Overview of Savage's PPM method.

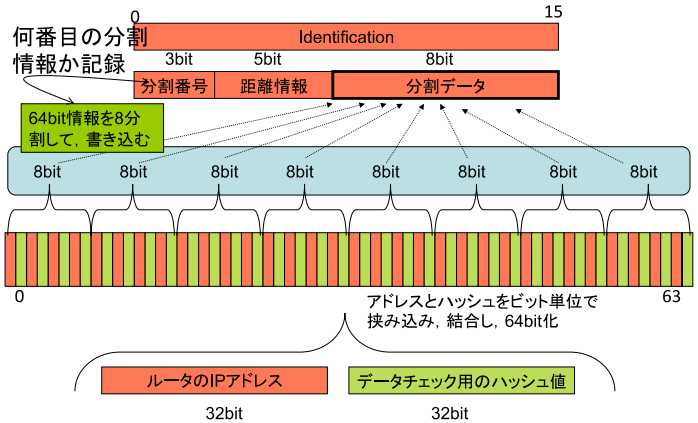

図 3　Savage らの方式の Identification フィールド利用法
Fig. 3　Identification field usage for Savage's method.

3.　インターネットトポロジ

インターネットの構造を解析することを目的として，トポロジ情報の収集と公開がなされている．特に，インターネットのルータ接続トポロジは，スモールワールド性を持つことが

表 1　CAIDA データを基にした 2 点間距離分布
Table 1　Distribution of AS path length based on CAIDA data.

距離 d	占める割合(%)	距離 d	占める割合(%)
1	0.003%	11	1.864%
2	0.055%	12	0.930%
3	0.572%	13	0.417%
4	3.772%	14	0.164%
5	13.216%	15	0.075%
6	24.134%	16	0.035%
7	25.061%	17	0.012%
8	17.036%	18	0.003%
9	8.722%	19	0.001%
10	3.928%	20	0.000%

知られており，トポロジ情報を基にしたサンプリングによる調査研究では，ルータ間距離が 15 ホップ以内において 99%以上のノードに到達できるとされている[3),6)]．また，これらの調査研究では，任意のルータ間距離分布が算出されており，2003 年に調査，公開された CAIDA データのサンプル調査[3)] では，**表 1** の距離分布となっている．

本研究においては，表 1 の 2 点間距離分布を考慮すべき事項の 1 つとし，確率的パケットマーキングにおける最適確率計算に用いる．

4. 確率的パケットマーキング方式の実装とスループット測定

本章では，攻撃経路の逆探知に必要な攻撃パケット数の期待値が少ないとされる Savage らの方式を改良した金岡らの方式を Linux へ実装し，マーキング確率を変化させ実装へ与える負荷変化を測定した．確率的パケットマーキング方式では，マーキングを行う際だけではなく，マーキングを行わない場合でも，距離情報の加算や，距離情報 bit のオーバフロー処理が行われるため，結果としてルータがパケットを転送するごとに IP ヘッダのチェックサムの再計算が実行される．

これまで実装による負荷評価は金岡ら[3)] によって一部行われていた．しかし各 PPM 方式の性能評価にあたっては逆探知に必要なパケット数期待値のみが議論されていたが，逆探知に必要となる時間については議論がされてこなかった．本論文においては，これまで行われていなかった攻撃経路の逆探知機能についても実装を行い，逆探知機能が実時間で実現可能であることを確認する．

表 2　実験環境の詳細
Table 2　Details of marking load experiment environment.

	ハードウェア	OS 環境
PPM ルータ実験機	IBM SystemX3560M2 CPU:Intel E5540 4core 2.53GHz メモリ:DDR3 RDIMM 32GBytes NIC :Broadcom 5709	CentOS 5.3
パケット送出機，受信機	Think Center A55 CPU:Intel Core2Duo E4400 メモリ:DDR2 SDRAM 4GBytes NIC:Broadcom 95751	CentOS 5.3

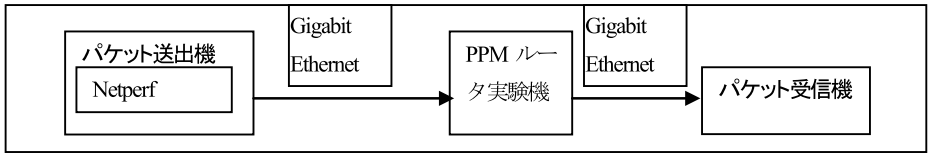

図 4　マーキング負荷計測環境
Fig. 4　Marking load measurement environment.

