推薦論文

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[†] 鈴木彩子[††]

インターネットの普及にともなって，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はじめている．その対策として，いくつかの発信源探査方式（トレースバック方式）が提案されているが実用レベルには至っていない．本稿では，既存方式の問題点を解決したハイブリッドトレースバック方式を提案し，探査性能および導入（実装）の容易さの点から既存方式との比較を行う．探査性能については数学モデルと PC ルータを用いたテストベッドでの実験により評価する．これらの評価により，提案する新方式の優位性を示す．

Efficient Traceback Method for Detecting DDoS Attacks

Toshifumi Kai,[†] Hiroshige Nakatani,[†] Hiroshi Shimizu[†]
and Ayako Suzuki[††]

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 have serious impacts on the society. Various attacker detection techniques have been proposed until now. However, they have not been put in practical use. We propose hybrid traceback method that solves the drawbacks of the existing techniques. Its characteristics in performance and easiness of implementation are discussed in this paper. Advantages of this proposed method to the existing ones are clarified by some numerical models and experiment on the test bed.

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たどっている．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．

このような攻撃の発信源を探査する一般的な手法として，不正パケットの経路をもとに探査を行うトレースバック（**図 1**）がある．

ただしインターネットは，プロバイダネット，行政ネットなど固有のポリシによって管理された AS（Autonomous System）の集合体で構成されているため，複数の AS にわたって同じ方法で探査することは不可能に近い．そこで，AS 間のトレースバックと AS 内のトレースバックを階層的に行う必要があるといわれている[1),2)]．

AS 内のトレースバック方式については，現在までにさまざまな方式が提案されているが[3)~7)]，それぞれに一長一短があり，どれも絶対的なものとはいえない．また，複数の方式を併用する手法も提案されているが[8),9)]，有効性は明らかになっていない．

我々は，AS 内トレースバック方式を対象として，既存方式の長所を生かしながら，それらが持つ短所を

† 松下電工株式会社先行技術開発研究所
Advanced Technologies Development Laboratory, Matsushita Electric Works, Ltd.
†† NTT アドバンステクノロジ株式会社コアネットワーク事業本部
Core Networks Business Headquarters, NTT Advanced Technology Corporation

本論文の内容は 2004 年 12 月のコンピュータセキュリティ研究会にて報告され，CSEC 研究会主査により情報処理学会論文誌への掲載が推薦された論文である．

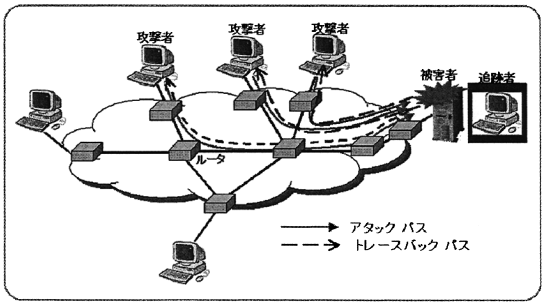

図 1 トレースバック
Fig. 1 Image of traceback system.

補完する組合せの手段とその実現方法について検討し[9),10)]，性能面および実用面で既存方式を上回る独自方式を考案した．さらに，この方式を用いて既存の課題を抜本的に解決した新方式を考案した[11)]．

本稿ではまず，既存トレースバック方式の中でも最も有効といわれる 3 つの方式（ICMP 方式，マーキング方式，Hash 方式）に着目して各方式の特徴を述べる．次に，既存の方式では困難とされる DDoS 攻撃を高速に探査するために考案した独自方式（連動方式，uTrace）と Hash 方式を組み合わせたものを新方式（ハイブリッド I，II）として提案する．特に，新方式の核となる独自方式については，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，優位性を示す．

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．

どの方式もすべてのルータ上（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なる．

本章の 2.1 節〜2.3 節では各方式の中から代表的な実装例（表 1 に ∗ 印で示す）を取り上げ，概要（仕組み）と特徴について述べる．また，2.4 節にこれら既存方式の問題点をまとめる．

2.1 ICMP 方式

ICMP 方式の具体的な実装方式として，IETF（Internet Engineering Task Force）で標準化が検討されていた iTrace[3)] を我々が独自に改良した iTrace-II について説明する．iTrace-II の動作手順を**表 2** に示す．ICMP 方式では探査情報を送るために新たにパケットを生成する必要があり，ネットワークに流れるパケット量が増加する．なお，探査端末では集まってくる iTrace パケットから探査したいパケットの特徴と一致するサンプリングパケットの情報を組み合わせることで攻撃経路を再現する．

表 1 既存のトレースバック方式
Table 1 Existing traceback methods.

