A Proposal of an Extended Method of IP Trace-Back for Distributed Denial of Service Attacks Using Dynamic Marking Scheme

Katsuhiro Koga Non-member (Graduate School of Engineering, University of Miyazaki)
Naonobu Okazaki Member (Faculty of Engineering, University of Miyazaki)
Akira Watanabe Non-member (Faculty of Science and Technology, Meijo University)
Mi Rang Park Non-member (Mitsubishi Electric Corporation)

Keywords: Distributed Denial of Service, IP traceback, traffic monitoring, IDS

Recently, Distributed Denial of Service (DDoS) attacks is the highest priority problems on the network security. To solve this problem, the technique called "IP traceback" is developed. Fragment Marking Scheme (FMS) is a kind of IP traceback technique. In FMS, the overhead is very low. However, the number of packets for identifying attackers is huge because the downstream routers overwrite the link information marked by upstream routers.

In this paper, we propose a method called "attack detection marking scheme (ADMS)" to solve this problem by monitoring the feature of attack traffic and changing the "marking probability" of the routers. Our scheme is constructed on the system consisting of the routers on attack paths, a tracer with the network intrusion detection system (NIDS) and the victim. In this system, each router has functions of FMS, attack detection and changing the marking probability.

Each router detects on attack by monitoring traffic. We call the router which is detects attack as "attack detection router" (ADR) and denote ADR which is d hops away from the victim as $ADR(d)$. When a router detects an attack, the router changes marking probability of itself from p_{low} to p_{high} $(0 < p_{low} < p_{high} \leq 1)$. The tracer reconstructs attack path after collects packets at regular time intervals. The tracer requests $ADR(d_0)$ to change marking probability to "0" after the tracer reconstructs the attack path for $ADR(d_0)$. After this procedure, the packet marked by $R(d_0+1)$ will not be overwritten by downstream routers. Also, if $(d > d_0 + 1)$, the arrival rate of packets marked by $R(d)$ increases before $ADR(d)$ has reconstructed. In this paper, we assume that the procedure of changing the marking probability is implemented based on the simple network management protocol (SNMP) (Fig. 1).

We evaluate ADMS and FMS by some simulations and conclude that the proposal scheme is suitable for application to large scale attack compared to FMS (Fig. 2).

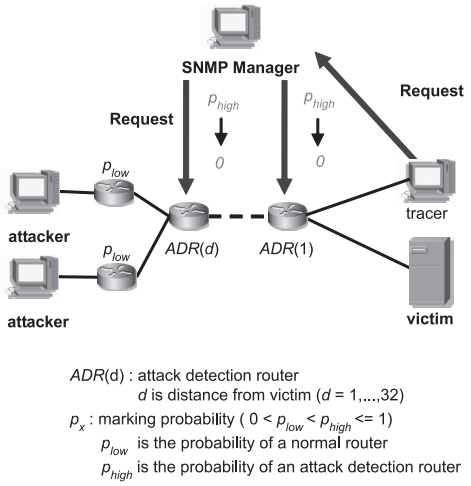


Fig. 1. Procedure of changing the marking probability in the reconstruction phase

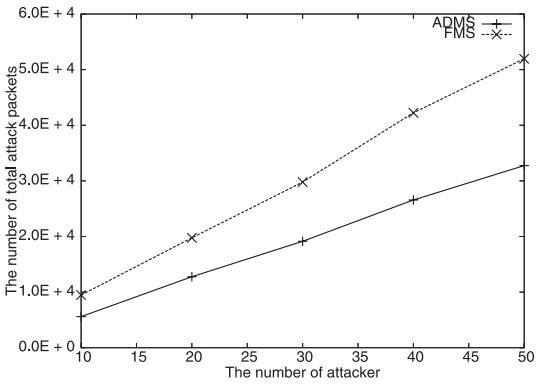


Fig. 2. The number of attack packets for reconstruction attack paths

論　文

動的マーキングを用いた効率的なネットワーク攻撃追跡手法の提案

非会員　古賀　勝寛*　　正　員　岡崎　直宣**
非会員　渡邊　　晃***　非会員　朴　　美娘****

A Proposal of an Extended Method of IP Trace-Back for Distributed Denial of Service Attacks Using Dynamic Marking Scheme

Katsuhiro Koga*, Non-member, Naonobu Okazaki**, Member, Akira Watanabe***, Non-member, Mi Rang Park****, Non-member

In recent years, DoS (Denial of Service) attack and more powerful DDoS (Distributed DoS) attack pose security problems on the Internet. As the measure to these attacks, it is important to trace attackers and stop the attacks. However, since information of the attacker is "spoofed", it is difficult to trace. Therefore, the method of specifying attackers is required. Savage et al. proposed a method to trace flooding attacks by "marked" packets. This method, however, has some problems gathering the attack packets through a lot of hops. In this paper, we propose a method to solve this problem by observing the feature of attack traffic and change the "marking probability" of the routers. We implement algorithms both of our proposed method and extending marking method to estimate the efficiency of them. From the results of some experiments, we will conclude the effectiveness of our proposed scheme.

キーワード：DDoS 攻撃，IP トレースバック，トラフィック監視，IDS
Keywords: Distributed Denial of Service, IP traceback, traffic monitoring, IDS

1. はじめに

近年，ネットワーク上の不正行為は年々増加傾向にあり，その内容も悪質化・巧妙化の一途を辿っている。中でも特に問題となっているのが，Denial of Service（DoS）攻撃である。DoS 攻撃は，攻撃対象となるサーバに対して大量の IP パケットを送りつけることで標的の持つ資源の枯渇やネットワークの輻輳を起こし，正常なサービスの運営を妨害することを目的とした攻撃である [(1) (2)]。さらに，複数の攻撃者が一斉に DoS 攻撃を行う Distributed DoS（DDoS）攻撃の増加が確認されており，攻撃による被害は今もなお拡大している。これらの攻撃への対処は，攻撃対象となるノードや，攻撃対象の属するネットワークへの影響を小さくするために，できる限り攻撃者に近いルータでパケットフィルタリングを行うことが望ましい。しかし，攻撃パケットの送信元アドレスは偽装されていることが多いため，攻撃者の特定は非常に困難である。また，DDoS 攻撃は攻撃者 1 人あたりの攻撃パケット数が通常の DoS 攻撃よりも小さいため，正規トラフィックと区別しにくいことも追跡を難しくする要因となっている。これらの送信元アドレスを偽装した攻撃に対して，その発信源を追跡するための技術を IP トレースバック技術 [(3)] と呼ぶ。既存の手法では，リンク検査手法 [(4)]，逆探知パケット手法 [(5)]，ダイジェスト手法 [(6)]，マーキング手法 [(14)] などが知られている。本論文では，これらの手法のうちネットワークやルータへの負荷が小さく，事後検討が可能であるといった利点をもつマーキング手法に着目する。マーキング手法は，ルータが転送するパケットに対して一定の確率で自身と隣接するルータの

* 宮崎大学大学院工学研究科
〒 889–2192 宮崎市学園不花台西 1–1
Graduate School of Engineering, University of Miyazaki
1–1, Gakuen-kibanadai-nishi, Miyazaki-shi 889–2192
** 宮崎大学工学部
〒 889–2192 宮崎市学園不花台西 1–1
Faculty of Engineering, University of Miyazaki
1–1, Gakuen-kibanadai-nishi, Miyazaki-shi 889–2192
*** 名城大学理工学部
〒 468–8502 名古屋市天白区塩釜口 1–501
Faculty of Science and Technology, Meijo University
1–501, Shiogamaguchi, Tempaku, Nagoya 468–8502
**** 三菱電機 (株) 情報技術総合研究所
〒 247–8501 鎌倉市大船 5–1–1
Information Technology R&D Center, Mitsubishi Electric Corporation
5–1–1, Ofuna, kamakura 247–8501

リンク情報を書き込み，このリンク情報を基に攻撃者を追跡する手法である。マーキング手法には，攻撃者の追跡に必要なパケット数が膨大になるという問題がある。この問題は，攻撃者に近い上流のルータによって書き込まれたリンク情報が，攻撃対象に近い下流のルータがリンク情報を書き込むことによって上書きされ，損失することで起こる。本論文では，トラフィック監視による攻撃の検知とマーキング確率の動的な制御によりマーキング情報の上書きを軽減し，攻撃者追跡の効率化を図る手法を提案する。

以下，まず2章でDoS攻撃とDDoS攻撃について述べる。次に，3章でDoS/DDoS攻撃の対策技術であるIPトレースバック技術について述べる。そして4章で既存のマーキング手法を紹介する。さらに5章において本論文で提案する手法について詳説する。また，6章でシミュレーションを用いて既存手法と提案手法の評価を行い，提案手法の有効性を示す。7章で6章の評価に対する考察を述べ，8章においてまとめと今後の課題を示す。

2. DoS/DDoS攻撃

DoS攻撃とは，ネットワークを利用して攻撃対象となるサーバの正常なサービスを妨害する攻撃である。一般的なDoS攻撃は，標的の処理能力を超える大量のパケットを送信することで行われる。このとき起こる攻撃対象のパフォーマンス低下は，正規トラフィックの急増によるパフォーマンスの低下と見分けることが難しい。加えて，DoS攻撃はTCP/IPに則った動作を利用しているため，回避することは非常に困難である。

DDoS攻撃とは，複数の攻撃者が同一の攻撃対象に対して一斉にDoS攻撃を行う攻撃である。DDoS攻撃は一般的に通常のDoS攻撃よりも攻撃規模が大きくなるため，サーバやネットワークへの被害はより大きくなる。DDoS攻撃において，実際にDoS攻撃を実行するノードは真の攻撃者によってウイルス等を感染させられた脆弱なノードであり，ノードの使用者は自分が攻撃を行っていることに気づかないまま攻撃に参加させられていることが多い。また，真の攻撃者は直接DoS攻撃に参加することがほとんど無いため，特定することが非常に難しい。本論文では，真の攻撃者によって踏み台とされたノードを攻撃者として扱い，提案手法では，この攻撃者を特定することを目的とする。攻撃者の特定によって，以降の攻撃を防ぎ，また可能であれば攻撃者のアクセスログから真の攻撃者を特定していくことができると考えられる。

