DDoS 攻撃に対する高性能発信源探査方式の提案

甲斐 俊文*　　中谷 浩茂*　　清水 弘*　　塚本 克治**

Efficient Traceback Method for Detecting DDoS

Toshifumi KAI*　Hiroshige NAKATANI*　Hiroshi SHIMIZU*　Katsuji TSUKAMOTO**

あらまし インターネットの普及に伴って、不正アクセスによる被害が増加傾向にある。特に、送信元アドレスを偽装した DoS (Denial of Service) 攻撃や DDoS (Distributed DoS) 攻撃は、システムを停止に追いやることもあり、社会生活への影響が出始めている。その対策のために、幾つかの発信源探査技術が提案されている。本稿では、既存方式の問題点を解決したハイブリッド方式を提案する。また、提案する新方式の有効性を示すために、探査性能および導入（実装）の容易さから評価し、既存技術との比較を行う。探査性能については数学モデルとシミュレーションにより評価する。

Abstract　The amount of damage by illegal access is increasing with the spread of the Internet. Especially the DoS (Denial of Service) and DDoS (Distributed DoS) attacks cause system down and often influence social life. The attacker detection technologies have been proposed until now. We evaluate them to show their properties from the point of view of performance and easiness of implementation. And we propose hybrid traceback method that solves the disadvantages of existing technologies. Advantages of our new technology to the existing methods clarified by simulation.

1. はじめに

ネットワークが社会的インフラとして定着した今日、これを用いたサービスの提供は当然のものと認識されている。一方で、それを停止させようとする妨害も増加の一途を辿っている。このような「攻撃」と呼ばれる妨害行為の代表的なものに DoS (Denial of Service) 攻撃や DDoS (Distributed DoS) 攻撃がある。これらの攻撃は一般的に送信元 IP アドレスを偽装したパケットを用いていることが多く、被害者側には真の発信源が特定できないため、対策が困難なものとなっている。

今までに図 1に示すようなトレースバックと呼ばれる、不正パケットの発信源探査を行う方式が多数提案されているが、それぞれに一長一短があり、どれも絶対的な手法とは言えない[1][2][3][4]。また、複数の方式の単純な併用または組合せを行ったとしても、実用的なものにはならない。しかし我々は、お互いの方式の長所を生かしつつ短所を補完し合うような組合せ方が考案できれば有効な方式の実現に繋がる可能性があると考え、これを今回の新方式の研究開発の基本方針とした[5][6]。

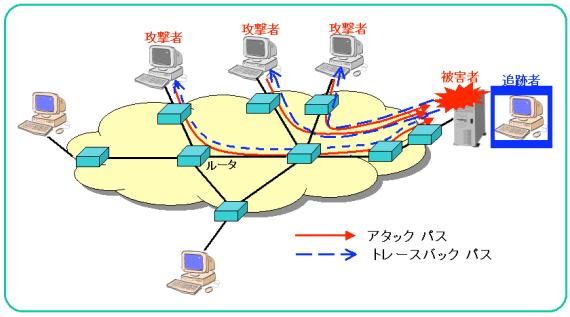

図 1　トレースバック

* 松下電工株式会社　システム技術研究所
Matsusita Electric Works, Ltd.　Systems Technology Research Laboratory
** 工学院大学　情報工学科
Kogakuin University　Dept. of Computer Engineering

本稿ではまず、既存トレースバックの中でも最も有効と言われる３つの方式（ICMP 方式、マーキング方式、Hash 方式）に着目して評価を行うことで、各方式の特性を明らかにする。次に、これらの持つ問題点を解決する最適な組合せの候補とその方法を考え出し、それを新方式（ハイブリッド方式）として提案する。さらに、探査時間に対する成功率、および実ネットワークへの導入の容易さという２つの視点から既存方式との比較を行い、新方式の優位性を示す。

なお、本研究で想定したネットワークはインターネット全体ではなく、プロバイダネット、イントラネット、行政ネットなど単一のポリシーによって管理されたネットワーク（AS：Autonomous System）である。我々は今回評価した既存方式や提案した新方式を AS 内トレースバックと分類し、複数 AS 内での探査を連携させるための AS 間トレースバックについても並行して研究中である[7]。

2. 既存方式

IP トレースバック技術の代表的な３つの既存方式とそれぞれの実装例を表 1に示す。

表 1　既存のトレースバック方式

方式名	実装例
ICMP 方式	iTrace **iTrace-II ※**
マーキング方式	FMS AMS **AMS-II ※**
Hash 方式	Paffi **SPIE ※**