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 ∗

表 2 iTrace-II の動作
Table 2 Operation step of iTrace-II system.

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 ・一つ前のルータ＋自ルータ＋一つ先のルータのIPアドレス ・IPヘッダ＋ペイロード数バイトなど (iii)iTraceパケットに書きこまれたサンプリングパケットが定数L個を超え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

表 3 AMS-II の動作
Table 3 Operation step of AMS-II system.

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のハッシュ値を算出し，8bit単位で8分割(フラグメント)して，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)へマーク値として書き込む (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を書込む (iv) (i) から繰返す

2.2 マーキング方式

マーキング方式の代表的な実装例として AMS-II[5)] を取り上げる．その動作を**表 3** に示す．マーキング方式は新たなパケットを生成しないためネットワークに流れるパケット量は増加しない．なお，探査端末ではあらかじめ IP アドレスの Hash 値を計算済みのルータマップを持っておき，探査したいパケットの特徴と一致するパケットに付加されているマーク値から攻撃

表 4 SPIE の動作
Table 4 Operation step of SPIE system.

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)ハッシュ値記録用テーブル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)問合せされたパケットのハッシュ値を計算する (ii)ハッシュ値記録用テーブルのハッシュ値番地のフラグを確認する (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に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

表 5 既存方式の比較
Table 5 Evaluation of existing traceback methods.

方式名		ICMP (iTrace-II)	マーキング (AMS-II)	Hash (SPIE)
攻撃端末一台辺りのパケット流量	大量 (DoS)	○	○	—
	少量 (DDoS)	×	△	—
	単発	—	—	○
導入時の問題		ほぼ問題なし	要ルータマップ／ヘッダ改変	コスト（必要メモリ量やや大）

○:性能高 △:性能中 ×:性能低 —:非対応

経路上にあるルータを見つけていく．

2.3 Hash 方式

Hash 方式は前出の 2 つの方式とは異なり，探査端末から各ルータに対して能動的に問合せを行うトレースバック方式である．この方式の代表的な実装例である SPIE[6] の動作を**表 4** に示す．

Hash 方式ではルータがすべてのパケットについてハッシュ値を記録しておくため，1 パケット攻撃に対する探査が可能であり，精度も高い．

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．

ICMP 方式（iTrace-II）は，ネットワークにかける負荷を考慮してサンプリング確率を低く設定しなければならない．そのため，数万個以上の攻撃パケットが送信されなければ探査できない．

マーキング方式（AMS-II）は探査によるパケットの増加がないため，サンプリング確率を高く設定できる．しかしそれでも確率的サンプリングを行うため，探査には数千個以上の攻撃パケットを要する．また，探査端末が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るため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．

Hash 方式（SPIE）は 1 パケットに対する探査が可能であり，確率に依存しないために ICMP 方式やマーキング方式に比べ正確な探査が可能である．ただし，1 パケットの探査に対して複数の問合せパケットを送信するため DoS 攻撃や DDoS 攻撃のような被害端末に大量のパケットが送信される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．

3. 考案した新方式（ハイブリッド方式）

3.1 新方式へのアプローチ

どのような攻撃であっても探査可能なトレースバックシステムを実現するために，我々は複数の方式を組み合わせることを検討した．

1 パケット攻撃に対する探査は Hash 方式でカバーすることでほぼ問題はない．しかし複数パケットの攻撃向けのトレースバック方式は，2.4 節で述べたとおり既存の方式では不十分である．

我々は，論文 10) で ICMP 方式と Hash 方式を連動させることで複数パケット攻撃に対してマーキング方式と同等の性能を持つ連動方式を考案し，それを通常の Hash 方式と組み合わせたハイブリッド I 方式を提案した．その後，新たにマーキング方式よりも単独で性能の良い UDP 方式（uTrace）を作り出し，それを Hash 方式と組み合わせたハイブリッド II 方式を考案した．この 2 つのハイブリッド方式の構成と，研究の流れを**図 2** に示す．

3.2 ハイブリッド I 方式

3.2.1 ハイブリッド I 方式の構成

ハイブリッド I 方式は，複数パケット攻撃に対しては ICMP（iTrace-II）方式と Hash（SPIE）方式の技術を組み合わせた連動方式で探査を行い，単発パケット攻撃は Hash 方式のみで探査を行う．Hash 方式単体の特徴，動作については前述のとおりであるため，

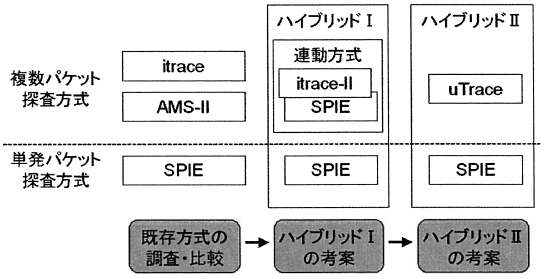

図 2 ハイブリッド方式の構成と研究の流れ
Fig. 2 Structure of two hybrid traceback methods and step of our development.