〈2·1〉 DoS/DDoS攻撃の種類

本節では，代表的なDoS/DDoS攻撃と攻撃を行う際に利用される技術について説明する。

〈2·1·1〉 IP spoofing IP spoofingとは，信頼できるネットワーク上に存在する別のコンピュータになりすますことをいう。攻撃者は，自身のIPアドレスとは別の実在するIPアドレスを取得し，そのアドレスを利用してネットワークの防御をやぶる[8]。

〈2·1·2〉 Smurf Smurf攻撃は，ネットワークの到達可能性を調査する「pingコマンド」を悪用した攻撃である。この攻撃では，踏み台となるネットワークAのブロードキャストアドレスに対して，実際の攻撃対象となるホストBを送信元に設定したICMP Echo Requestパケットを送信する。これにより，ネットワークAに存在するコンピュータはホストBに対して一斉にICMP Relay Packetを送信することになる。ここで，大量のpingを実行した場合，その応答パケットは増幅された膨大な量のICMP Echo Replyパケットとなって，標的を攻撃することになる[9]。

〈2·1·3〉 Teardrop Teardrop攻撃とは，断片化されたIPパケットをつなぎ合わせる際の，TCP/IPの実装上の問題を突いた攻撃方法である。この攻撃では，IPv4ヘッダ中のIDフィールドの情報を擬装し，オフセット情報が重複するような不正なIPパケットの断片を生成する。攻撃対象のシステムが重複したIPパケットの断片をうまく処理できない場合，このパケットはクラッシュの原因となる[10]。

〈2·1·4〉 SYN flooding攻撃 SYN flooding攻撃は，IP spoofingを行ったSYN（接続要求）パケットを大量に送信する攻撃である。このとき攻撃対象となったサーバは，送信元アドレスに対してSYN/ACKパケットを返信するが，送信元アドレスは偽装されたものであるため通信できない。そのため攻撃対象は，応答待ち状態を維持するために大量のリソースを消費することになり，正規の通信の遅延や，システムのクラッシュやダウンが起きる[11]。

〈2·2〉 攻撃トラフィックの特徴

一般的なDoS攻撃では，攻撃者は攻撃対象に対してIP spoofingを行った特定の種類のパケットを大量に送信する。そのため，DoS攻撃は特定の種類のパケットが攻撃開始からの短時間で急増するといった特徴を持つ。代表的な例では，SYN flood攻撃におけるSYNパケットの急増が挙げられる。正規の通信において，SYNパケットはTCP接続を行う際に1コネクションにつき1パケットだけ発生する。しかし，DoS攻撃時のSYNパケットの数は通常時の数十倍以上に増加し，1つのホストに対して少なくとも200packets/second(pps)から500pps，大規模な攻撃では600,000ppsものSYNパケットが発生することがわかっている[1][2]。また，攻撃の期間は短いもので十分間，長いもので数日間にわたって行われることが確認されている。以上のことから，本論文では攻撃トラフィックを以下に示す特徴を持つものとして扱う。

- 特定の種類のパケットについて，通常時の数十倍を上回るパケットが発生する
- 攻撃時のパケットは，IP spoofingを伴う
- トラフィックの増加は，一定時間継続する

また，一般的なDDoS攻撃は攻撃対象に最も近いルータ（以下，NVR:Nearest Victim Router）を根とし，攻撃者に最も近いルータ（以下，NAR：Nearest Attacker Router）を葉とする木構造をとる。そのため，攻撃トラフィックはNVRに集約し，NARに向かって分散していく特徴を持つ。

このとき，NAR 付近のトラフィック量の増加は DoS 攻撃ほど顕著ではないため，NAR 付近のルータによる攻撃の検知は難しいと考えられる。

3. トレースバック技術

前述したように，DDoS 攻撃は送信元アドレスを偽装したパケットを用いて攻撃を行うため，送信元を特定することは非常に難しい。そこで，攻撃経路上のルータを利用して攻撃者を推定するトレースバック技術が研究されている。本章では，トレースバック技術の主な手法を紹介し，それらについて比較を行う。

〈3･1〉 アプリケーショントレースバック技術　アプリケーショントレースバック技術は，アプリケーション層の情報を利用して攻撃者を追跡する技術である。そのため，プロクシサーバを経由する渡り歩き攻撃にも対応している。しかしながら，多量のトラフィックを常時観測し，さらにトラフィックをストリームごとに分けてダイジェストを取るといった処理を行う必要があり，大規模な攻撃に対する適時性に問題がある。

〈3･1･1〉 thumbprinting　本手法は，ネットワーク上を流れるパケットストリームを離散的時間間隔に分け，一定間隔毎にパケットストリームのダイジェストを作成し，複数個所で生成されたダイジェスト間の類似性を求めることで攻撃経路を推定する手法である [12]。広範囲でダイジェストの比較を行うことで，非暗号化パケットストリームに対して有効なトレースバックを行うことができる。

〈3･1･2〉 timing thumbprinting　本手法は，thumbprinting 手法と同様に，パケットストリームのダイジェストを比較することによって攻撃者を推定する技術である [13]。ダイジェストを生成する際に，ネットワークプロトコルの特徴，及び人間，コンピュータの相互関係を取り入れることで，ダイジェスト比較の際に時間をベースにした比較を可能にした。時間を主軸にした比較を行うことで，暗号化された通信に対してもより正確な比較を行うことができる。

〈3･2〉 IP トレースバック技術　IP トレースバック技術は，主にネットワーク層の情報を利用したトレースバックを行う技術である。以下に，IP トレースバック技術の主な手法を紹介し，それらについて比較を行う。

- リンク検査手法
- 逆探知パケット手法
- ダイジェスト手法
- マーキング手法

以下に各手法の特徴について述べる。

〈3･2･1〉 リンク検査手法　本手法は，ルータの持つフィルタリング機能を利用し，ネットワーク管理者が手動で攻撃フローの特定をする手法である [4]。まず，攻撃対象に一番近いルータの出力ポートで攻撃パケットの特徴を抽出することで，攻撃パケットの入力ポートを特定する。そして，この入力ポート情報から，隣接する上流のルータを特定する。この作業を NAR に到達するまで繰り返すことで，攻撃者の追跡を行う。既存のルータを利用した追跡が可能なため，導入コストが最小限で済むといったメリットがある反面，攻撃トラフィックが発生している間しか追跡が行えないことや，管理者の手動追跡であるため，長い追跡時間を要する点が問題である。

〈3･2･2〉 逆探知パケット手法　本手法は，攻撃経路上にあるルータが追跡用の端末に向けてリンク情報を含むパケットを送信し，追跡用の端末が収集したリンク情報を基に攻撃経路の特定を行う手法である [5]。リンク情報の送信には ICMP(Internet Control Message Protocol) を用いる。全てのルータは，低い確率 p（例： $p = 1/20000$）で ICMP Traceback メッセージを新たに生成して，追跡用の端末に送り届ける。この ICMP Traceback メッセージには，メッセージを生成したルータの IP アドレスやリンク情報，並びにインターフェース名，公開鍵などが収められる。追跡用の端末は，受け取った ICMP Traceback メッセージを基に攻撃経路を推定する。この手法は，既存バックボーンシステムに影響を与えることなく導入することが可能であるという利点がある。しかし，ネットワーク上に ICMP パケットをフィルタリングするルータやファイアウォールを実装している場合は導入ができないことや，追跡を行うときに新たなパケットが生成されるため，ネットワークへのオーバーヘッドが発生することが問題である。

〈3･2･3〉 ダイジェスト手法　本手法は，ルータがパケットを転送する際にそのログを保持し，このログを辿ることで攻撃者の追跡を行う手法である [6]。このとき，ログの保存にハッシュ値を用いることで記録領域の節約を図っている。この手法は，1 パケットからの追跡が可能であることや，事後検討が可能であるといった大きな利点がある。しかし，ログを保持するのに莫大な記憶容量が必要であることや，高いハッシュ処理能力が必要であるといった問題がある。本手法の発展である L2-based トレースバックでは，DoS 攻撃の可能性のあるパケットのみを記録の対象とすることにより，メモリと CPU パワーの削減を可能としている [7]。ただし，DDoS 攻撃は対象としていない。

〈3･2･4〉 マーキング手法　本手法は，攻撃経路上にあるルータが転送するパケットに対して直接リンク情報を書き込み，この情報を基に攻撃経路の特定を行う手法である [14]。新たなパケットを生成しないためルータやネットワークへのオーバーヘッドが小さいという利点がある反面，攻撃対象から同じ距離に複数のルータがある場合，分割したリンク情報を復元する際にその組み合わせ数が膨大になり，整合性を確認するのに非常に時間がかかるという問題がある。本論文では，管理コストの低さ，ネットワークへのオーバーヘッドの小ささ，事後検討が可能である点からマーキング手法に着目し，そのスケーラビリティ向上を図る。

4. マーキング手法

本章では，既存のマーキング手法として Fragment Marking Scheme(FMS) [14] 及び関連する手法について紹介する。

〈4·1〉 FMS と関連手法　FMS では，隣接する 2 つのルータが持つ IP アドレスの組から生成した情報によってリンクを表現する。このリンク情報は奇数ビットにルータの IP アドレス，偶数ビットに IP アドレスから生成したハッシュ値を持つ 64bit の値となる。ルータはリンク情報を 8 つに分割し，一定の確率 p（例 : $p = 1/25$）で分割した値のいずれか 1 つをパケット中の通常使用されていない領域に挿入する。FMS では，リンク情報を書き込む領域として IPv4 ヘッダ中の識別子 (Identification) フィールドを 3 つに分割して用いる。