4.1 確率的パケットマーキング実装実験環境と実験方式

実験環境と構成は，**表 2**，**図 4** のとおりである．実験はマーキング確率ごとのパケット転送スループットを測定するため，パケット送出機からパケット受信機へ試験パケットを複数パターンのマーキング確率を設定した PPM ルータを経由し送出する．パケット送出には Linux で動作する netperf[7)] を用いた．今回の実験では，測定するマーキング確率として，PPM を行わない $p = 0$，これまでの研究で使われてきた $p = 0.04$ と比較的高マーキング確率である $p = 0.4$，$p = 0.5$ を対象とした．

4.2 実験結果と評価

スループット測定実験では，netperf のパラメータとして，Delay = 0，パケットサイズ = 64 Byte から 10,000 Byte，あて先 IP アドレス数 = 単一，使用するトランスポートプロトコル = UDP とし，マーキング確率，パケットサイズごとに 10 回の試行を行った．試行の結果を**図 5** に示す．本スループット試験では，パケットサイズが 1,000 Byte 以内では，すべてのマーキング確率において，秒間転送速度（Bit Per Second，bps）は，パケットサイ

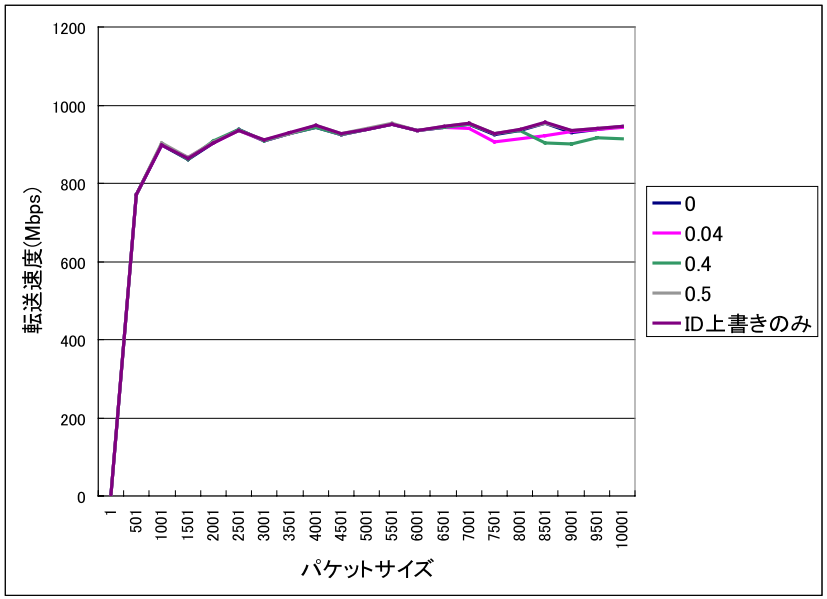

図 5　確率とパケットサイズごとの転送スループット
Fig. 5　Packet forwarding throughputs when probability and packet sizes are varied.

ズが増えるにつれ増大し，パケットサイズが 1,000 Byte 超では，800 Mbps から 900 Mbps となった．結果として，今回実験では，マーキング確率の変化において，スループット差を観察することはできなかった．

4.3　マーキングパケットからの逆探知機能実装

マーキングパケットを収集し，攻撃経路の再構成機能を実装し，逆探知時間を実際に計測する．本研究での実装は，tcpdump プログラムによって受信し転送するパケットの IP ヘッダ情報を，標準入出力を利用して解析プログラムが受け取り，距離情報とオフセットから攻撃経路を再構成する機能を実装した．実験環境と構成は**表 3**，**図 6** のとおりである．実験では，攻撃者から被害者へ試験パケットを連続して送出し，試験パケットは途中経路の PPM ルータ 2 台により確率的にマークされる．被害者と想定するパケット受信機へ到着したパケットは，前述のとおり，tcpdump プログラムによってパケットを取り出し，復元プログラムが解析して，攻撃経路の逆探知を行う．

表 3　実験環境の詳細
Table 3　Details of attack path reconstruct experiment environment.

	ハードウェア	OS 環境
PPM ルータ1，2	Think Center A53　small CPU Intel Pentium4 524 メモリ:DDR2 4G Bytes NIC：Broadcom 5722	CentOS 5.3
パケット送出機，受信機	Think Center A55 CPU:Intel Core2Duo E4400 メモリ：DDR2　SDRAM 4GBytes NIC：Broadcom 95751	CentOS 5.3

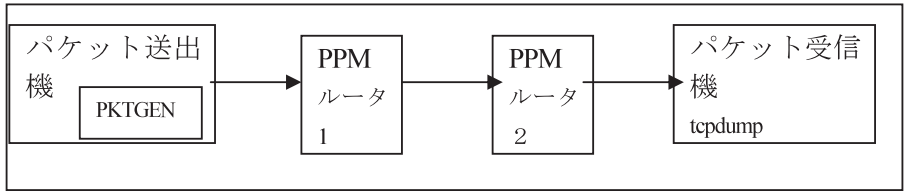

図 6　PPM 攻撃経路逆探知実験環境
Fig. 6　PPM attack trace back experiment environment.