以下では我々の考案した連動方式について構成と動作を述べる．

3.2.2 連動方式の構成

各ルータには iTrace-II と SPIE のモジュールを実装する．探査端末側も iTrace-II の受信機能と SPIE の問合せ機能を持つ．攻撃を探査する際には双方が連動して経路情報を収集し，攻撃経路を構築する．

3.2.3 連動方式の動作

ルータ側では，表 2 と表 4 にあるような iTrace-II と SPIE の両方の動作を行う．探査端末は通常時には何も処理を行わないが，攻撃が発生し，IDS（Intrusion Detection System）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 パケットのチェック
ルータから送られてきた iTrace パケットに含まれているサンプリングパケットが，探査対象に該当すればステップ 2 を実行する．この判定は，探査要求に含まれている探査したいパケットの特徴情報（送信先 IP アドレスやポート番号，ペイロードの内容など）との比較により行う．該当しない場合は次の iTrace パケットの到着を待つ．

（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 iTrace パケットを送信してきたルータを最初の問合せ先とする．

（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，ステップ 1 に戻る．

3.3 ハイブリッド II 方式

3.3.1 ハイブリッド II 方式の構成

ハイブリッド II 方式では，単発パケット攻撃の探査には Hash 方式のみを使用し，複数パケット攻撃に対しては新たに考案した uTrace（UDP 方式）を用いる．以下では uTrace について説明を行う．

3.3.2 uTrace の構成

各ルータには uTrace のモジュールを実装する．探査端末は uTrace の探査要求メッセージをルータに送信する機能と，各ルータから送信された uTrace パケットを受信する機能を持つ．

3.3.3 uTrace の動作

uTrace では通常時はルータと探査端末は特別な処理を行わない．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．なお，探査開始時は被害端末最寄りのルータに対して探査要求メッセージを送る．

（ステップ 1）探査要求メッセージの送信
探査端末は指定されたルータに探査要求メッセージを送信する．内容は，探査したいパケットの特徴情報（連動方式と同様），探査端末の IP アドレス，uTrace パケットの要求数，要求の有効期間，などである．

（ステップ 2）uTrace パケットの送信
探査要求メッセージを受けたルータは，要求の有効期間が過ぎるまで通過パケットをすべて監視し，探査したいパケットの特徴にマッチするものを選択する．そして選択したパケットの探査情報を uTrace パケットに書き込んで探査端末に送信する（ただし uTrace パケットの要求数以上は送信しない）．

（ステップ 3）次のルータの選択
探査端末は uTrace パケットを受信すると，そのパケットに書き込まれている 1 つ攻撃端末寄りのルータの IP アドレスを探査リストに加える．もし，探査リストにまだ登録されていないアドレスであったら，そのアドレスについて（ステップ 1）のメッセージ送信を行う．

以上を繰り返すことで，攻撃パケットが通過するたびに，攻撃経路上のルータに順次探査要求メッセージが送信され，探査端末は各ルータから探査情報を集めることができる．

図 3 に uTrace の動作概要を示す．

探査要求 0 を受け取ったルータ R1 は，被害端末 V に向かう通過パケットの監視を開始する．その後，探査したいパケットの特徴に合致する攻撃パケット P1 が通過すると，R1 はルータ R2 の IP アドレスや P1 の IP ヘッダ＋ペイロード数バイトなどが書き込まれた uTrace1 を探査端末 M に送信する．探査端末 M はそれを受け取ると，R2 の IP アドレスを探査リストに登録し，R2 に探査要求 1 を送信する．攻撃パケット P2 が通過した場合も同様に，R1 が uTrace2 を M に送信し，その後 M は R3 に探査要求 2 を送信する．

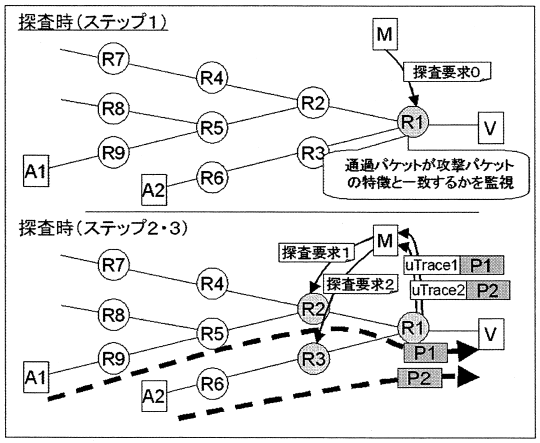

図 3 uTrace の動作概要
Fig. 3 Operation image of the uTrace system.