識別子フィールドは，パケットが断片化するときに用いられるフィールドである。しかし，フラグメント化されたパケットは，インターネット全体を流れるトラフィックから見てほんの僅かである [3]。そこで，マーキング手法では識別子フィールドを利用することによる正規通信への影響は無いものと仮定している。

分割したフィールドには，それぞれ以下の値を書き込む。

（1） フラグメント値：分割したリンク情報。

（2） オフセット値：フラグメント値が，リンク情報のどのビットを表すのか識別するための値。

（3） 距離値：リンク情報を書き込んだルータと，攻撃対象までの距離を示す。初期値として 0 を取り，リンク情報を書き込まれなかった場合に 1 つ増加する。そのため，攻撃対象から d ホップの位置にあるルータが初期マーキングを行った場合，距離値は $d-1$ となる。

リンク情報の生成と分割の様子を図 1 に示し，FMS におけるマーキング領域の構造を図 2 に示す。そして，距離値 0 のパケットを受け取ったルータは，パケット中のフラグメント値と，自身のフラグメント値の排他的論理和を取る（以降，エッジ ID と呼ぶ）。ルータはエッジ ID をパケットのフラグメント値に上書きすることで 2 つのルータのリンクを表す。以降，ルータがパケットにフラグメント値を書き込む処理を初期マーキング，エッジ ID を書き込む処理を終端マーキングと呼び，初期マーキングされたパケットをマーキングパケットと呼ぶ。

攻撃対象は収集したリンク情報を基に，NVR を根とする攻撃経路ツリーを構築することで攻撃者の特定を行う。この処理を攻撃経路の再構築処理と呼ぶ。このとき，攻撃対象はパケット中のフラグメント値，及びエッジ ID をオフセット値と距離値に基づいて整理し，同じ距離値を持つリンク情報の全ての組み合わせを作る。この復元したリンク情報の整合性を確認するため，攻撃対象は復元したリンク情報に対して，奇数ビット (IP アドレス) からハッシュ値を生成する。リンク情報が正しければ，ここで生成したハッシュ値は偶数ビット (ハッシュ値) と一致する。このようにして得られたリンク情報中の IP アドレスを用いて攻撃経路の特定を行う。ここで，マーキング時にルータが書き込むリンク情報と攻撃対象が収集する情報の一覧，及び攻撃対象が収集した情報から攻撃経路の推定を行う様子を，図 3 に示す。ただし，ここでは簡単化のためリンク情報を分割しないときの様子を示す。

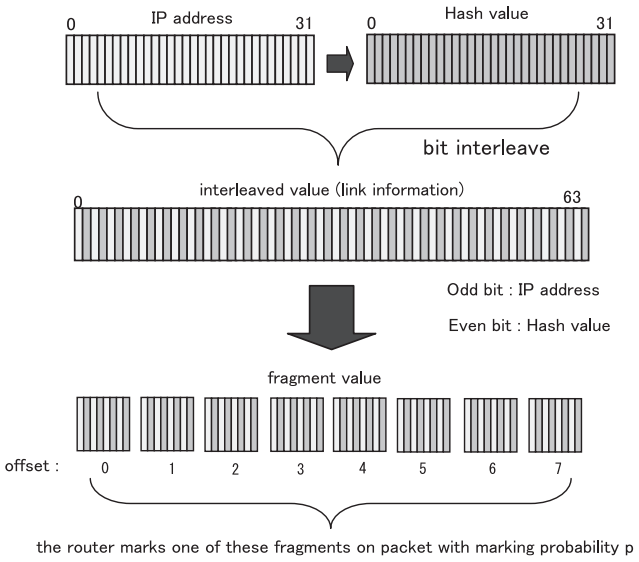


Fig. 1.　Generation of marking information.

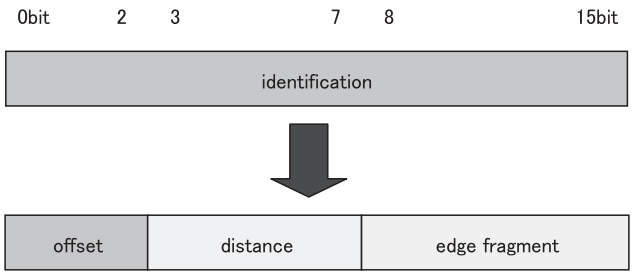


Fig. 2.　Marking field of FMS.

また，攻撃対象に NVR を根とする上流ルータマップを持たせることで追跡の効率化を図る手法として，AMS [15]，FIT [16] が挙げられる。これらの手法は，上流ルータマップとそれに対応するリンク情報テーブルを持つことを前提とし，これを利用することでリンク情報の整合性を効率的に確認することができる。しかしながら，攻撃対象が常に最新のルータマップを持つ必要があるため，実装が難しいことが問題である。

〈4·2〉 FMS の問題点　FMS では，マーキング領域として識別子フィールドを採用している。しかし，識別子フィールドに設定される値は実装により異なるため，一般的には不定であると考えられる。そのため，この値を用いてパケットがマーキングされたものであるかどうかを識別することは難しい。そこで，リンク情報の復元はマーキングされていないパケットも含めた全てのパケットを対象に行われる。そのため，攻撃経路の再構築に用いられるパケット数は非常に大きなものになる。ここではこれを FMS の観察量問題と呼び，全ての攻撃経路を再構築するために必要なパケット数を観察量と呼ぶ。

■Marking information of each router

router	initial marking	end marking
R(4)	frag(4)	
R(3)	frag(3)	edgeID(3) = frag(3) xor frag(4)
R(2)	frag(2)	edgeID(2) = frag(2) xor frag(3)
R(1)	frag(1)	edgeID(1) = frag(1) xor frag(2)

■Marking information that the victim obtains
frag(1), edgeID(1), edgeID(2), edgeID(3)

■Procedure of path reconstruction
1. frag(1) xor edgeID(1) = frag(2)
2. frag(2) xor edgeID(2) = frag(3)
3. frag(3) xor edgeID(3) = frag(4)

■Reconstructed router's information
frag(1), frag(2), frag(3), frag(4)

■The routers on reconstructed attack path
R(1), R(2), R(3), R(4)

R(i) : the router at i hops away from the victim
frag(i) : fragment value marked by R(i)
edgeID(i) : edge value marked by R(i) and R(i−1)

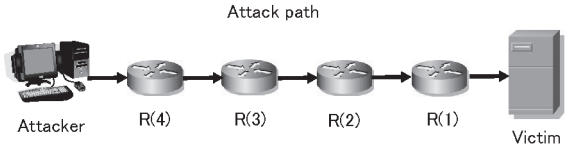


Fig. 3. Procedure of the marking and the path reconstructing.

また，ルータから d ホップ離れた位置にあるルータの数を r_d とすると，距離値 $d-1$ を持つマーキングパケットからリンク情報を復元すると，その組み合わせ数は $(r_d)^8$ になる。ここで，攻撃対象に届くパケットのうちマーキングされていないパケットが n_{fms} 個あり，これらのパケットの識別子フィールドはランダムであると仮定する。このとき，マーキングされていないパケットがある特定の距離値とオフセット値を持つ確率は $1/(32\times 8)$ である。このような値を持つ非マーキングパケットの数の期待値は， $n_{fms}/256$ となる。ここで，距離値 $d-1$ を持つパケット全てを対象に考えた場合，リンク情報の候補数 $L_{max}(d)$ は，

$$L_{max}(d) = \left(r_d + \frac{n_{fms}}{256}\right)^8 \quad \cdots\cdots\cdots\cdots\cdots\cdots (1)$$
$$(2^{64} > L_{max}(d) > 0)$$

となる。例えば $r_d = 10$ のとき，$L_{max}(d) > 10^8$ となり，復元したリンク情報の整合性を判断するために莫大な時間が必要になる。ここでは，これを FMS の計算量問題と呼び，リンク情報の整合性を判断する回数を計算量と呼ぶ。

また，ルータは転送するパケットが既にマーキングされているか否かに関わらず，一定の確率で初期マーキングを行う。そのため，マーキングを行ったルータから攻撃対象まで距離があるとき，マーキングパケットはさらに下流のいずれかのルータによってマーキング情報を上書きされることがある。その結果，攻撃者を特定するためにより多くのパケットが必要となる。

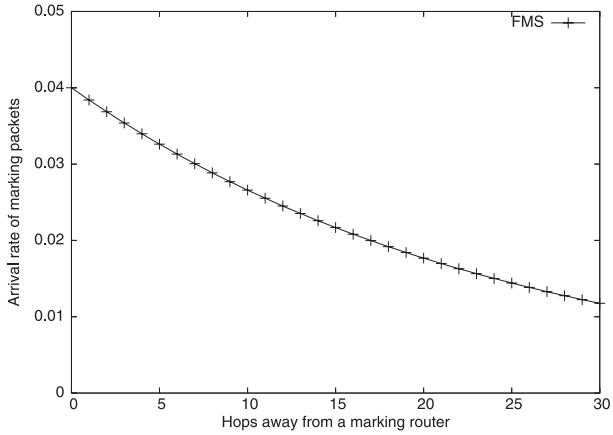


Fig. 4. The arrival rate without overwriting the marking.