復元，探知実験のパケットへのマーキング確率は，本節以後は最適と推定した 0.082 とした．パケット送出タイミングは，送出機が PKTGEN[8] でパケットロスを発生させない上限であった 80 KPacket Per Second（PPS）とした．試行を 10 回行った結果，パケット受信機上で逆探知までに必要な逆探知時間の平均値は 3.45 秒となった．逆探知時間の平均値は逆探知プログラムの起動から PPM ルータ 2 までの逆探知終了までの合計時間となっている．

4.4　実装実験評価のまとめ

本論文による実装実験においては，マーキング確率の変化はパケット転送スループットへ影響がないと観察することができることから，最適なマーキング確率は PPM を実施するルータの負荷を無視して考慮することができ，攻撃パケット数期待値が少なく逆探知時間が最短となる確率を求めることが最適であるということができる．

本実装の基本構成は，Intel 系 CPU を使ったハードウェア構成上に，基本ソフトウェアとして Linux を用いて実装した．この構成は，ルータやファイアウォールなどのパケット

転送装置として一般的な構成に類似しており，本実装実験の結果はある程度一般的な構成での実験結果に近いと考えられる．

しかしながら，Linux OS 以外のソフトウェアや Intel 系 CPU だけでなく，他の CPU やハードウェアパケット転送装置が存在することを考えると，他の実装系での実装実験は今後課題となると考えられる．

また，攻撃元探知プログラムについても実装し，攻撃実施ノードから犠牲者ノードへパケットを送出し，実際に攻撃経路再構成と逆探知が可能であることが分かった．

5. 最適マーキング確率の推定手法

5.1 攻撃元探索に必要なパケット数の期待値

最適マーキング確率を推定するにあたり，前提条件としてインターネット上のすべてのルータが確率的パケットマーキング機能を実装し，すべてのルータが同一のマーキング確率 p でマーキングを行うものとする．パケット発生場所から被害者までのインターネットトポロジを基にした距離分布を f_i，パケットがマークされる場所から被害者までの距離を d とする．このとき，マーク位置が距離 d であるパケットの届く確率 P_d は，以下の式となる．

$$P_d = p(1-p)^{d-1} \sum_{i=d}^{\infty} f_i \tag{1}$$

式 (1) を金岡ら[3] で算出された，確率的パケットマーキングにおける攻撃者の経路再構成に必要なパケット数の期待値へ適用する．トポロジ分布を考慮した必要収集パケット数 n の期待値 $E_d[n]$ は，攻撃者の数を m，マーキング方式ごとに定められたパケット分割数を l とするとき，以下の式となる（γ はオイラーの定数．$\gamma = 0.5772156649\ldots$）．

$$E_d[n] = \frac{ml\ln(ml) + \gamma ml + \frac{1}{2}}{P_d} \tag{2}$$

また，トポロジを考慮した距離に依存しない必要パケット数 n の期待値 $E[n]$ は，別途集計するインターネットトポロジにおけるルータ距離分布を f_d とすると，以下のとおり算出することができる．

$$E[n] = \sum_{d=1}^{\infty} f_d E_d[n] \tag{3}$$

5.2 時間軸を考慮した最適マーキング確率の推定

本節では，逆探知に必要なパケット収集時間を攻撃経路のインタフェース転送速度と 5.1 節において導いたパケット数の期待値より算出する．犠牲者は，攻撃経路の逆探知を行う際，攻撃者から発信されルータにおいてマークされたパケットを収集する．このとき，犠牲者の 1 秒間に受信するパケット数は，攻撃時の攻撃者から犠牲者間の平均パケット単位秒間転送速度（Average Packet Per Second，AveragePPS）に依存する．AveragePPS の算出式は以下のとおり．

$$\text{AveragePPS} = \frac{\text{攻撃経路平均インタフェース転送速度 [bps]}}{(\text{パケットサイズ} + \text{パケットヘッダサイズ})\,\text{[Byte]} \times 8} \tag{4}$$

このとき，逆探知に必要なパケット収集数について，式 (3) のトポロジを考慮した距離に依存しない必要パケット数 n の期待値 $E[n]$ と上記式 (4) の平均パケット単位秒間転送速度（AveragePPS）より，逆探知時間（TraceTime）は以下のとおりに算出できる．

$$\text{TraceTime} = \frac{E[n]}{\text{AveragePPS}}\ \text{[sec.]} \tag{5}$$

以上より，最適なパケットへのマーキング確率は，逆探知時間 TraceTime を最短とする確率 p が最適確率となる．本推定手法は，前提条件が成り立つ限り，任意のパケットマーキング方式，ネットワーク接続インタフェースへ適用することができ，将来，インターネットトポロジ分布が変化した際にも適用することが可能である．