こうして，攻撃パケットが通過するごとに，攻撃端末に近いルータに探査要求が送られていく．

A1 から大量に攻撃パケットが送信されてきても，R1 は探査要求メッセージで指定された要求数以上の uTrace パケットは送信しない．ただし，R1 は uTrace パケットの送信数を隣接ルータごとに区別してカウントする．このため，A1 からの攻撃パケットに対する uTrace パケットの送信数が上限に達していても，それとは無関係に A2 からの攻撃パケットに対して uTrace パケットを送信できる．これにより，DDoS 攻撃の場合でもすべての経路を探査することが可能になる．

4. 性能評価

方式ごとに複数パケット攻撃に対する探査性能の数学モデルを求め，比較を行う．また，PC ルータ（Linux）で構成されたテストベッドで実験を行った結果から，uTrace の性能を確認する．

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，評価モデルを以下のようにした．

4.1.1 発信源探査の定義

本稿では，コンピュータフォレンジックの観点から，攻撃端末と攻撃パケット通過経路の両方を見つけ出すことを発信源探査と定義した．

4.1.2 前提とする環境条件

攻撃パケットと非攻撃パケットの正確な切り分けおよび攻撃発生と同時にアラート生成ができる理想的な IDS と，通信遅延・輻輳・パケットロスが発生しない理想的なネットワークを用いた環境下を前提とする．

また，通常トラフィックの流量は iTrace-II や連動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．

表 6 数学モデルに用いる記号一覧
Table 6 Symbol list for numerical model of each traceback system.

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 台あた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	−
探査成功率	Q	−

※方式によって定義が異なる

4.1.3 攻撃パラメータ

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）のみとした．また，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 H である．攻撃端末数は S^H となる．

4.1.4 経路確定閾値

この値は探査情報の信頼度を上げるための閾値である．ICMP 方式や連動方式では iTrace パケット，UDP 方式であれば uTrace パケット，マーキング方式ではマーク値を単位探査情報としたときに，この値以上同じ単位探査情報が集まったときに初めてその情報を信頼する．この値を増やすと誤検知を抑えることができるが探査により時間が必要となるため，状況に応じて探査者が任意に決める値である．本稿の計算例や実験では各方式とも 2 としたが，別の値を用いても各方式の比較結果に影響はない．

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 6** にまとめた．また，二項分布関数 $fb(k,n,p)$ を用いる．これは確率 p で成功する独立試行を n 回繰り返したときに，成功数がちょうど k 回になる確率を意味する関数であり，これを用いることで n 個のパケットがルータを通過した際に iTrace パケットやマーク値が得られる確率を求めることができる．

4.2.1 既存方式の数学モデル

式 (1) は iTrace-II について，式 (2) は AMS-II について，それぞれ発信源探査時間と探査成功率の関係

を示している．攻撃端末からのホップ数 $d = 0 \sim H-1$ に位置する攻撃経路上のすべてのルータが，iTrace-II の場合は B 個以上 iTrace パケットを送信する確率，AMS-II の場合は 8 つのマーク値すべてを B 個以上送信する確率が探査成功率である．なお，T [sec] の間に攻撃端末から d ホップ目にあるルータを通過する攻撃パケットの数は ATS^d 個である．また，AMS-II の場合は攻撃端末に近いルータがマークした値が被害端末に近いルータにより上書きされることも考慮している．

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

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

4.2.2 連動方式の数学モデル

連動方式では攻撃経路上のルータのどれか 1 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．このため，探査成功率は式 (3) で表される．

$$Q = 1 - \sum_{k=0}^{B-1} fb(k, ATH, P) \quad (3)$$

4.2.3 uTrace の数学モデル

uTrace は確率に依存しないため，探査に必要な情報が取得できるだけの時間が経過すれば 100%探査成功であり，その時間までは探査は成功しない．必要な情報が集まる時間とは，探査開始後，ホップ数 H と同数の攻撃パケットが送信されるまでの時間である．経路確定閾値 B が 2 以上であれば，さらに $B-1$ 個の攻撃パケットの送信を待つことで全ルータからその分の uTrace パケットを得る必要がある．よって発信源探査時間と探査精度の関係は式 (4) になる．

$$Q = \begin{cases} 0 & \text{ただし} \quad T < \dfrac{H+(B-1)}{A} \\ 1 & \text{ただし} \quad T \geq \dfrac{H+(B-1)}{A} \end{cases} \quad (4)$$