ここで，全てのルータが一定確率 p でマーキングを行うとする。このとき，あるパケットが攻撃対象から d ホップ離れたルータ $R(d)$ によってマーキングされ，かつ下流のルータによってマーキング情報を上書きされずに攻撃対象まで届く確率 $Np(d)$ は，

$$Np(d) = p(1-p)^{d-1} \quad \cdots\cdots\cdots\cdots\cdots\cdots (2)$$

となる。ここで，図 4 は $p = 1/25$ における，$Np(d)$ の値を示している。この図から，攻撃対象から特に遠いルータ (NAR など) からのマーキング情報を得ることのできる確率が，攻撃対象に近いルータ (NVR など) からの情報が届く確率と比較して小さいことがわかる。例えば $R(15)$ のマーキングパケットが攻撃対象に届く確率は，$R(1)$ のマーキングパケットが到達する確率の約半分しかない。

また，$R(d)$ がリンク情報を k 分割して書き込むとする。このとき，1 つの攻撃経路を再構築するのに必要なパケット数の期待値 $E(X)$ は，

$$E(X) = \frac{k \cdot ln(kd)}{p(1-p)^{d-1}} \quad \cdots\cdots\cdots\cdots\cdots\cdots (3)$$

となる [14]。ここで，FMS では $k = 8$ であるため，$E(X)$ は $d = 1$ で 433 パケット， $d = 15$ で 1766 パケットとなる。また，NAR の特定に必要なパケット数は，途中で複数の攻撃経路が合流したとしても殆ど変化しない。マーキング手法では NAR の特定により攻撃者の追跡を完了するため，観察量は $E(X)$ に攻撃者数をかけた値に近似できると考えられる。DDoS 攻撃の攻撃者数は数千～数万にも至ることがあるため，この時の観察量は膨大なものになると考えられる。

一般に，DDoS 攻撃の攻撃経路は攻撃対象を根とし攻撃者を葉とする木を構築する。したがって，攻撃対象に近いルータほどトラフィック量が多く，より多くのパケットをマーキングすることになる。つまり，攻撃対象に近いルータほど，必要以上のマーキングパケットを生成し，同時にマーキング情報の上書きを行う傾向があると考えられる。したがって，トラフィック量の多いルータにおける処理を

改善することで，より効率的な攻撃者の追跡が可能になると考えられる。

〈4・3〉 動的確率パケットマーキング手法　マーキング手法では，攻撃対象となるサーバから遠い位置にあるルータの情報を得るのに多くのパケットを必要とする。そこで，攻撃者に近い上流のルータのマーキング確率を高くし，攻撃対象に近づくに従ってマーキング確率を減らすことで，攻撃対象から遠い位置にあるルータのマーキング情報を取得する確率を高め，効率の良いトレースバックを試みる研究が行われている。本論文ではこの技術を動的確率パケットマーキング手法と呼ぶ。以下に，代表的な動的確率パケットマーキング手法を挙げる。

〈4・3・1〉 Adjusted probabilistic packet marking scheme　本手法は，攻撃者と現在パケットの中継をしているルータとの距離を基にマーキング確率を変更する手法である[17]。攻撃者からルータまでの距離を，パケットのIPv4 ヘッダに含まれる IP option フィールド内に記述する。以下では，本手法を APPM と呼ぶ。

〈4・3・2〉 Dynamic probabilistic packet marking scheme　本手法は，パケット中の IPv4 ヘッダに含まれる TTL 値 (Time to live) の値を基にマーキング確率を調整し，効率的なトレースバックを試みる手法である[18]。以下では，本手法を DPPM と呼ぶ。

5. 提案手法

〈5・1〉 ADMS の概要　図5 に，式3 において，$k = 8$ のときに 1 つの攻撃経路を再構築するのに必要なパケット数を示す。このとき，各グラフはマーキング確率 $p = 1/100, 1/25, 1/10, 1/5, 1/2$ のときのパケット数の期待値を表す。

この図からわかるように，マーキング確率が高いとき，攻撃対象に近い位置からの攻撃を素早くトレースバックすることができる。しかし，マーキング確率が低いときのほうが，マーキング確率が高いときよりも，攻撃対象に遠い位置からの攻撃を素早くトレースバックすることができている。これは，マーキング確率が高いと，マーキング情報の上書きが起こりやすいからであると考えられる。従って，トレースバックを行う際に，マーキング確率を高くし，さらに攻撃経路を擬似的に短くすることができれば，より効率的なトレースバックを行うことができると考えられる。

本論文ではこの点に着目し，動的にマーキング確率を変更することで効率的に攻撃者の追跡を行う手法を提案する。

以下では，この手法を Attack Detection Marking Scheme（ADMS） と呼ぶ。

提案手法は，従来手法の機能に加えて，いくつかの機能を必要とする。新たに追加する機能として，ルータ上での簡易な攻撃検知機能，攻撃対象側からルータに対してマーキング確率を動的に制御する機能が挙げられる。このとき，提案手法のシステムは，マーキング手法対応ルータと，NIDS（ネットワーク型侵入検知システム）[19] 機能やトレースバック機能を持つトレーサ端末，及びルータに対してマーキング中止命令を出す管理端末によって構成される。また，攻撃対象へのトラフィックはトレーサによって監視されているものとする。

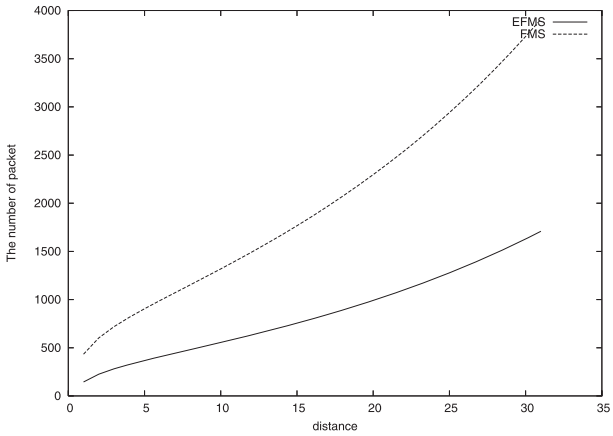


Fig. 5. The expected number of necessary attack packets for attack paths reconstruction.

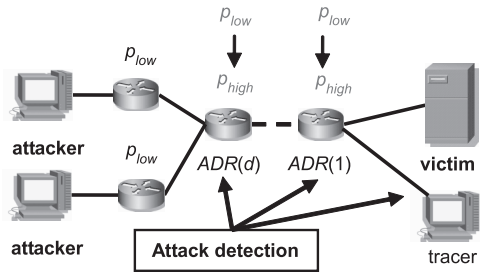
本論文ではシステムの基幹となる従来のマーキング手法として，ルータマップを必要としないことによる実現性の高さから FMS のアルゴリズムを基にしたマーキングと経路の再構築を行う。次に，ADMS の手順を攻撃検知手順，攻撃検知時のマーキング確率変更手順，経路再構築時のマーキング確率変更手順，マーキング手順，経路再構築手順の 5 つに分けて述べる。

〈5・2〉 ADMS の処理手順

A. 攻撃検知手順

ルータは攻撃の特徴を持つトラフィックを識別することで簡易な攻撃の検知を行う。以下，攻撃を検知したルータを ADR (Attack Detection Router) と呼ぶ。ルータは起動後，一定確率でマーキングを行いながら自身を流れるトラフィックの監視を行う。DDoS 攻撃中は特定の種類のパケットが少なくとも通常時の数倍から数十倍発生するため，ルータは宛先アドレスごとにパケットの監視を行い，このようなトラフィックの急増を攻撃の特徴として捉える[20]。しかし，DDoS 攻撃による 1 攻撃者あたりのトラフィック量の増加は，DoS 攻撃におけるトラフィック量の増加に比べて非常に小さい。そのため，ADR は攻撃者数人分のトラフィックが集約された際のトラフィック量を閾値とすることで，正規のトラフィックを攻撃として誤検出することをできるだけ防ぐ。このとき，攻撃トラフィック量は攻撃対象に近い下流のルータほど多くなる。そのため，ある ADR より下流にあるルータは ADR になると考えられる。

また，攻撃対象はトレーサを用いて攻撃の検知を行う。ここでは，トレーサは攻撃パケットと正規のパケットを識別する機能を持ち，正確に攻撃を検知することができるものとする。このとき，トレーサには全ての攻撃トラフィックが集約するため，いち早く攻撃を検知することができる。



ADR(d) : attack detection router
d is distance from victim (d = 1,...,32)
p_x : marking probability (0 < p_{low} < p_{high} <= 1)
p_{low} is the probability of a normal router
p_{high} is the probability of an attack detection router

Fig. 6. Procedure of changing the marking probability in the detection phase.

B. 攻撃検知時のマーキング確率変更手順

攻撃対象から d ホップの位置にあるルータを $R(d)$，ADR を $ADR(d)$ と表す。このとき，NVR は $d = 1$ である。また，通常時のマーキング確率を p_{low}，攻撃検知時の ADR のマーキング確率を p_{high} とする。

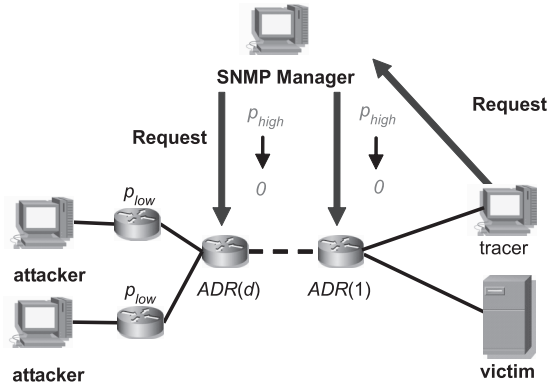
攻撃を検知したルータは，自身のマーキング確率を通常時よりも高い値 p_{high} に変更する（図 6）。

この変更により，ADR はより少ないパケット数で自身のリンク情報をトレーサに届けることができるため，通常のルータよりも素早く攻撃経路を再構築できる。

このとき，トラフィックが集約する下流のルータはいち早く攻撃を検知するため，特に素早く経路の再構築ができると考えられる。このとき，一時的にマーキング情報の上書きが発生しやすい状態になるが，その一方で次に示す経路再構築時のマーキング確率の変更手順を早い段階で受けることが可能となる。