いずれの方式も全てのルータ上（または外付け）の探査情報取得用モジュールと、各モジュールから集めた探査情報を元にパケットの通過した経路を構築する探査端末から成る。

本章では各方式の中から※印で示した代表的な実装例を取り上げ、概要（仕組み）と特徴について述べる。また、2.4 節に既存方式の問題点をまとめる。

2.1　ICMP 方式

(1) 方式概要

ICMP 方式の動作概要を図 2に示す。

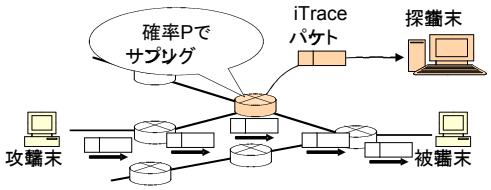

図 2　ICMP 方式の動作

ICMP 方式では、確率的にサンプリングしたパケットの探査情報を探査端末に送るために、iTrace パケットと呼ばれる特別な ICMP パケットを生成する。

ここでは ICMP 方式の具体的な実装方式として iTrace-II について説明する。iTrace-II は IETF(Internet Engineering Task Force)で標準化の検討をされていた iTrace[1]に我々が独自に改良を加えたものである。

iTrace-II の動作手順を表 2に示す。iTrace では一つのサンプリングパケットにつき一つの iTrace パケットを生成するが、iTrace-II では複数のサンプリングパケットを一つの iTrace パケットにまとめて送ることで、ネットワーク負荷を上昇させずに、サンプリングレートを上げることができる。

表 2　iTrace-II の動作

ルータ上のモジュールの動作
(i) フォワーディングされるパケットを無作為に確率 P でサンプリングする
(ii) サンプリングしたパケットについて、以下の情報を iTrace パケットに書き込む ・ IP ヘッダ＋ペイロード数バイト ・ 一つ前のルータ＋自ルータ＋一つ先のルータの IP アドレス ・ サンプリング時刻など
(iii) 書きこまれたサンプリングパケットが定数 L 個以上になったら発信源探査端末宛に iTrace パケットを送信する
(iv) (i)から繰返す(探査時用の特別な動作はない)

攻撃パケットの探査情報が含まれた iTrace パケットを、攻撃端末から被害端末までの全ルータから経路確定閾値以上得られれば、探査成功となる。経路確定閾値とは、探査精度を上げるために集めるべき探査情報の量であり、方式によって定義が異なる。

(2) 特徴

iTrace パケットがネットワークに掛ける負荷を考慮してサンプリング確率は低く設定し

なければならない。このため探査可能な攻撃は、DoS 攻撃のように一台の攻撃端末が送信するパケット数が大量になるものに限られる。

2.2 マーキング方式

(1) 方式概要

マーキング方式の動作概要を図 3に示す。ICMP 方式との大きな違いは、特別に探査用のパケットを生成せず、サンプリングしたパケットに探査情報を書き込む点である。

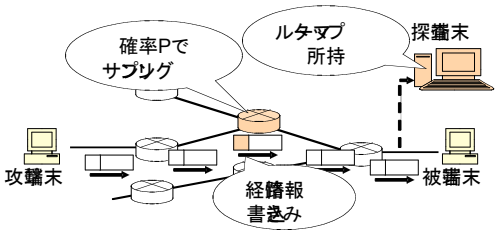

図 3 マーキング方式の動作

代表的な実装例として AMS-II[3]を取り上げる。その動作を表 3に示す。AMS-II では発信源探査端末（ルータマップ所有）に、攻撃経路上の全ルータからハッシュ値（フラグメントを集めて再生したもの）が全て経路確定閾値以上集まれば探査成功となる。

表 3 AMS-II の動作

ルータ上のモジュールの動作
(i) フォワーディングされるパケットを無作為に確率 P でサンプリングする
(ii) 自身の IP アドレスから 64bit のハッシュ値を計算し、それを 8bit 単位で 8 分割（フラグメント）し、そのいずれかを、ランダムにサンプリングしたパケットの ID フィールド(16bit)に書き込む
(iii) ID フィールドの残り 8bit にフラグメント番号（0～7）と被害端末からのホップ数の値を書き込む （そしてサンプリングパケットを送信）
(iv) (i)から繰返す(探査時用の特別な動作はない)