ただし，式 (4) は探査する立場から見て悪条件下での成功率を示している．攻撃者が複数いる場合，被害端末に近いルータでは攻撃パケットが集中し 1 台からの攻撃のときよりも探査時間が短くなるが，式 (4) ではそれを無視している．これは複数の攻撃端末がつねに同時に攻撃パケットを送信するような特殊な状況に相当する．

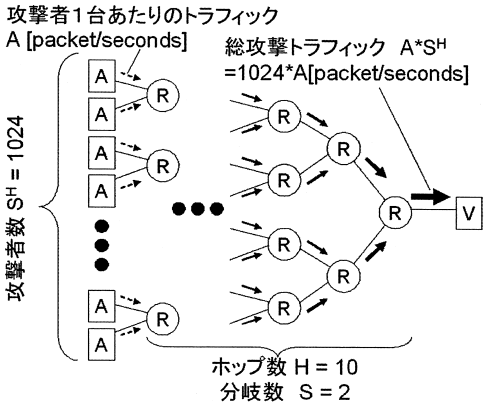

図 4 評価に用いた DDoS 攻撃モデル
Fig. 4 DDoS attack model for the numerical analysis.

表 7 探査可能な攻撃パケット流量
Table 7 Minimum attack traffic which each method can traceback in 10 seconds (Result of numerical analysis).

方式名	10秒間で探査可能な最低攻撃パケット流量[packet/sec]
ICMP方式(iTrace-II)	1904.5
マーキング方式(AMS-II)	181.3
連動方式(iTrace-II+SPIE)	189.8
ＵＤＰ方式(uTrace)	1.1

4.2.4 探査可能な攻撃パケット流量の範囲の比較

DDoS 攻撃に対する探査性能を比較するために，探査時間を 10 秒とした場合，方式ごとに探査可能な攻撃者 1 台あたりの攻撃パケット流量（packet/sec）の最低値を数学モデルにより求めた．なおここでは，探査成功率が 95%以上になることを，探査可能と見なした．また，比較に用いた攻撃モデルを**図 4** に示す．

その他の条件は経路確定閾値 $B = 2$，iTrace-II のサンプリングパケット集約数 $L = 5$，iTrace-II と連動方式のサンプリングレート $P = 1/4000$，AMS-II のサンプリングレート $P = 1/20$ とした．サンプリングパケット集約数とサンプリングレートはそれぞれの方式の推奨値である．この条件で探査可能な攻撃者 1 台あたりの攻撃パケット流量の最低値を数学モデルから求めた結果を**表 7** に示す．

この条件下で DDoS 攻撃のような少量パケット攻撃に対する各方式の性能を比較すると，iTrace-II よりも連動方式と AMS-II は 1/10 以下の攻撃パケット流

表 8 テストベッドの構成
Table 8 Specification of the test-bed.

機器・環境	項目	内容
ネットワーク	PCルータ数	40台
	エンドノード数	160台 (実PC30台)
	ネットワークタイプ	Ethernet (100base)
PCルータ	OS	Redhat Linux 7.3
	CPU	Celeron2.0GHz
	メモリ	512Mbytes
エンドノード (仮想マシン)	仮想マシンアプリケーション	User Mode Linux
	ホストマシン (実PC)	PCルータと同スペック

量まで探査可能であり，uTrace はさらにその 1/100 以下の攻撃パケット流量まで探査可能であることが分かる．追跡可能な 1 台あたりの攻撃パケット流量の上限については，各方式とも制限がなくどんなに流量の大きな攻撃でも追跡可能である．したがって，uTrace は他の方式よりも広い範囲の攻撃を探査可能であるといえる．

4.3 テストベッドでの実験

uTrace の性能を検証するために Linux PC ルータで構成されたテストベッド上で実験を行った．なお，既存方式についてもこのテストベッド上で試験がなされており，論文 12) で報告されている．

4.3.1 実験環境

テストベッドの構成と使用した機器の仕様を**表 8** に示す．仮想マシンを用いて，1 台の実 PC あたり 5 から 6 台のエンドノードを模擬している．

4.3.2 実験方法

まず，攻撃端末数 1 台あたりの攻撃パケット流量を一定（50 packet/sec）にし，攻撃端末から被害端末までのホップ数を変化させて，探査が完了する時間を測定した．次に，1 台あたりの攻撃パケット流量と攻撃端末台数が異なる 4 つのテストパターンを用意し，すべての攻撃者を探査し終える時間を測定した．

図 5 にテストベッドの構成図を示す．攻撃端末数を複数にした場合の配置も示している．

ホップ数を変化させる試験において，ホップ数を 15 や 20 にして実験する際には一部配線の変更も行った．攻撃の種類は syn flood とし，経路確定閾値は 2 とした．試験はそれぞれ 60 回行い，探査時間の平均値と