C. 経路再構築時のマーキング確率変更手順

トレーサは攻撃を検知すると，攻撃パケット中のマーキング情報を収集し始める。そして，その情報を基に攻撃経路の再構築を行う。ここで，トレーサが距離 d_0 にあるルータ $ADR(d_0)$ までの攻撃経路を再構築したとする。このとき，トレーサは管理端末に対して，$ADR(d_0)$ のマーキングを中止するように要請する。管理端末はトレーサから要請を受けると，$ADR(d_0)$ に対して，マーキングを中止するように命令する (図 7)。この変更後，$ADR(d_0)$ の 1 つ上流に位置するルータ $R(d_0+1)$ がマーキングしたパケットは，マーキング情報を上書きされることなくトレーサに届けることができる。同様に $d > d_0+1$ に位置するルータ $R(d)$ は，$ADR(d_0)$ の再構築前よりも高い確率でマーキングパケットをトレーサに届けることができる。このようにマーキング情報が上書きされる確率が減少することによって，トレーサは $R(d_0+1)$ より上流のルータの再構築を素早く行うことができる。この手順を繰り返すことで，より少ない観察量で全ての攻撃者の特定が可能となる。このとき，マーキング中止命令はトラフィック量の多いルータほど早い段階で行われる。そのため，トラフィック量が多いルータほど再構築後のマーキング情報の上書きを，より大きく抑えることができる。マーキング中止命令は，例えば SNMP(Simple Network Management Protocol) を用いて実現することができる†。ここでは，ルータは SNMP エージェントを備えているものとし，拡張 MIB(Management Information Base) にルータのマーキング確率をオブジェクトとして追加することを前提とする。また，ルータへの命令は，トレーサが SNMP マネージャを実装した管理端末を介して行うものとする。以下に，SNMP のコマンドを用いて処理手順を示す。



ADR(d) : attack detection router
d is distance from victim (d = 1,...,32)
p_x : marking probability (0 < p_{low} < p_{high} <= 1)
p_{low} is the probability of a normal router
p_{high} is the probability of an attack detection router

Fig. 7. Procedure of changing the marking probability in the reconstruction phase.

【STEP1】 トレーサは管理端末に，再構築済みのルータが以降のマーキングを行わないように要請する。

【STEP2】 管理端末は SetRequest コマンドを用いて，再構築したルータに対してマーキング確率を 0 に落とすように要求する。

【STEP3】 ルータは GetResponse コマンドを用いて，管理端末にマーキング確率を 0 に落としたことを通知する。

【STEP4】 管理端末はマーキングの中止が完了したことをトレーサに通知する。

D. マーキング手順

（1） **準備段階** ルータが起動時に行う処理である。ルータは自身の IP アドレスを基にリンク情報を生成し，リンク情報を分割してフラグメント値を得る。

（2） **初期マーキング** ルータがパケットの転送時に行う処理である。通常時，及び攻撃検知時に予め設定した確率で，パケットにオフセット値とそれに対応するフラグメント値を書き込み，距離値を 0 にする。また，通常時と攻撃検知時の相違点を以下に述べる。

† SNMP はルータやホスト，ハブといったネットワークに接続された通信機器をネットワーク経由で監視・制御するためのプロトコルである [21]。

i) 通常時

ルータは一定の確率 p_{low} で初期マーキングを行いながら，自身を流れるパケットの監視を行う。このときのマーキング確率は，距離の離れたルータからのマーキングパケットの到達率が大きく，ルータへの負担が小さい値として従来手法と同じ確率を用いる (例: $p_{low} = 1/25$)。ルータは監視しているトラフィックから攻撃の特徴を捉えると，攻撃検知時の動作に移行する。

ii) 攻撃検知時

$ADR(d)$ は自身のマーキング確率を一時的に高い値 p_{high} に変更し，以降は一定の確率 p_{high} で初期マーキングを行う。

（3） **終端マーキング** ルータがパケットの転送時に行う処理である。初期マーキングが行われなかった距離値 0 のパケットに対して，自身のフラグメント値とパケットのフラグメント値の排他的論理和を取り，この値 (以下，エッジ ID と呼ぶ) をパケットに上書きし，距離値を 1 つ増やす。

（4） **転送ルータによる処理** ルータがパケットの転送時に行う処理である。初期マーキングが行われなかった距離値 0 以外のパケットに対して距離値を 1 つ増やす。

このとき，距離値は初期値を 0 とするため， $R(d)$ によってマーキングされたパケットの距離値は $d-1$ となる。

E. 経路再構築手順

トレーサは一定時間パケットを収集した後，収集したパケット中のフラグメント値とエッジ ID から，リンク情報の復元を行う。トレーサは，このとき復元した $R(d)$ に対して管理端末経由でマーキングの中止命令を出す。管理端末はこの $R(d)$ が ADR であった場合，マーキング確率を 0 に変更し，処理が完了したことをトレーサに通知する。トレーサはその後，全ての NAR を復元するまでパケットの収集，経路再構築，及びマーキング中止要請を繰り返し行う。このとき，再構築手順によって攻撃経路上にあることを推定されたルータは，マーキング中止命令を受けるまでマーキングパケットを生成し続ける。提案手法では，マーキング中止命令を出すことで，以降のマーキング情報の上書きを防ぐことができる。そこで，提案手法ではパケットの収集間隔をできる限り短くすることで，マーキング中止命令を素早く出し，マーキング情報の上書きをトレースバックの早い段階から防いでいる。しかし，収集間隔を短くすると，一度のパケット収集で全ての経路を再構築することはとても難しくなる。そこで本論文では，フラグメント値の組み合わせによって生成されるリンク情報候補の数に注目して再構築処理の効率化を図る。$R(d)$ のリンク情報の候補数 $L(d)$ は，次の式で求められる。

$$L(d) = \prod_{i=0}^{k-1} chk(i)(d) \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (4)$$

ここで，i はオフセット番号であり，$i = 0...k-1$ (例：$k = 8$) をとる。また，$chk(i)(d)$ は，$R(d)$ から受け取った i 番目のフラグメントの重複分を除いた数を示す。

例えば， x 回目の再構築で $d = d_0$ となる $R(d_0 - 1)$ までの経路を全て再構築できていると仮定する $(x > 0)$ 。そして $(x+1)$ 回目のパケット収集で，$d_0 > d$ に位置する $R(d)$ からマーキングパケットが来たとする。このとき，$L(d)$ の値は変化することがないため再構築手順は行わず，パケットの収集を再開する。また， $(x+1)$ 回目のパケット収集で， $d >= d_0$ に位置する $R(d)$ から未知のフラグメントが届いたとする。このとき， $L(d)$ の値は増加するため，再構築手順を行う。この $(x+1)$ 回目の再構築手順では $R(d_0)$ の再構築を行い，また $d > d_0$ に位置するルータ $R(d)$ の再構築は，$(x+1)$ 回目の再構築手順で初めて特定された $R(d_0)$ のリンク情報だけを利用して再構築を継続する。

6. 評　価

本章では，従来手法である FMS と，FMS を拡張した APPM，DPPM，及び提案手法である ADMS についてシミュレーションを用いて評価を行う。しかし，FMS は観察量が非常に大きく，大規模な攻撃に対する評価を行うのに適していない。そこで，本論文では，FMS を拡張した Extended FMS (EFMS) を評価対象として用い，APPM，DPPM，ADMS を EFMS の拡張という位置づけでシミュレーションを行う。

〈6･1〉 Extended FMS　EFMS では新たにマーキング領域として ToS フィールド [22] を採用することでフラグメント数を減らし，より大きな規模の攻撃への対応を図る。ToS フィールドは通信の優先度を決めるフィールドであるが，通常の通信では用いられないため，正規通信への影響はごく小さいものであると考えられる。このときのマーキング領域の構造を図 8 に示す。以下に，観察量と計算量の観点から FMS と EFMS の評価を行う。

〈6･1･1〉 観察量の評価　ここでは，EFMS と FMS の観察量を比較する。ここでは簡単化のために攻撃経路が 1 つであると仮定する。このとき，FMS の観察量を $E_{fms}(X)$，EFMS の観察量を $E_{efms}(X)$ とする。このとき，FMS のフラグメント数は $k = 8$，EFMS のフラグメント数は $k = 4$ をとるため，両手法の観察量の比は，式 3 より

$$\frac{E_{efms}(X)}{E_{fms}(X)} = \frac{\frac{4 \cdot ln(4d)}{p(1-p)^{d-1}}}{\frac{8 \cdot ln(8d)}{p(1-p)^{d-1}}} = \frac{ln(4d)}{2 \cdot ln(8d)} \cdots\cdots\cdots (5)$$

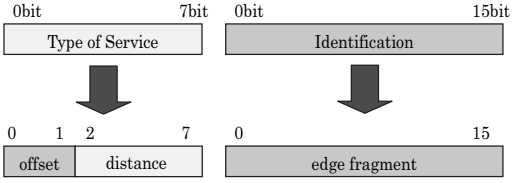


Fig. 8. Marking field of EFMS.

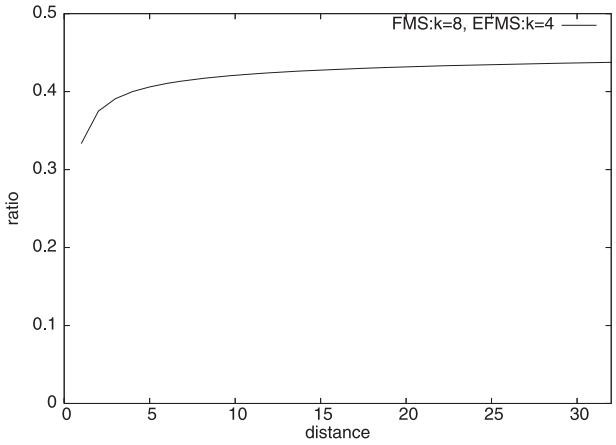


Fig. 9. $E_{efms}(X)/E_{fms}(X)$ for distance between an attacker and a victim.