(2) 特徴

探査用にパケットを生成しないためサンプリングレートを高く設定可能であり、DDoS 攻撃のように攻撃端末一台あたりの送信パケット量が少ない攻撃でも探査可能である。

しかし、発信源探査端末が常に正確なルータマップを持っていなければならない点と、IP ヘッダの ID フィールドを書き換えてしまうため IP パケットのフラグメントが発生する環境には適応できないという点で、現実のネットワークに導入する際の障壁が高い。

2.3 Hash 方式

(1) 方式概要

Hash 方式は前出の２つの方式とは異なり、発信源探査端末から各ルータに対して能動的に問合せを行なうトレースバック方式である。動作概要を図 4に示す。

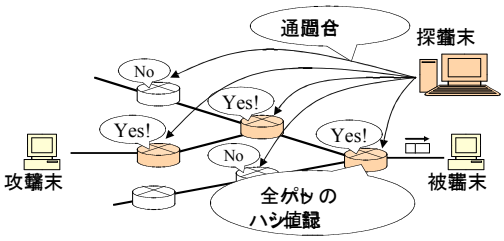

図 4 Hash 方式の動作

また、この方式の代表的な実装例である SPIE[4]の動作を表 4に示した。

表 4 SPIE の動作

ルータ上のモジュールの動作
＜通常時＞
(i) フォワーディングされるパケットのハッシュ値を計算する（全パケット対象）
(ii) メモリ上のハッシュ値番地にフラグを立てる
(iii) (i)から繰返す
＜問合せを受けた時＞
(i) 探査対象パケットのハッシュ値を算出する
(ii) メモリ上のフラグをチェックする
(iii) フラグに従って通過の有無を返信する
発信源探査端末の動作
＜IDS や管理者から探査要求を受けた時＞
(i) 探査するパケットについて被害端末最寄りのルータに問合せる
(ii) 通過が確認されたルータの隣接ルータに順次問合せする
(iii) (ii)を繰返す

(2) 特徴

Hash 方式は、１パケット単位での探査を目的としたものである。ルータが全てのパケットについてハッシュ値を記録しておくことでこれを可能にしている。ただし一つの攻撃パケットにつき数十回の問合せが発生し、ルータに処理負荷をかけるため、DoS 攻撃や DDoS 攻撃の探査には向かない。また、ハッ

シュ値を保存しておくためにルータにはある程度大きなメモリが必要になる。

2.4 既存方式の問題点

既存方式の評価に際して、探査可能な攻撃パケット流量の範囲と実ネットワークへ導入する際の問題点を表 5にまとめた。

表 5 既存方式の比較

方式		ICMP	マキング	Hash
追跡可能なパケット流量	大量(DoS)	○	○	×
	少量(DDoS)	×	○	×
	単発	×	×	○
導入問題		ほぼ問題なし	要ルータのファームウェア変更	コスト(必要メモリ量や未定)

ICMP 方式は、探査用のパケットがネットワークに負荷をかけないよう、サンプリングレートを低くしなければならない。そのため、大量の攻撃パケットが送信される攻撃しか探査できない。マーキング方式は探査によるパケットの増加がないため、ICMP 方式に比べてサンプリングレートを高く設定でき、DDoS 攻撃のように一台の攻撃端末からのパケット流量が少ない場合でも高速に探査できる。しかし、前述したように実ネットワークへの導入は難しいと考えられる。Hash 方式は１パケット毎に正確な探査が可能であるが、問合せによる負荷の問題でDoS攻撃やDDoS攻撃の探査には向かない。このため、既存方式単独ではもちろんだが、２つ以上の方式を単純に組み合わせても、多様な攻撃を探査可能かつ実ネットワークへの導入が容易なシステムは実現できない。

3. 考案した新方式（ハイブリッド方式）

２章で述べた既存方式の問題点を解決するため、我々は実ネットワークへの導入が容易で、かつマーキング方式（AMS-II）並みの探査性能を持つハイブリッド方式を考案した。

3.1 構成

ハイブリッド方式はICMP 方式と Hash 方式の技術の組合せにより実現する。

各ルータにはiTrace-II と SPIE のモジュールが実装される。ただし、ルータ内で双方のモジュールが干渉し合うことはない。また、特に既存のモジュールからの機能変更もない。