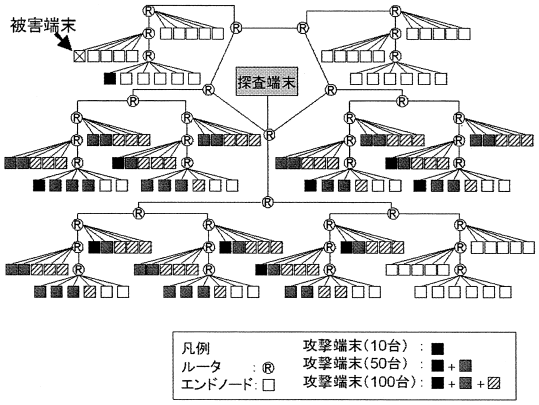

図 5 テストベッドの構成および攻撃端末の配置
Fig. 5 Network topology of the test-bed and distribution of attackers.

表 9 ホップ数変更試験の結果
Table 9 Traceback time for each hop number of attack path (Result of uTrace experiment on the test-bed).

ホップ数	理論値 [sec]	実測値 [sec]	標準偏差
3	0.080	0.077	0.0072
5	0.120	0.118	0.0077
10	0.220	0.217	0.0077
15	0.320	0.320	0.0107
20	0.420	0.419	0.0156

理論値を比較した．

4.3.3 実験結果

ホップ数変更試験の結果を**表 9** に示す．この結果により，攻撃端末単体では実測値と理論値がほぼ一致することが確認できた．

さらに，攻撃端末台数と攻撃パケット流量を 4 つのパターンに変化させた実験の結果を**図 6** に示す．各パターンとも被害端末に到着する攻撃パケットが合計 100 packet/sec となるように設定した．よって，攻撃端末台数が増えればその分 1 台あたりの攻撃パケット流量が少なくなるため，探査に時間がかかる．

この結果を見ると，攻撃端末が複数であるため，被害端末に近いルータで攻撃パケットが集約されて，悪条件を想定した理論値よりも早く探査が完了していることが分かる．よってこの実験では，攻撃端末の台数が増え，密集度合いが高くなるほど悪条件下の理論値よりも早く探索できるという傾向が確認できた．

ちなみに，数学モデルとテストベッドでの実験との違いは，ネットワーク遅延時間，ルータと探査端末の処

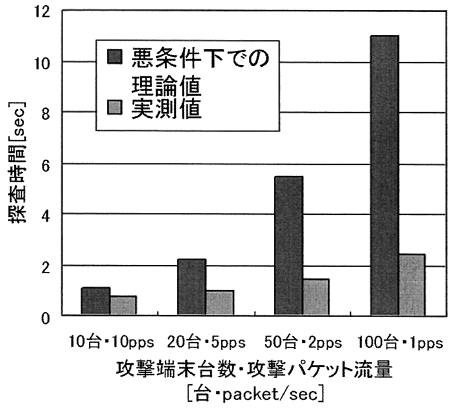

図 6 攻撃端末台数・攻撃パケット流量変更試験の結果
Fig. 6 Traceback time for each attack pattern (Result of uTrace experiment on the test-bed).

理時間，非対称なトポロジ，非同期の攻撃，syn flood を受けた被害端末からの TCP ACK 応答，といった点である．以上の実験では，これらの要素は特に探査時間に悪影響を与えていないことが分かる．

5. 考　　察

5.1 考案した方式の優位性

4.2.4 項で述べたように，少量パケット攻撃の探査について，連動方式はマーキング方式（AMS-II）と同等の性能を持ち，uTrace はさらに高い性能を持つ．

また，実環境への導入時の問題として，連動方式は Hash 方式同様，ルータにある程度大きなメモリを追加する必要がある．uTrace は ICMP 方式同様，特に導入時に問題になる特性は持たない．これらのことをまとめると，**表 10** のようになる．

また，Hash 方式とその他の方式を組み合わせた場合，**表 11** のようになる．前述のとおり，ハイブリッド I は連動方式，ハイブリッド II は UDP 方式（uTrace）を Hash 方式と組み合わせたものである．

ハイブリッド I 方式は，マーキング＋ Hash 方式と比較して，性能でほぼ同等，導入の容易さではこれを上回るものとなっている．さらにハイブリッド II 方式は，より高い性能を持ち，さまざまな攻撃が探査可能なものとなった．