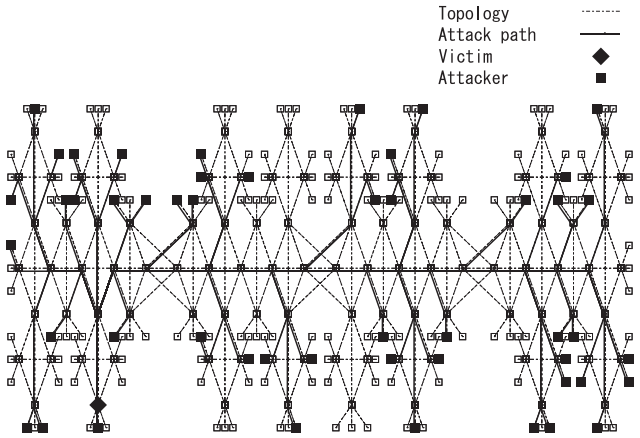


Fig. 10. Network topology and attack paths.

Table 1. The spec of PC.

OS	Fedora Core 5
CPU	Pentium4 1.7GHz
Memory	1GB

となる。攻撃対象から d ホップ離れた場所における $E_{efms}(X)/E_{fms}(X)$ の値を図9に示す。このとき，EFMSはFMSの45 %以下の観察量で攻撃者の追跡ができることが分かる。

〈6・1・2〉 計算量の評価 攻撃対象から d ホップ離れた位置に r_d 個のルータがあり，これらのルータはリンク情報を k 個のフラグメントに分割すると仮定する。ここで，簡単化のためマーキングパケットのみを対象とした場合の計算量について考える。このとき，FMSの計算量は $(r_d)^k = (r_d)^8$ となる。同様に，EFMSの計算量は，$(r_d)^4$ となる。従って，EFMSの計算量は，FMSの $\frac{(r_d)^4}{(r_d)^8} = \frac{1}{(r_d)^4}$ となる。例えば $r_d = 10$ のとき，EFMSはFMSの $1/10000$ の計算量となり，非常に早く計算ができることがわかる。

〈6・2〉 シミュレーション環境

〈6・2・1〉 ネットワークトポロジ 本論文では，トレーサが攻撃パケットと非攻撃パケットの正確な切り分けを可能とし，攻撃発生と同時に攻撃を検知できることを前提とする。また，ネットワークの通信遅延・輻輳・パケットロスは考慮しない。シミュレーションで用いたネットワークトポロジは，実際にインターネット上で構築されているトポロジを参考に構築した[23]。本ネットワークは，複数のリングネットワークが連結した状態を想定している。そして，攻撃経路はダイクストラ法によって導出した最短経路を用いて生成した。図10は，シミュレーションで用いたネットワークトポロジを破線，及び攻撃経路を実線で表している。同図は，298個のルータを持つネットワーク上で，50人の攻撃者によって行われる攻撃の様子を示している。

〈6・2・2〉 攻撃モデル 攻撃は全攻撃者で等しく $10packets/second(pps)$ で連続的に行われるものとする。攻撃者は10人から50人を想定し，DDoS攻撃全体の攻撃量は $100pps \sim 500pps$ で行われる。また，各攻撃者から送信されたパケットは同時に攻撃対象に届くものとする。攻撃者パケット中のIPv4ヘッダは容易に変更することができるため，攻撃パケットはIPv4ヘッダ中の送信元アドレスが改竄されているものとする。同様に，提案手法を含む各マーキング手法を掻い潜るため，識別子フィールド，ToSフィールドの初期値をランダムな値に設定し，さらにTTL値や距離値を調整しているものとする。

〈6・2・3〉 シミュレーション シミュレーションでは，EFMS, APPM, DPPM, ADMSのアルゴリズムをC言語を用いて実装した。表1にシミュレーションに用いた計算機の仕様を示す。また，シミュレーションは各パラメータにおいて100回ずつ行い，その平均値を結果として用いる。ここでは従来手法では攻撃対象，提案手法ではルータとトレーサが，それぞれ攻撃を検知した後の状況を想定して以下の実験を行った。そして攻撃対象はパケットを0.1秒間収集するごとに再構築処理を行い，全てのNARを再構築した時点でシミュレーションを終了する。

〈6・3〉 各マーキング手法のシミュレーションにおける前提条件

〈6・3・1〉 DPPMの前提条件 DPPMでは，TTL値を基にマーキング確率を変更する。このとき，各ルータにおけるマーキング確率は，$p = \frac{1}{c-TTL}$ (c：定数) となる。インターネット上の通信はそのほとんどが31ホップ以下であることから[24]，ここでは $c = 32$ とする。このとき，DPPM対応ルータはパケット中のTTL値が32以上のとき，パケットのTTL値を32に変更する。これによって，ネットワークの入り口で全てのルータをマーキングすることができるため，非常に効率の良いトレースバックが可能になる。しかし，攻撃者はパケット中のTTL値を容易に改竄することができるため，TTLの初期値を変更することでDPPMのパフォーマンスを下げることができる。インターネット上の通信距離は，17ホップを中心とした正規分布に近い形をとる[24]。そこで，ここでは攻撃者はTTLの初期値を21〜24にランダムに設定して攻撃を行うものとする。

〈6·3·2〉 APPMの前提条件 APPMでは，攻撃者からの距離値 d_1 をIPv4ヘッダ内のIP optionフィールドに追加することで，マーキング確率を調整する。この値はルータが転送を行うごとに1つ増加し，マーキングによって上書きされることはない。このとき，各ルータのマーキング確率は $p(d_1) = 1/d_1$ となる。しかし，攻撃者は攻撃パケット中のIPヘッダを容易に改竄できるため， d_1 の値を改竄することでAPPMのパフォーマンスを下げることができる。さらに，IP optionフィールドを用いた通信は，サーバの設定によって制限されることがあるため，エンドユーザとの協力が不可欠となる[25]。また，本手法は攻撃者とルータとの距離を利用している。そこで，ここではDPPMはAPPMを実用的な観点から発展させた手法と考え，APPMは評価せず，DPPMのみをシミュレーションでの比較に用いる。

〈6·3·3〉 ADMSの前提条件 ADMSでは，ルータは簡易な攻撃検知機能を持つ。ここでは，ルータが攻撃の特徴を検知する指標としてトラフィック量を用い，ルータに設定する閾値として $40pps$ を設定した。このとき，シミュレーションで用いたネットワークにおいて，平均して約半数の攻撃経路上のルータがADRになった。

〈6·4〉 攻撃検知時のマーキング確率の評価 本節では，基礎実験として p_{high} の値を評価する。p_{high} の値を0.1から1.0まで変化させ，各値において攻撃対象からADRまでの経路を全て再構築するのに必要なパケット数を比較した。図11より， $p_{high} = 0.5, 0.6$ の時に最も少ない観察量で再構築できたことがわかる。また，マーキング確率は低いほうがルータへの負荷が小さいと考えられるため，以降のシミュレーションでは， $p_{high} = 0.5$ を用いるものとする。

〈6·5〉 通常時のマーキング確率の評価 本節では，p_{low} の値について評価を行う。従来手法では，高い p_{low} の値はマーキング情報の上書きの要因となるため， p_{low} は低い値を使う必要があった。しかし提案手法では，マーキング中止命令を行うことで擬似的に攻撃経路の長さを短くすることができる。従って，従来手法より高い p_{low} の値が利用できると考えられる。p_{low} の値を0.04, 及び0.1から0.5まで変化させ，観察量を比較した。図12より，$p_{low} = 0.30$ のとき，最も低い観察量でトレースができた。そこで，以降のシミュレーションでは比較対象として従来手法と同じ $p_{low} = 0.04$ を用いた場合と， $p_{low} = 0.30$ を用いた場合について評価する。

〈6·6〉 観察量の評価 本節では， ADMSとEFMS, 及びDPPMに対して観察量の評価を行う。図13に，攻撃者数50におけるADMSとEFMSの観察量と攻撃経路再構築率の関係を示す。同図より，ADMSの方がEFMSと比べて，少ない観察量で多くの経路を再構築できていることがわかる。次に，ADMSとEFMS，及びDPPMに対して攻撃者数と観察量の関係を示す。図14はそれぞれ攻撃者数が $m = 10, 20, 30, 40, 50$ の場合の観察量を示している。

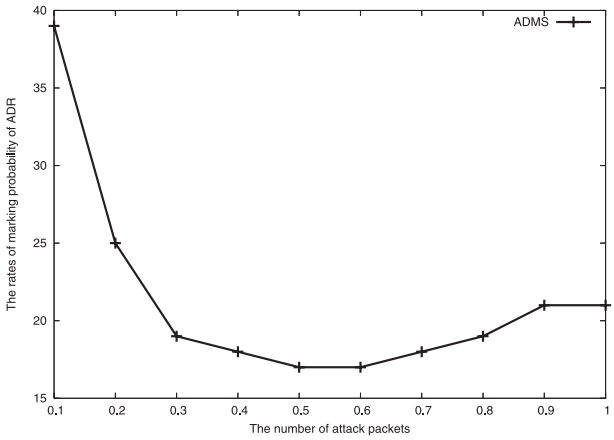


Fig. 11. The number of packets for attack path reconstruction until ADR.