6. 提案手法の適用と評価

本章では，5 章において提案した最適マーキング確率推定手法を以後に説明する前提条件下において複数の PPM 手法へ適用し，最適マーキング確率の評価を行う．

6.1 特定条件下での限定評価

本節では，代表的なマーキング方式である，Savage らの方式とその改良である金岡らの方式，Goodrich の方式の 3 方式について，必要パケット数期待値を得るために必要な時間が最短となる最適確率の計算を行う．前提として，攻撃者数 $m = 1$，インターネットトポロジ距離分布には 3 章において算出した表 1 の分布 f_d を用いる．評価対象とするルータ間距離 d は CAIDA トポロジにおいて 99%以上の任意のルータ間に到達可能な $1 \leq d \leq 15$ とした．

時間評価を行うにあたり，攻撃者は，日本国内で最も普及している光ブロードバンド環境[9] の接続インタフェースである FastEthernet を使用していると想定する．攻撃パケッ

表 4　FastEthernet におけるパケットサイズと PPS
Table 4　Packet size and packet per second (PPS) on FastEthernet.

パケットサイズ(Byte)	最大 PPS(MaxPPS)
64	148810
1500	8333

トサイズとして，パケットサイズが最小となる 64 Byte と，パケットサイズが最大となる 1,500 Byte でのパケット単位転送速度，Packet Per Second（PPS）を用い評価を行う．

5 章においては，パケット転送速度について，一般化した平均パケット転送速度を用いて算出した．本章では，評価を単純化するため，攻撃者は犠牲者に対して，接続するインタフェースの最大スループットを使い DoS 攻撃を行うことを前提として最大パケット単位転送速度（MaxPPS）を用い評価を行う．

この比較単純化について，実際のインターネット上のパケット転送環境と合わせて考慮すると，経路間のパケット転送速度は，経路中最低速度のインタフェースの最大転送速度が上限となることから，本節で想定する攻撃者の接続インタフェースは FastEthernet であること，わが国における ISP 間のトラフィックの推定[20] において，2010 年 5 月時点のトラフィック量は T（テラ）bps 規模となっていることの 2 点を考えると，FastEthernet インタフェースは経路中最も低速なインタフェースであることが想定でき，FastEthernet インタフェースにおける最大転送速度を用いて評価を行うことの問題は小さいと考える．以後の前提として攻撃者から犠牲者間においてパケットロスや遅延は発生しないものとする．

本評価で想定する，FastEthernet インタフェースにおけるパケットサイズと最大 PPS（MaxPPS）の関係を式 (6) に示す．式 (6) では，FastEthernet を前提としているため，Ethernet フレームの先頭に 8 Byte のプリアンブルと，フレームの末尾に 12 Byte の Inter Frame Gap がパケットごとに付加されることから，パケットサイズに対し 8 Byte＋12 Byte を加算している．

$$\mathrm{MaxPPS}_{\mathrm{FastEthernet}} = \frac{\text{FastEthernet 最大転送速度 [bps]}}{(8 + \text{パケットサイズ} + 12)\,[\mathrm{Byte}] \times 8} \tag{6}$$

このとき，**表 4** の MaxPPS を式 (5) の AveragePPS に代えて適用し，確率ごとの逆探知時間を算出する．マーキング確率ごとのパケット数期待値から算出した逆探知時間の変化を**図 7**，**図 8** のグラフに示す．距離に依存しない必要パケット数期待値と前述の攻撃者条件から算出した攻撃パケット送出数において，攻撃元探知時間が最短となる確率 p は，すべての確率的パケットマーキング方式において確率 $p = 0.082$ となった．

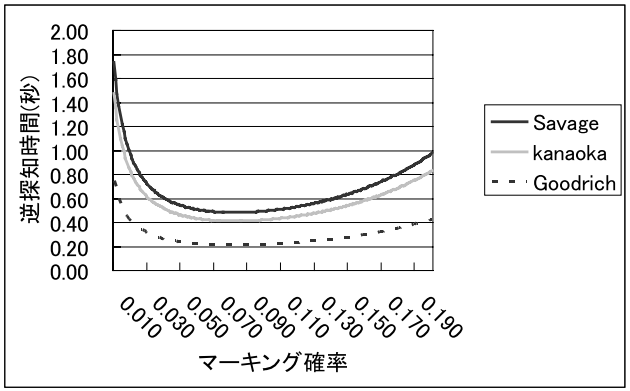

図 7　距離に依存しない逆探知時間と確率 p（パケットサイズ = 64 Byte）
Fig. 7　Distance independent trace back time and probability p (64 Byte).