5.2 必要になるメモリ量とルータの処理負荷

iTrace-II では探査情報をまとめて送信するため，探査情報を記憶しておくための若干のメモリが必要になる．AMS-II はルータに追加のメモリを必要としない．uTrace では隣接するルータごとに uTrace パケットの送信個数を計数するカウンタが必要になるが，100 台のルータと隣接するルータでも，1 Kbyte の以下のメモリで十分である．Hash 方式はパケットの Hash 値を記録するためにある程度大きなメモリを必要とする．SPIE の論文 6) によると，OC-3（156 Mbps）のインタフェースを 4 つ持ったルータでおよそ 47 MByte，OC-192（10 Gbps）のインタフェースを 32 個持つルータでおよそ 23.4 GByte のメモリが必要である．

また，実装したモジュールをインストールした PC ルータ単体の性能を測定したところ，どの方式でもモジュールをインストールしていない PC ルータと比較してスループットの低下は見られなかった．これは探査モジュールの処理負荷が小さく，CPU 負荷がボトルネックとならなかったことを意味する．なお，探査を実行した際に uTrace と SPIE はルータが問合せ応答処理を行うが，1 回の探査で各ルータともたかだか 1 個の探査要求について処理を行うだけである．このため，同時に多数の探査が実行されない限り，ルータにかかる負荷はほとんど増加しない．

ネットワークに増加するパケット量については，論文 11) で数学モデルを立てて評価した．探査を行っ

表 10 既存方式と考案した方式の比較
Table 10 Evaluation of proposal traceback methods and existing ones.

方式名		ICMP (iTrace -II)	マーキング (AMS-II)	Hash (SPIE)	連動方式 (iTrace-II + SPIE)	UDP (uTrace)
攻撃端末一台あたりのパケット流量	大量 (DoS)	○	○	−	○	○
	少量 (DDoS)	×	△	−	△	○
	単発	−	−	○	−	−
導入時の問題		ほぼ問題なし	要ルータマップ/ヘッダ改変	コスト (必要メモリ量やや大)	コスト (必要メモリ量やや大)	ほぼ問題なし

○:性能高 △:性能中 ×:性能低 −:非対応

表 11 Hash 方式との組合せでの比較
Table 11 Evaluation of hybrid systems which is combined hash method and each DDoS traceback method.

方式名		ICMP ＋ Hash	マーキング ＋ Hash	ハイブリッドI (連動方式 ＋ Hash)	ハイブリッドII (UDP ＋ Hash)
攻撃端末一台辺りのパケット流量	大量 (DoS)	○	○	○	○
	少量 (DDoS)	×	△	△	○
	単発	○	○	○	○
導入時の問題		コスト (必要メモリ量やや大)	要ルータマップ/ヘッダ改変/コスト	コスト (必要メモリ量やや大)	コスト (必要メモリ量やや大)

○:性能高 △:性能中 ×:性能低

ていない場合には，iTrace-II と連動方式が同じ数だけ増加する．AMS-II や uTrace は増加数 0 である．DDoS 攻撃の探査を行った場合には，連動方式が最も増加数が大きく，次いで iTrace-II，uTrace の順である．このため，uTrace は iTrace-II や連動方式に比べ，ネットワークにかける負荷は小さいといえる．なお，AMS-II は探査を行った場合にも増加数 0 である．

5.3 DDoS 攻撃探査における未検知と誤検知

4.2 節で攻撃者の発見に成功する確率を数学モデルで示した．未検知率（FNR）はこの成功率を 1 から引いた値になる．また，我々は論文 13) において探査結果に含まれる誤検知の割合（FPR）についても明らかにしている．通常のユーザが送信するものと同じ種類のパケットを使って攻撃が行われており，かつ 1 台あたりの攻撃パケット流量も通常のユーザが送信するパケット流量と同程度に低い場合，理論的に攻撃端末と通常ユーザとの区別がつけられないため，どの方式を用いても誤検知が発生する．攻撃パケットもしくは 1 台あたりの攻撃パケット流量が明らかに通常ユーザと異なる場合には，ルータの故障，Hash コリジョンの発生，および探査中の攻撃終了という場合を除き，誤検知は発生しない．

6. おわりに

我々は，トレースバックの代表的な既存方式について評価を行い，その結果を基にハイブリッド方式を考案し，優位性を示した．また，PC ルータを用いたテストベッドでの実機試験も行い，性能を確認した．

なお，本稿では AS 内のトレースバック方式について述べたが，複数 AS での探査を連携させるための AS 間トレースバック[14] に関してもテストベッドでの性能評価を完了しており，別途報告する．