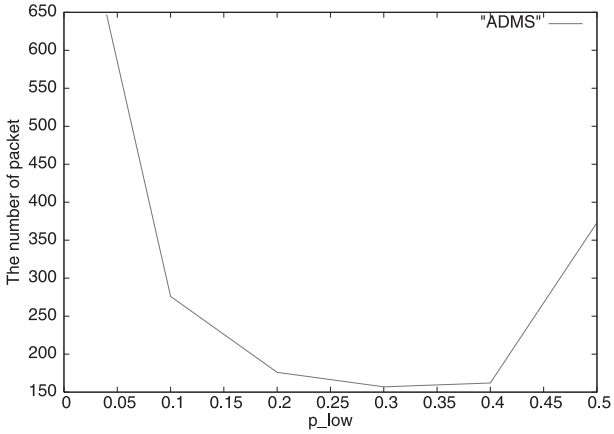


Fig. 12. The number of packets for attack path reconstrustion for p_{low}.

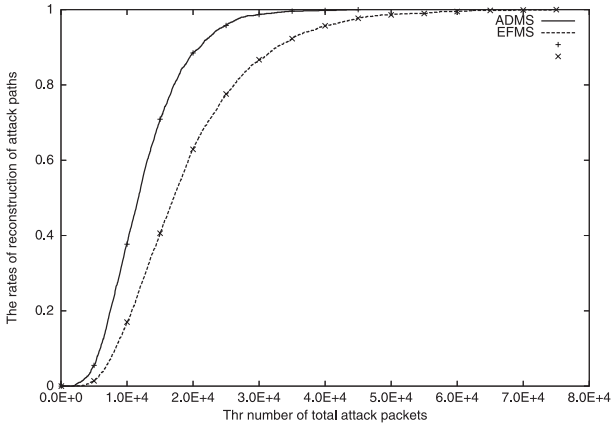


Fig. 13. Rates of attack path reconstruction.

いる。

このとき，攻撃者数に関わらず，全ての動的確率パケットマーキング手法がEFMSよりも少ない観察量でトレースバックを完了している。また，各手法で収集されたパケット中の非マーキングパケットの数を，図15に示す。同図より，攻撃パケット中のTTL値を改竄されている場合，ADMSはDPPMと比較して非マーキングパケット数がとても小

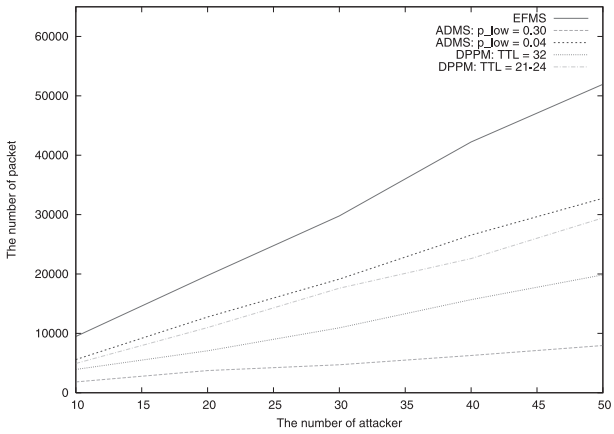


Fig. 14. The number of attack packets for attack path reconstruction.

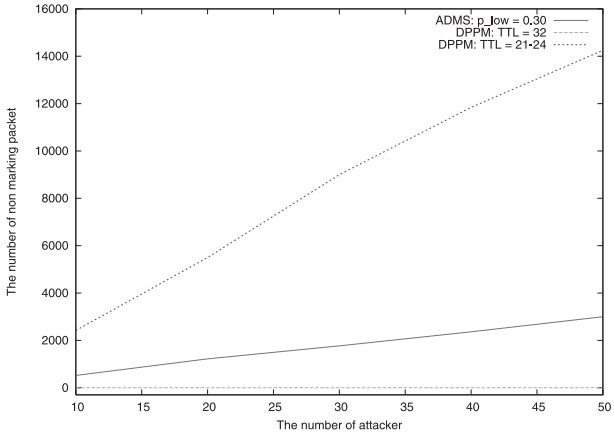


Fig. 15. The number of non-marking packet.

さいことがわかる。また，DPPM では，TTL 値を改竄した攻撃を受けると観察量が倍近くにまで増加している。次に ADMS は， p_{low} の値によって観察量が大きく変化している。特に，$p_{low} = 0.30$ のとき，攻撃者 50 人を特定するのに 7,950 パケットと他手法と比較して最も少ない観察量でトレースを完了している。

7. 考　察

本章では，ADMS のシミュレーションの結果に対する考察を行う。

〈7・1〉 攻撃検知手順におけるマーキング確率の変更が観察量に与える影響　本節では，ADR の p_{high} の値が観察量に及ぼす影響について検討する。

ADR を少ない観察量で再構築できれば，それだけ素早くマーキング中止処理を行うことが可能となる。そこで，ここでは攻撃経路上の全ての ADR を再構築するのに必要な観察量が最も少ないとき， p_{high} は最適であるとする。図 11 より，p_{high} の値が 0.5，及び 0.6 ，のとき ADR の再構築に必要なパケット数は最も少ないことがわかる。このとき，よりマーキング確率が低いほうがルータへの負担が小さいと考えられるので，シミュレーションに用いたネットワークにおいて， p_{high} の最適値は 0.5 であるといえる。

また，マーキング手法では確率的にマーキングが行われるため，p_{high} の値が小さいときは ADR からのマーキングパケットが十分に得られず，必要なパケット数が増加していると考えられる。また， p_{high} の 値が大きい場合について考える。このとき，攻撃対象に最も近い ADR の情報は即座に収集されるが，マーキング確率が高いと短い時間で収集するにも関わらずマーキングパケットの上書きが多く起こるため，収集されたパケットの数が増加していると考えられる。これらの結果から，攻撃トラフィック量が多くなる大規模な攻撃ほどより低い p_{high} の値が最適値となると考えられる。また，パケットの収集間隔やネットワークトポロジによって，マーキングが中止するまでに行われるマーキングの上書き量は変化すると考えられるので， p_{high} の最適値は一定ではないと考えられる。ただし，全ての ADR を特定するのに必要なパケット数は，p_{high} の値をチューニングしても最大で 20 パケット程度しか 変化していない。そのため，攻撃の規模が小さい場合は， p_{high} のパラメータチューニングが観察量に与える影響は小さいと考えられる。以上の結果から，特に規模の大きな攻撃において p_{high} の値を調整することは有効であると考えられる。また，ADR の再構築に必要なパケット数が少ないことから，マーキング確率が上昇している時間は非常に短く，ルータに与える影響はごく小さいものであると考えられる。

〈7・2〉 経路再構築時におけるマーキング確率の変更が観察量に与える影響　図 13 から，ADMS は EFMS と比べて早い段階から攻撃者の特定が可能になっていることがわかる。ここで，全ての ADR がマーキングを中止した後の攻撃経路上にある各ルータのマーキング確率を図 16 に示す。この図から，ADR にマーキング中止命令を行うことで攻撃経路ツリーの深さが浅くなっていることが分かる。例えば R(6) を経由する攻撃は，従来手法では 6 ホップの攻撃として認識されるが，提案手法では R(4) を根とする 3 ホップの攻撃として扱うことができる。このとき，攻撃対象までの距離が近いルータはさらに攻撃対象までの距離が縮まるため，特に早く特定することができると考えられる。特に，図 5 にみられるように，マーキング確率が高く，攻撃者が遠くにいるほどこの傾向は強くなる。このとき，$d > d_0$ となるルータ $R(d)$ によってマーキングされたパケットが下流のルータに上書きされずに攻撃対象に到達する確率は， $ADR(d_0)$ がマーキングを中止することで式 (2) より

$$\begin{aligned} Np(d-1) - Np(d) &= p(1-p)^{d-2} - p(1-p)^{d-1} \\ &= p^2(1-p)^{d-2} \quad \cdots\cdots\cdots (6) \end{aligned}$$

だけ高くなる。以上より，提案手法では ADR がマーキングを中止することで，効率的にパケットを収集していると考えられる。

〈7・3〉 非マーキングパケットの割合による計算量への影響　また，図 16 で示されるように，提案手法では，従来

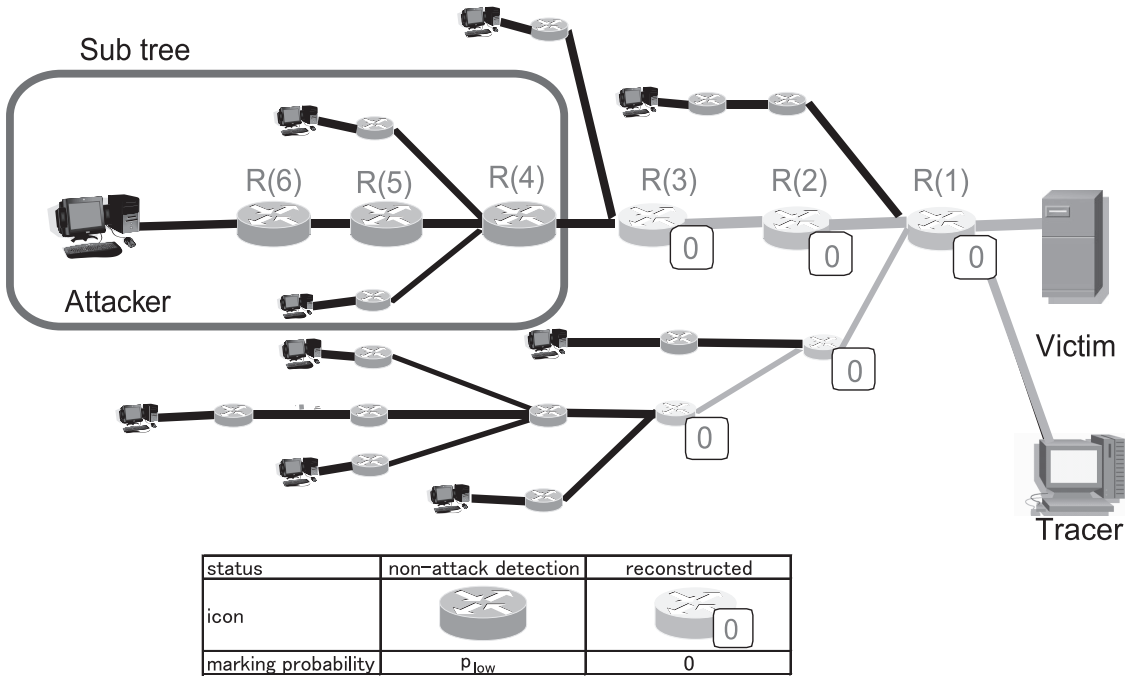


Fig. 16. Marking probability after decreasing procedure.