探査端末側もiTrace-II受信機能と SPIE 問合せ機能を持つ。攻撃を探査時は双方が連携して経路情報を収集し、攻撃経路を構築する。

3.2 動作説明

ルータ側では、iTrace と SPIE の両方の動作を行う。つまり表 2と表 4にあるように、通常時には確率的に通過パケットをサンプリングしてiTrace パケット生成を行い、同時に全ての通過パケットの Hash 値をメモリ上に記録する。探査端末からの SPIE 問合せの際には、通過の有無を確認して結果を返す。

探査端末は、攻撃が発生し IDS もしくはネットワーク管理者から探査要求を受け取ると、下記の手順で探査を行う。

（ステップ１）iTrace パケットの受信

受信したiTraceパケットに含まれているサンプリングパケットが、探査対象の攻撃に該当すれば、ステップ２を実行する。

（ステップ２）SPIE 問合せ

該当したサンプリングパケットについて、表 4と同様の手順で SPIE による経路探査を行う。ただし被害端末の最寄りのルータではなく、iTrace パケットを送信してきたルータに最初の問合せを行う。

（ステップ３）経路の記録

SPIE による探査が完了したら、発見した攻撃経路を記録し、再びiTrace パケットが届くのを待つ。

図 5に動作イメージを示す。A が攻撃端末、V が被害端末、P1 が攻撃パケットである。SPIE 問合せは①から③の順に行われている。この例では R2 が iTrace パケットを送信したのをきっかけに SPIE による探査が行われ、R9-R5-R2-R1 という攻撃経路が明らかになることを示している。

このようにハイブリッド方式ではiTraceパケットをトリガーにして SPIE による探査を行うため、攻撃経路上のルータのどれか一台

が攻撃パケットをサンプリングすれば経路を発見できる。経路上の全てのルータでサンプリングされるまで経路を構築できない iTrace-II と比べると、少ないパケット数の攻撃まで探査可能である。また、SPIE 問合せの回数は、攻撃パケットをサンプリングした iTrace パケット数に比例する。このため、攻撃パケット全てについて SPIE 問合せを行う場合よりも少ない問合せ回数で済む。

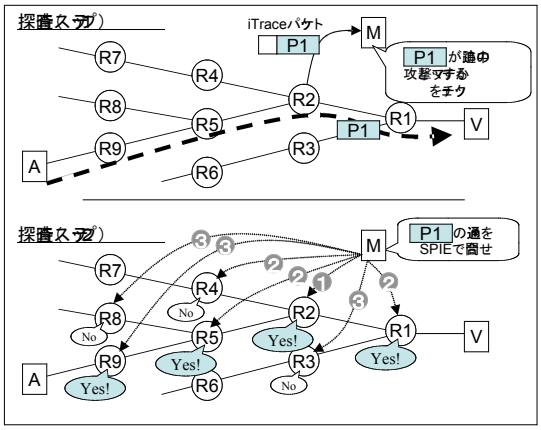

図 5　ハイブリッド方式の動作

4. 性能評価

考案したハイブリッド方式の優位性を確認するために、発信源探査時間と探査精度の関係および探査のために生成されるパケット数の２点から各方式を評価する。

4.1　評価モデル

定量的に各トレースバック方式の性能を比較するために、表 6の評価モデルを用いた。以下、各項目について説明する。

表 6　トレースバック方式評価モデル

分類	項目	内容
定義	発信源探査	・全経路探査（攻撃者→被害者）
前提	環境条件	・理想的 IDS ・理想的ネットワーク ・理想的ハッシュ（衝突無し） ・通常トラフィック大
パラメータ	攻撃	・攻撃パケット流量 （packets/sec）
	ネットワーク	・ツリー分岐数 ・ホップ数（攻撃者→被害者）

4.1.1　発信源探査

コンピュータフォレンジックの観点から、発信源探査は、攻撃端末（攻撃者）に加え、攻撃パケットが通過した経路も併せて突き止めることが望ましい。このため本稿では、攻撃端末と攻撃パケット通過経路（攻撃端末→被害端末（被害者））の両方を見つけ出すことを発信源探査と定義した。

また、攻撃を行なっていない端末を攻撃端末と誤認知する確率を減らすために、経路確定閾値というものを設定する。この閾値を超える量の探査情報が集まらない限り、経路探査ができたとは判定しないこととする。