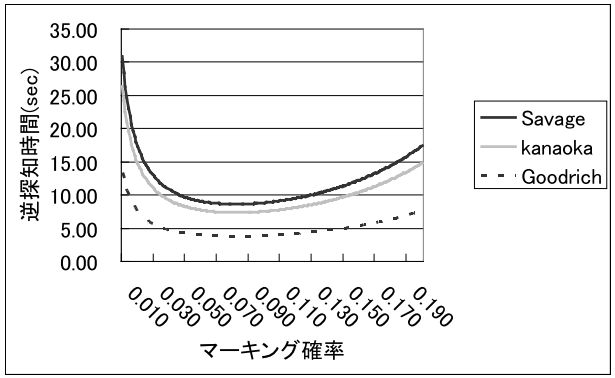

図 8　距離に依存しない逆探知時間と確率 p（パケットサイズ = 1,500 Byte）
Fig. 8　Distance independent trace back time and probability p (1,500 Byte).

攻撃者が単独の状態で，パケットサイズ 64 Byte，148,810 pps で攻撃を行った場合，確率 $p = 0.082$ でパケットへマーキングを行うと，計算上 0.2 秒から 0.6 秒で探知に必要なパケットが収集可能である．また，パケットサイズ 1,500 Byte，8,333 pps で攻撃を行う場合は，同様に確率 $p = 0.082$ でマーキングを行うと，4 秒から 6 秒で必要なパケットを集めることが可能である．

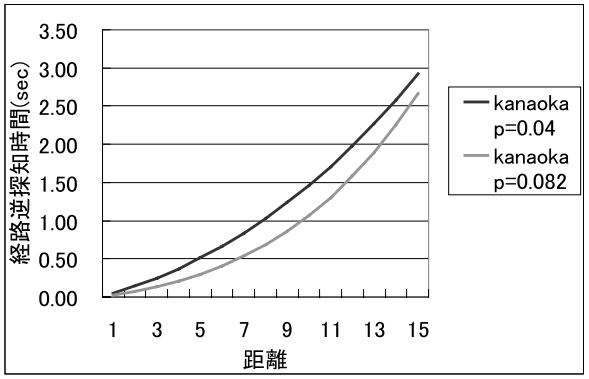

図 9　金岡らの方式における確率 p と逆探知時間
Fig. 9　Trace back time and probability p in Kanaoka's method.

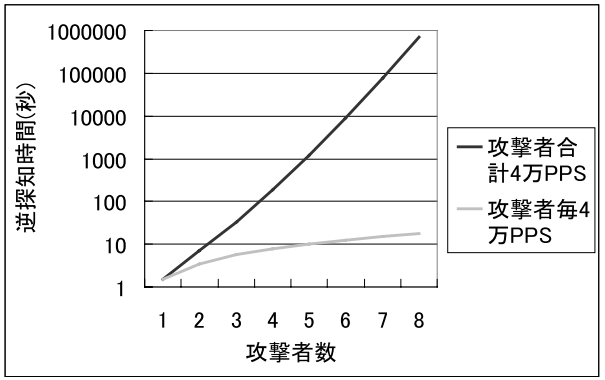

図 10　DoS 事例パラメータにおける攻撃者と金岡らの方式の逆探知時間
Fig. 10　Trace back times in attacker and Kanaoka's method under practical DoS parameters.

Savage らの方式の改良である金岡らの方式について，パケットサイズ 1,500 Byte，8,333 pps での確率 $p = 0.082$ と従来の研究で使われてきた確率 $p = 0.04$ との攻撃元探知時間の比較結果を**図 9** に示す．確率 $p = 0.082$ と $p = 0.04$ の比較では，$1 \leq d \leq 15$ において確率 $p = 0.082$ の攻撃元逆探知時間が短くなることが分かった．

6.2　実際の DoS 攻撃事例のパラメータを用いた評価

本節では，実際に ISP で発生した DoS 攻撃事例で公開されている情報をパラメータとし，確率 $p = 0.082$ で確率的パケットマーキングを適用した際の攻撃者数と探知時間の関係について評価する．DoS 攻撃事例として，文献 10) で報告された事例である，4 万 PPS，160 Mbps の攻撃を想定する．探知時間の計算範囲は，本事例では，40 分以内に収束する攻撃が 92%となっていることから，40 分以内に探知可能な時間までを算出した．シミュレーションに用いた方式は金岡らの方式とした．