手法と比較して観察量に含まれる非マーキングパケットの数が少ない。非マーキングパケット数を n，距離 d にあるルータ数を r_d，フラグメント数を k とする。ここで，非マーキングパケットが持つ距離値がランダムであると仮定すると，計算量 E は $(r_d + \frac{n}{32 \times k})^k$ となる。攻撃規模が大きいとき，n は r_d よりも遥かに大きくなるため，計算量は $(\frac{n}{32 \times k})^k$ と近似できる。例えば，$ADMS(p_{low} = 0.3)$ と $DPPM(TTL = 21 - 24)$ の場合，攻撃者 50 人，$k = 4$ とすると，計算量は

$$\frac{E_{ADMS}}{E_{DPPM}} = \frac{(\frac{3000}{32 \times 4})^4}{(\frac{14250}{32 \times 4})^4} = 0.0019 \quad \cdots\cdots\cdots\cdots (7)$$

となり，ADMS は DPPM の 500 分の 1 の計算量でトレースをしている。攻撃規模が大きくなれば，この差はさらに大きくなると考えられる。このように，攻撃経路の再構築に必要な計算量は収集したパケット数が多くなると非常に大きくなるため，ADMS では再構築済みの ADR のマーキングを中止することによって，より素早く攻撃者の特定が可能であることがわかる。これらの結果から，提案手法が従来手法と比較して攻撃パケットの改竄に強く，高速なトレースバックが可能であることがわかった。

8. ま と め

本論文では，分散型サービス拒否（DDoS）攻撃の攻撃者を追跡する IP トレースバック技術の一つであるマーキング手法に関して，追跡の効率化を図る手法を提案した。従来のマーキング手法では攻撃者を特定するのに必要なパケット量が膨大になるという問題がある。そこで，要因となる下流のルータによるマーキング情報の上書きに注目し，トラフィック監視による攻撃の検知と，動的なマーキング確率の変化によって問題の解決を図った。その結果，マーキング確率の制御によって経路再構築に必要なパケット量を大きく減らすことができることを示した。今後の課題として，マーキング確率を下げる際の通信遅延による影響や，攻撃対象がパケットを収集する時間などを検証する予定である。

謝　辞

本研究の一部は科学研究費補助金 (20500069) の助成を受けたものである。

（平成 20 年 5 月 10 日受付，平成 20 年 10 月 3 日再受付）

文　献

（1） H. Burch and B. Cheswick: “Tracing Anonymous Packets to Their Approximate Source”, Proc.2000 USENIX LISA Conf., pp.319-327 (2000-12)

（2） D. Moore, G. Voelker, and S. Savage: “Inferring Internet Denial-of-Service Activity”, Proc.of the 2001 USENIX Security Symposium (2001-5)

（3） Y. Kadobayashi, and M. Oe: “IP Traceback Techniques”, IPSJ Magazine, Vol.42, No.12, pp.1175-1180 (2001-12) (in Japanese)
門林雄基・大江将史：「IP トレースバック技術」，IPSJ Magazine, Vol.42, No.12, pp.1175-1180 (2001-12)

（4） R. Stone: “CenterTrack : An IP Overlay Network for Tracking DoS Floods”, 9th USENIX Security Symposium (2000)

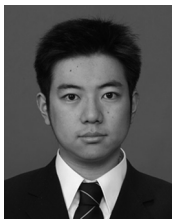
（5） Bellovin, S. M and Leech, M. D: “ICMP Traceback Messages”, Internet Draft, draft-ietf-itrace-00.txt (2000)

（6） A. C. Snoeren, C. Partridge, L. A. Sanches, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Stayer: “Hash based IP Traceback”, Proc.SIGCOMM ’01, San Diego, USA (2001-8)

（7） H. Harima, M. Ito, H. Suzuki, N. Okazaki, and A. Watanabe: “Proposal and Its Implementation of L2-based IP Trace Back Method”, IPSJ Journal, Vol.49, No.6, pp.1234-1245 (2008-1) (in Japanese)
播磨宏和・伊藤将志・鈴木秀和・岡崎直宣・渡邊　晃：「L2-based IP トレースバック方式の提案と実装」，情処学論，Vol.49, No.6,

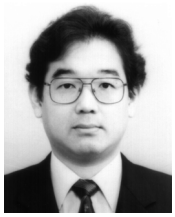
pp.1234-1245 (2008-1)
（8） R. T. Morris: “A Weakness in the 4.2BSD UNIX TCP/IP Software”, Bell Labs Computing Science Technical Reports #117 (1985)
（9） “Smurf: IP Denial-of-Service Attacks”, CERT Advisory CA-98.01 (1998-1)
（10） “IP Denial-of-Service Attacks”, CERT Advisory CA-97.28 (1997-12)
（11） “TCP SYN Flooding and IP Spoofing Attacks”, CERT Advisory CA-1996-21 (1996-9)
（12） S. Staniford-Chen and L. T. Helberlein: “Holding intruders accountable on the internet”, Proceedings of the 1995 IEEE Symposium on Security and Privacy, Oakland, CA, pp.39-49 (1995-5)
（13） Y. Zhang and V. Paxson: “Detecting stepping stones”, In Proceedings of 9th USENIX Security Symposium (2000-8)
（14） S. Savage, D. Wetherall, A. Karlin, and T. Anderson: “Practical Network Support for IP Traceback”, Proc. SIGCOMM ’00, pp.295-306 (2000)
（15） D. Song and A. Perrig: “Advanced and Authenticated Marking Schemes for IP Traceback”, IEEE INFOCOMM’ (2001)
（16） A. Yaar, A. Perrg, and D. Song: “FIT：Fast Internet traceback”, IEEE INFOCOM 2005 13-17 March, Vol.2, pp.1395-1406 (2005-3)
（17） T. Peng, C. Leckie, and K. Ramamohanarao: “Adjusted Probabilistic Packet Marking for IP Traceback”, NETWORKING ’02: Proceedings of the Second International IFIP-TC6, Vol.2345, pp.697-708 (2002)
（18） J. Liu, Z. Lee, and Y. Chung: “Dynamic probabilistic packet marking for efficient IP traceback”, Computer Networks, Vol.51, pp.866-882 (2007-2)
（19） R. Hiyoshi: Practical Guide to Intrusion Detection Systems, Gijutsu-Hyohron Co, Japan (2004-4) (in Japanese)
日吉 龍：「IDS 入門」, 技術評論社 (2004-4)
（20） D. Towsley and L. Gao: “The Monitoring and Early Detection of Internet Worms, ” IEEE/ACM TRANSACTION ON NETWORKING, Vol.13, No.5, OCTOBER
（21） J. Case, “A Simple Network Management Protocol (SNMP)”, RFC1157 (1990)
（22） Philip Miller・苅田幸雄：「マスタリング TCP/IP 応用編」, pp.88-93 (1998)
（23） OCN ネットワーク構成. http://www.ocn.ne.jp/business/info/pdf/ipbackborn_080521.pdf
（24） W. theilmann and K. Rothermel: “Dynamic Distance Maps of the Internet”, In Proceeding of the 2000 IEEE INFOCOM Conference (2000)
（25） 松木隆宏･松岡正明･寺田真敏：「IP マーキングによる不正活動ホストの広報機能の開発」, IPSJ-SIG Technical Reports 2008-CSEC-42, pp.323-328 (2008-7)
（26） K. Koga, N. Okazaki: “A proposal of an extended method of IP trace-back for distributed denial of service attacks”, IS-07-15, pp.31-36, (2007-4) (in Japanese)
古賀勝寛・岡崎直宣：「分散 DoS 攻撃追跡手法の効率化に関する検討」, 電学研資, IS-07-15, pp.31-36 (2007-4)

古 賀 勝 寛



（非会員） 2007 年宮崎大学工学部情報システム工学科卒業。現在，同大学院工学研究科情報システム工学専攻修士課程在学中。ネットワークセキュリティに関する研究に従事。

岡 崎 直 宣



（正員） 1986 年東北大学工学部通信工学科卒業。1991 年東北大学大学院工学研究科電気及び通信工学専攻博士後期課程了。同年，三菱電機（株）入社。2002 年より宮崎大学工学部助教授。2007 年同准教授。通信プロトコル設計，ネットワーク管理，ネットワークセキュリティ，モバイルネットワーク等の研究に従事。博士（工学）。電子情報通信学会，情報処理学会，IEEE 各会員。

渡 邊 晃

（非会員） 1974 年慶応義塾大学工学部電気工科学科卒業。1976 年同大学大学院工学研究科修士課程修了。同年三菱電機（株）入社後，LAN システムの開発・設計に従事。1991 年同社情報技術総合研究所に移籍し，ルータ，ネットワークセキュリティ等の研究に従事。2002 年名城大学理工学部教授，現在に至る。博士（工学）。電子情報通信学会，情報処理学会，IEEE 各会員。

朴 美 娘

（非会員） 1983 年漢陽大学工学部電子工学科卒業。同年，漢陽大学工学部助手。1993 年東北大学大学院工学研究科情報工学専攻博士後期課程修了。同年，東北大学電気通信研究所助手。1994 年三菱電機（株）入社。現在，同社情報技術総合研究所勤務。通信プロトコル設計，ネットワークセキュリティ等の研究に従事。博士（工学）。♪電子情報通信学会，情報処理学会各会員。