4.1.2　環境条件

理想的な IDS（Intrusion Detection System）と理想的なネットワークを用いた環境を前提とする。ここで理想的な IDS とは攻撃パケットと非攻撃パケットの正確な切り分けと、攻撃発生と同時のアラート生成ができるものであり、理想的なネットワークとは通信遅延・輻輳・パケットロスが発生しないものである。

Hash 方式とマーキング方式で使用するハッシュ値も衝突が無いものとする。

また、通常トラフィックの流量は iTrace-II やハイブリッド方式においてサンプリングしたパケットが探査端末に送られる遅延時間を無視できる程度に大きいものとする。

4.1.3　攻撃

本稿で評価した各方式では、パケットの中身やサイズが動作に影響を与えることはない。よって攻撃パケットについて変化させるパラメータは、流量(packets/sec)のみとする。

なお、攻撃の形態は攻撃端末が複数あるもの（DDoS）とし、攻撃端末数は経路の分岐数とホップ数によって一意に決まるようにする。

4.1.4　ネットワーク

ネットワークがループを含んでいても、攻撃経路は直線状もしくはターゲットホストを根としたツリー状になる。今回は評価をシンプルにするために、攻撃経路を S 分木として扱うことにした。パラメータはツリー分岐数 S と攻撃端末と被害端末間のホップ数である。

4.2　数学モデル

数学モデルを扱うにあたって、各方式共通に用いる値と記号を表 7にまとめた。また、

二項分布関数として *fb*(成功数,試行回数,成功率)を用いる。

表 7　数学モデルに用いる記号一覧

パラメータ	記号	単位
サンプリングレート	P	－
経路確定閾値	B※	個
攻撃端末１台当りの攻撃パケット流量	A	packets/sec
探査時間	T	Sec
ホップ数	H	Hops
ツリーの分岐数	S	－
ルータ総数	R	台
探査成功率	Q	－

※方式によって定義が異なる

4.2.1　既存方式の数学モデル

２章で説明した３つの既存方式について、発信源探査時間と探査精度の関係を表す式を以下に示す。式１は iTrace-II、式２は AMS-II、式３は SPIE の式である。評価モデル上では SPIE の経路探査は必ず成功する。

$$Q = \prod_{d=0}^{H-1}(1-\sum_{k=0}^{B-1} fb(k, ATS^d, P)) \quad (式１)$$

$$Q = \prod_{d=0}^{H-1}(1-\sum_{k=0}^{B-1} fb(k, ATS^d, (1-P)^d P/8))^8 \quad (式２)$$

$$Q = 1 \quad (式３)$$

ネットワーク全体の iTrace-II のパケット増加数を式４に示す。１台のルータを通過するパケット数が N で、１つの iTrace に L 個のサンプリングパケットを入れるものとする。

$$RPN/L \quad (式４)$$

AMS-II では探査用のパケット増加はない。

SPIE の問合せ回数は、式５のようになる。$AT*S^H$ は全攻撃パケット数、HS は一回の探査で問合せるルータの数である。

$$AT*S^H*HS \quad (式５)$$

4.2.2　ハイブリッド方式の数学モデル

ハイブリッド方式では攻撃経路上のルータのどれか一つが iTrace パケットを送信すれば、後は SPIE を使って全経路を明らかにできる。よって、探査成功率は式６で表され、攻撃端末数やネットワークトポロジには依存しない。

$$Q = 1-\sum_{k=0}^{B-1} fb(k, ATH, P) \quad (式６)$$

攻撃パケット数 $AT*S^H$ 個に対する問合せの回数の期待値は式７で表される。これは式２に攻撃パケットが経由するルータ数 H とサンプリングレート P を掛けたものである。

$$AT*S^H*H^2SP \quad (式７)$$

4.3　シミュレーションモデル

数学モデルの妥当性確認するために、各探査方式のシミュレータを C++で作成した。以下に各方式共通のアルゴリズムを示す。

（ステップ１）初期化

S 分木 H ホップのルータネットワーク構造を生成し、各ルータの持つ属性変数である検出数 F を０に初期化する。攻撃パケット数αも０に初期化する。

（ステップ２）攻撃パケットに対するトレースバック処理

```
α=α+1
for each 攻撃端末 do
  for each 経由ルータ do
    探査処理を実行（注：探査方式依存）
     （if ルータ検出条件をクリア then
      ルータの属性変数 F=F+1）
    endif
  done
done
```