図 10 より，本 DoS 攻撃事例において，攻撃者全体の合計で 4 万 PPS のパケットを送出する場合では，攻撃者数が単独である場合には，1.5 sec での探知が可能であり，攻撃者が増加するにつれ，攻撃者数が 5 では探知時間が 20 分，攻撃者数 6 では 130 分となった．攻撃者数が 7 以上では，探知に必要なパケット収集時間が 24 時間以上となっている．攻撃者全体で 4 万 PPS を想定すると，逆探知に必要な時間は攻撃者が増加するにつれ急激に増加することが分かる．一方で，攻撃者がそれぞれ 4 万 PPS でパケットを送出し，攻撃を実施している場合には，攻撃者数 8 では，17 秒となっており，40 分以内に攻撃経路を逆探知できる攻撃者数は 679 となった．

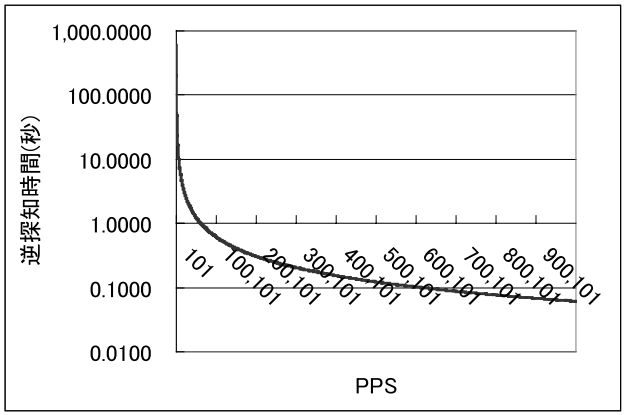

図 11　攻撃者数 1 における送出 PPS と探知時間
Fig. 11　Packet per second and trace back time in attacker #1.

6.3　攻撃者のパケット送出速度と再構成時間の評価

次に，パケット転送速度と逆探知に必要な時間の関係を考察する．攻撃者数 1 の場合における，攻撃者 PPS と逆探知時間の関係を**図 11** に示す．攻撃者の PPS 値については，

Gigabit Ethernet 環境における最大 PPS 値に近い値として 100 万 PPS（1 MPPS）までを対象とした．

図 11 より，50,000 pps 以上での攻撃は 1 sec 以内に探知が可能となっていることが分かる．確率的パケットマーキングは，攻撃経路逆探知には一定のパケットを収集する必要があるため，PPS の値が大きい攻撃ほど，短時間で攻撃経路逆探知が可能となっている．しかしながら，PPS の値が大きいということは，回線帯域を消費し，途中経路のルータやネットワーク装置への負荷が増大するため，経路再構成と攻撃停止を速やかに行う仕組みが実運用上では必要となる．

7. 確率的パケットマーキング方式の法的問題点と整理

本章では，日本国内において，確率的パケットマーキング方式が電気通信事業者法第 4 条に規定する，通信の秘密を侵害する行為に該当するか否かについて検討する．本方式を整理すると，確率的パケットマーキング方式は，その実施者によって，下記の行為を実施する．

(1)　ISP などの PPM 方式実施組織支配下のルータにおいて，ヘッダ IP アドレスとそのハッシュ値を取得する．

(2)　攻撃を受けたと想定されるエンドユーザはそのパケットヘッダ IP アドレスとハッシュ値を収集し，当該パケットの通過経路を取得，特定する．

(3)　エンドユーザは特定した攻撃者の攻撃行為の停止処置を行う．

一方，通信の秘密とは，それぞれの通信内容，通信にかかわる双方当事者の発信場所や通信日時などの構成要素を含み，侵害行為とは，発信，受信者の意思に反して通信の構成要素を利用することを含むとされる．これを確率的パケットマーキング方式へ適用すると，上記 (1) のヘッダ IP アドレスとそのハッシュ値の取得，(2) ヘッダ IP アドレスを用いた経路探索，(3) 攻撃行為の停止処置という行為は，明らかに攻撃者である発信者の意図に反することとなる．しかしながら，通信の秘密を侵す行為においても，正当防衛や緊急避難，正当業務行為に該当すれば当事者の同意の有無にかかわりなく許されることになる．上記 (1)〜(3) が正当業務行為にあたるかどうかの判断は，以下 3 点の正当性を満たさなければならない．

- 目的の正当性

確率的パケットマーキング方式は，正当な通信行為を維持するため，ISP などの電気通信事業者の設備や顧客を守るために攻撃を止めるために行うのであり，目的に正当性が認められる．

- 行為の正当性

確率的パケットマーキング方式は，攻撃を軽減，抑止するためにあたり，攻撃経路，攻撃者を特定する方式として他のトレースバック方式と同様に有効な方式の 1 つであって，パケットヘッダ収集から逆探知の一連の行為について，行為の正当性を有する．