謝辞 本研究は故塚本克治教授と共同で進めてきた．故人の冥福を祈るとともに，ここに記して謝意を示す．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) 塚本克治，高橋輝壮，橋口　輝，清水　弘，中谷浩茂，甲斐俊文：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).
2) 大江将史，門林雄基：階層型 IP トレースバック機構の実装と検証，電子情報通信学会インターネットアーキテクチャ技術論文特集 (Aug. 2003).
3) Bellovin, S.M.: ICMP Traceback Message, InternetDraft: draft-bellovin-itrace-00.txt, submitted (Mar. 2000).
4) Savege, S., Wtherall, D., Karlin, A., Anderson, T.: Practical Network Support for IP Traceback, *Proc. Sigcomm 2000*, Stockholm, Sweden (Aug. 2000).
5) Song, D. and Perrig, A.: Advanced and Authenticated Marking Schemes for IP Traceback, *Proc. IEEE INFO-COM* (Apr. 2001).
6) Snoeren, A.C., Partridge, C., Sanchez, L.A., Jones, C.E., Tchakountio, F., Kent, S.T. and Strayer, T., Hash-Based IP Traceback, *Proc. ACM SIGCOMM 2001 Conf.*, San Diego (Aug. 2001).
7) 早川晃弘，馬場達也，小久保勝敏，松田栄之：不正アクセス発信源追跡システムにおける追跡時間の評価，情報処理学会第 64 回全国大会，pp.389–390 (Mar. 2002).
8) 山田竜也，池田竜朗，森尻智昭，才所敏明：発信源追跡のためのハイブリッドトレースバック方式の設計と実装，情報処理学会分散システム/インターネット運用技術シンポジウム (Jan. 2003).
9) 福田尚弘，甲斐俊文，中谷浩茂，清水　弘，塚本克治：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).
10) 甲斐俊文，中谷浩茂，清水　弘，塚本克治：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，情報処理学会第 12 回マルチメディア通信と分散処理ワークショップ (Dec. 2004).
11) 甲斐俊文，中谷浩茂，清水　弘，鈴木彩子，塚本克治：DDoS 攻撃に対する高性能発信源探査方式の提案，情報処理学会第 27 回 CSEC 研究発表会 (Dec. 2004).
12) 大森圭祐，松嶋　竜，鈴木彩子，川端まり子，大室　学，甲斐俊文，西山　茂：IP トレースバックの数学モデルと検証，情報処理学会第 12 回マルチメディア通信と分散処理ワークショップ (Dec. 2004).
13) 鈴木彩子，大森圭祐，大室　学，松嶋　竜，川端まり子，西山　茂，甲斐俊文：IP トレースバックシステムの信頼性の特性分析，情報処理学会第 27 回 CSEC 研究発表会 (Dec. 2004).
14) 甲斐俊文，長嶋昭人，中谷浩茂，清水　弘，高橋輝壮，鈴木彩子：DDoS 攻撃に対する AS 間発信源探査方式の提案，情報処理学会第 28 回 CSEC 研究発表会 (Mar. 2005).

(平成 17 年 6 月 6 日受付)
(平成 18 年 1 月 6 日採録)

推薦文

DDoS 攻撃に対するトレースバック方式として，新たに uTrace 方式を考案しており，この方式と従来法との組合せにより，高い探査性能を実現できると考えられる．また，方式ごとに数学モデルを用いた性能評

価を行う一方，テストベッド上での実験評価も行い，実験と理論値がほぼ一致することを確認しており，信頼性も高いと考えられる．新規性，信頼性に優れ，論旨も明確であるので，推薦する．
（コンピュータセキュリティ研究会主査　村山 優子）

甲斐　俊文（正会員）
2000 年九州工業大学情報工学部知能情報工学科卒業．2002 年同大学大学院情報工学研究科博士前期課程修了．同年松下電工株式会社入社．2002〜2004 年トレースバック技術の研究に従事．現在，未知ウィルス検知をはじめとするネットワークセキュリティ技術の研究開発に従事．電気情報通信学会正会員．

中谷　浩茂
1990 年筑波大学情報学類卒業．同年松下電工株式会社入社．LAN 機器相互接続性技術の開発，暗号 ASIC の開発等に従事．現在，未知ウィルス検知をはじめとするネットワークセキュリティ技術の研究開発に従事．

清水　　弘
東京大学大学院博士課程修了．農学博士．光磁気ディスク装置の開発，電力線搬送システムの開発等に従事．1989 年松下電工株式会社入社．現在，同社先行技術開発研究所ネットワークセキュリティ研究室室長．

鈴木　彩子
2000 年東海大学開発工学部情報通信工学科卒業．同年 NTT アドバンステクノロジ株式会社入社．通信サービス関連のソフトウェア開発，トレースバック技術の研究開発に従事．現在，通信サービス関連のソフトウェア開発に従事．