（ステップ３）攻撃端末発見のチェック

```
for each 攻撃端末 do
  if 既に攻撃端末は発見済み then
    continue
  endif
  if 全ての経由ルータ検出数 F ＞
       経路確定閾値 B then
    攻撃端末に発見済みフラグを立てる
    発見時パケット数リスト L にαを
     追加
  endif
done
if 未発見攻撃端末が存在 then
  ステップ２に戻る
endif
```

このステップ１～３を実行することで一試行が完了する。指定した試行回数分繰り返すと、最終的に発見時パケット数リスト L に（試行回数）×（一試行の攻撃端末数）分の値を

得ることができる。攻撃端末発見時のパケット数を攻撃速度 A で割ることで、各攻撃端末の探査時間が求められる。したがって、このシミュレーションの結果から、探査時間と探査成功率を求めることができる。

また以下に（ステップ２）におけるハイブリッド方式の探査処理アルゴリズムを示す。攻撃パケットがサンプリングされると、SPIE によって経由した全ルータが発見されるため、各ルータの検出数 F を１増加させている。

（ハイブリッド方式の探査処理）

```
if 確率 P でサンプリング then
  for each 経由ルータ do
    ルータの属性変数 F=F+1
  done
endif
```

4.4 シミュレーション結果

iTrace-II、AMS-II、ハイブリッド方式について、探査時間と成功率の関係を数学モデルとシミュレーションの両方で比較した。パラメータとしてホップ数 H=10、攻撃端末１台当りの攻撃パケット流量 A=10[packets/sec]、経路確定閾値 B=2 を与えた。サンプリングレート P は iTrace-II とハイブリッド方式で 1/4000、 AMS-II で 1/20 とした。また、攻撃経路の分岐数 S=1 と S=2 についてそれぞれ解析した。攻撃端末数は S=1 の場合は１台（DoS 攻撃など）、S=2 の場合は H=10 であるため、1024 台（DDoS 攻撃）である。

数学モデルに基づいて算出した結果を図 6、シミュレーションの結果を図 7に示す。シミュレーションでの試行回数が少ない場合は数学モデル（理論値）と一致しないが、ある程度の回数を重ねると理論値に収束する。

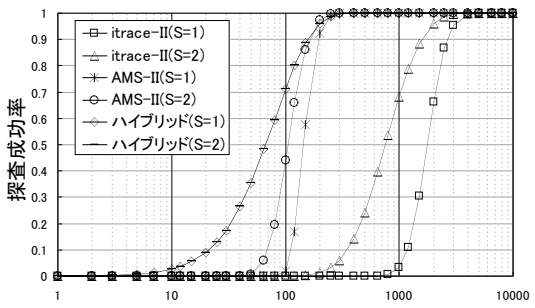

図 6 探査時間と成功率の関係（数学モデル）

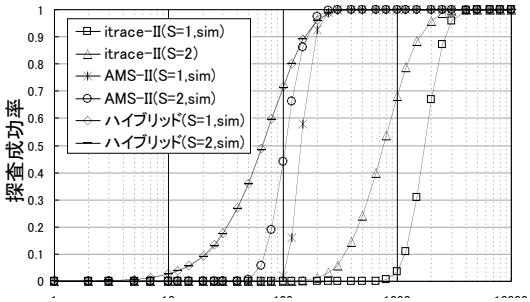

図 7 探査時間と成功率の関係（シミュレーション）

図 7は、S=1 の時、試行回数 20000 回（延べ攻撃端末数 20000 台）、S=2 の時、試行回数 20 回（延べ攻撃端末数 20480 台）の条件によるシミュレーション結果であり、数学モデルによる結果とほぼ完全に一致している。これにより数学モデルの妥当性が確認できた。

4.5 性能比較

(1)探査速度

前節と同じ条件で、成功率が 95%以上になる探査時間を図 8に示す。この条件下では AMS-II とハイブリッド方式はほぼ同等の性能であり、iTrace-II よりも約 10～15 倍の速度で攻撃端末を発見できることが分かる。

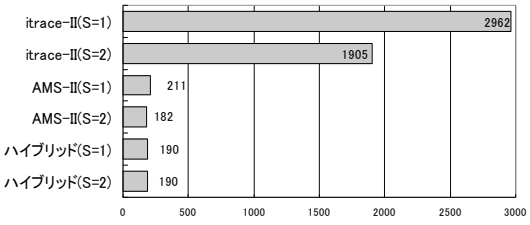

図 8 成功率が 95%になる探査時間

(2)パケット増加数

1 秒間にトレースバックシステムが生成するパケット数を計算した結果を表 8に示す。

前項の条件に加え、ルータの台数 R=1000、各ルータがフォワードするパケット数 N=10000（ノーマルパケットも含む）、1 つの iTrace パケットに含まれるサンプリングパケット数 L=5 とした。攻撃端末１台当りの攻撃パケット流量は 10packets/sec であるから、S=2 の場合は、総攻撃パケット流量が 10240 packets/sec の DDoS 攻撃となる。