- 手段の正当性

確率的パケットマーキング方式は，パケットヘッダのみの情報を収集し，外部へ公開をしないこと，組織内においても秘密情報として限られた対象へ提供されることが想定されることから手段として最低限度のものであり手段として正当であるといえる．

しかしながら，AS などの組織を超えて，パケットヘッダ情報を加工することなく平文の状態で提供することは，通信の秘密を侵害する行為となる恐れがあるため，組織を超えて PPM で得た情報を連携するためには，門林ら[11] の考察にもあるように，パケット情報をハッシュ化するなどの対策が必要である．このような秘匿化対策について，確率的パケットマーキングの各方式を法的側面から評価すると，パケットのハッシュ値，トラフィック情報などをマーキング情報とする Song らの方式，Law らの方式では通信の秘匿性を侵害する可能性が低く，組織をまたいだ IP トレースバックに用いることが可能となる．また，Goodrich の方式についてもマーキング情報が特定されていないことから，マーキング情報について，ハッシュ値などを用い秘匿化することで，組織間の IP トレースバックに適用できる．

Savage らの方式，岡崎らの方式，そして金岡らの方式については，マーキング情報が平文の IP アドレス情報となっているため，平文のままの情報を，組織を超えて共有することは通信の秘匿を犯すことにつながり，これらの方式の普及には確率的パケットマーキング情報の秘匿化のための枠組みが必要となる．

8. ま と め

本論文では，過去よりサービス妨害（Denial of Service，DoS）攻撃への対策として複数提案がされている確率的パケットマーキング方式において，従来触れられていなかった最適マーキング確率の算出を目的として，各種の評価，実験を行った．

はじめに，最適マーキング確率算出の前提となる，パケットへのマーキング負荷と攻撃経路逆探知機能について，ルータのマーキング負荷の有無，実際に逆探知が実時間内で可能であるかを確認するため，Linux PC へ確率的パケットマーキング機能の実装実験を行い，マーキング負荷は無視してよい程度であることと，実験環境でのルータ距離 $d = 2$ の実験では，3.45 秒で経路逆探知が可能であることが分かった．

上記の負荷実験により，ルータでのマーキング負荷は問題とならないことから，確率的パケットマーキングにおける最適マーキング確率は，最も短時間で攻撃経路の逆探知が可能となる確率を算出することが最適であるとして，実際のインターネットを構成するルータトポロジとあわせて確率の算出を行った．

今回の推定では，インターネットトポロジのルータ距離分布を前提とした環境を考慮し，確率的パケットマーキングにおける最適マーキング確率の算出手法を提案した．本提案手法を CAIDA 提供のインターネットトポロジ距離分布へ適用し，パケット収集時間が最短となる確率は $p = 0.082$ であるという結果を得た．さらに実際の DoS 攻撃事例として公表された情報をパラメータとして最適マーキング確率 $p = 0.082$ で確率的パケットマーキングを適用した場合の攻撃経路逆探知が可能となるパケット収集時間についてのシミュレーションを行い，攻撃者の数が 6 以下であれば 20 分以内での逆探知が可能であると予測することができた．

最後に，確率的パケットマーキング方式を実際に適用する場合に必要な，法的問題点の整理を行い，組織内で確率的パケットマーキング方式を適用し，逆探知を行うことは通信の秘密の侵害行為に該当するが，正当業務行為として違法性が阻却されると考えられることが分かった．

現在のインターネットトポロジを前提とすると，本論文において推定した，マーキング確率によって，確率的パケットマーキングを行うことにより，最短時間で攻撃経路逆探知が可能となることが明らかとなった．

参 考 文 献

1) Peng, T., Leckie, C. and Ramamohanarao, K.: Survey of Network-Based Defense Mechanisms Countering the Dos and DDoS Problems, *ACM Computing Surveys*, Vol.39, Issue 1 (2007).
2) Savage, S., Wetherill, D., Karlin, A.R. and Anderson, T.: Practical network support for IP Traceback, *Proc. ACM SIGCOMM*, pp.295–306 (2000).
3) 金岡　晃，岡田雅之，勝野恭治，岡本栄司：DoS 攻撃経路を効率的に再構築するためのトポロジ特性を利用した確率的パケットマーキング手法，*DICOMO2010* (2010).
4) 岡崎直宣，河村栄寿，林　美娘：サービス不能攻撃の経路追跡手法の効率化に関する検討，情報処理学会論文誌，Vol.44, No.12, pp.3197–3201 (2003).
5) Goodrich, M.T.: Probabilistic Packet Marking for Large-Scale IP Traceback, *IEEE/ACM Trans. Netwoking*, Vol.16, No.1, pp.15–24 (2008).
6) 竹森敬祐，遠藤彰一，中尾康二：IP 追跡システムの追跡効率を高めるための制御方式の提案と特性解析，*CSS2006* (2006).
7) Jones, R.: Netperf, available from ⟨http://www.netperf.org/netperf/⟩.
8) Olsson, R.: pktgen the linux packet generator, *linuxsimposium2005*, available from ⟨http://www.linuxfoundation.org/collaborate/workgroups/networking/pktgen⟩.
9) 総務省：情報通信統計データベース「ブロードバンド契約者数等の推移」，入手先⟨http://www.soumu.go.jp/johotsusintokei/field/tsuushin01.html⟩.
10) インターネットイニシアティブ：Internet Infrastructure Report, Vol.8, インフラストラクチャセキュリティリポート，入手先⟨http://www.iij.ad.jp/development/iir/index.html⟩.
11) 門林雄基，櫨山寛章，武智　洋：IP トレースバック相互接続におけるパケットの秘匿性に関する一考察，信学技報，電子情報通信学会 (2006.4).
12) 財団法人日本データ通信協会 Telecom-ISAC 推進会議：本トレースバック手法導入に関する法的問題の整理，トレースバック研究ポータル，入手先⟨https://www.telecom-isac.jp/tb/⟩.
13) Law, T.K.T., Yau, D.K.Y. and Lui, J.C.S.: An effective statistical methodology to trace back DDOS attackers, *IEEE Trans. Parallel Distrib. Syst.*, Vol.16, No.9, pp.799–813 (2005).
14) Snoeren, A.C., Partidge, C., Sanchez, L.A., Jones, C.E., Tchakountio, F., Kent, S.T. and Strayer, W.T.: Hash-Based IP Traceback, *Proc. 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications* (*SIGCOMM 2001*) (2001).
15) Hazeyama, H., Oe, M. and Kadobayashi, Y.: A Layer-2 Extension to Hash-Based IP Traceback, *IEICE Trans. Information and Systems*, Vol.E86, No.11 (2003).
16) CAIDA: CAIDA's Router-Level Topology Measurements, available from ⟨http://www.caida.org/tools/measurement/skillter/router_topology⟩.
17) 澤井裕子，大江将史，飯田勝吉，門林雄基：IP トレースバック逆探知パケット方式のトラヒック量と攻撃経路再構成時間の性能解析，電子情報通信学会技術研究報告 IA，インターネットアーキテクチャ，102(252), 7–13 (2002-07-19).
18) Song, D. and Prrig, A.: Advanced and Authenticated Marking Schemes for IP Traceback, *Proc. IEEE INFOCOM*, pp.876–886 (2001).
19) Nichols, K., Blake, S. Baker, F. and Black, D.: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, RFC 2474 (Dec. 1998).
20) 総務省：我が国のインターネットにおけるトラヒックの集計・試算，入手先⟨http://www.soumu.go.jp/menu_news/s-news/01kiban04_01000001.html⟩.

(平成 22 年 11 月 30 日受付)
(平成 23 年 6 月 3 日採録)

岡田　雅之

2004 年社団法人日本ネットワークインフォメーションセンター入社，2008 年筑波大学大学院システム情報工学研究科リスク工学専攻博士後期課程．インターネット経路制御，IP アドレス管理・ネットワーク運用に関するシステムの研究と開発に従事．

金岡　　晃（正会員）

2004 年筑波大学大学院博士課程システム情報工学研究科修了．同年セコム株式会社入社．筑波大学大学院システム情報工学研究科研究員を経て，2008 年より筑波大学大学院システム情報工学研究科助教．2010 年より情報通信研究機構招聘専門員兼務．ネットワークシステムの安全設計方式，暗号応用，電子認証に関する研究に従事．博士（工学）．電子情報通信学会会員．

勝野　恭治（正会員）

1998 年慶應義塾大学大学院理工学研究科計算機科学専攻修士課程修了．同年日本アイ・ビー・エム株式会社入社．東京基礎研究所主任研究員．2009 年筑波大学大学院システム情報工学研究科リスク工学専攻後期博士課程修了．2003 年ソフトウェア科学会高橋奨励賞受賞．情報セキュリティ，コンピュータ・ネットワーク，クラウドコンピューティングに関する研究開発に従事．博士（工学）．

岡本　栄司（正会員）

1973 年東京工業大学工学部電子工学科卒業．1978 年同大学院博士課程修了．工学博士．同年日本電気中央研究所入社．その後，北陸先端科学技術大学院大学，東邦大学を経て，2002 年より筑波大学教授．情報セキュリティの教育・研究に従事．1990 年電子情報通信学会論文賞，1993 年本会ベストオーサ賞受賞．著書『暗号理論入門』（共立出版），『電子マネー』（岩波書店）等．