この結果から問合せ数の増加の問題で、総パケット流量が大きい攻撃には SPIE が適していないことが分かる。ハイブリッド方式ではSPIE単体のH*P倍(ここでは10*(1/4000))という少ない問合せ数で済む。しかも SPIE では、DDoS 攻撃の際に攻撃パケットが集中する被害端末に近いルータにも問合せが大量に発生し、負荷が大きくなる。一方、ハイブリッド方式はiTraceパケットを送信してきたルータから問合せを開始でき、すでに探査済みであれば被害端末に近い方のルータへの問合せは省くことができる。このため被害端末に近いルータには小さな負荷しかかからない。

表 8 発信源探査によるパケット増加数

S=1 (攻撃端末 1 台)	iTrace パケット数	SPIE 問合せ数
iTrace-II	500	0
AMS-II	0	0
SPIE	0	100
ハイブリッド	500	0.25
S=2 (攻撃端末 1024 台)	iTrace パケット数	SPIE 問合せ数
iTrace-II	500	0
AMS-II	0	0
SPIE	0	204800
ハイブリッド	500	512

4.6 既存方式に対する新方式の優位性

前節で述べたように、探査速度についてはハイブリッド方式と AMS-II は同等の性能である。このことは、ハイブリッド方式でもAMS-II と同様に､攻撃端末一台当たりのパケット流量が小さい DDoS 攻撃でも高速に探査可能であることを意味する。また、ハイブリッド方式はSPIEの技術を内包しているため、攻撃の種類によって使い分けることで、単発パケット攻撃も探査できる｡したがって､表 9 に示すように、ハイブリッド方式は様々なパケット流量の攻撃を探査可能である。

表 9 既存方式とハイブリッド方式の比較

方式		ICMP	マキヅ	Hash	ハイブリッド
追跡可能なパケット流量	大量(DoS)	○	○	×	○
	少量(DDoS)	×	○	×	○
	単発	×	×	○	○
導入問題		ほぼ問題なし	要ルータマップ／ヘダ改	コスト(必要メモリ量や未)	コスト(必要メモリ量や未)

ハイブリッド方式の導入時の問題は SPIE と同様であり、発信源探査システムの投資対効果が高ければクリアできる。

5. おわりに

トレースバックの代表的な既存方式の評価を行い、その結果を基にハイブリッド方式を考案し、既存方式との比較を行った。今後、ルータ数十台規模のネットワーク環境での実機試験による評価も行う予定である[8]。

また、複数 AS 内での探査を連携させるための AS 間トレースバックについても並行して研究中である。

(注)本研究は独立行政法人 情報通信研究機構からの委託(H14～H16 年度)による。

参考文献

[1]Steven M. Bellovin, "ICMP Traceback Message",InternetDraft:draft-bellovin-itrace-00.txt, submitted Mar. 2000,

[2] S. Savege, D. Wtherall, A. Karlin, T. Anderson, "Practical Network Support for IP Traceback", Proceedings of Sigcomm 2000, Aug 2000, Stockholm, Sweden,

[3] D. Song and A. Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback,” Proc. IEEE INFO-COM, April 2001.

[4] Snoeren AC, Partridge C, Sanchez LA, Jones CE, Tchakountio F, Kent ST, Strayer T, "Hash-Based IP Traceback", Proc. of the ACM SIGCOMM 2001 Conf. San Diego, Aug 2001,

[5]福田尚弘他”発信源探査システムの研究開発”, 電子情報通信学会 2004 総合大会,Mar.2004

[6] 甲斐俊文他“送信元アドレスを偽装した不正パケットの発信源探査方式”,情報処理学会 DPS 研究会 2004
[7] 塚本克治他” AS 間のトレースバックに関する一考察” ,電子情報通信学会 2004 総合大会,Mar.2004
[8] 大森圭祐他“IP トレースバックの数学モデルと検証”,情報処理学会 DPS 研究会 2004