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

2004－ＱＡＩ－12　（1）
2004／7／12

DoS攻撃に対するIPトレースバック手法のシミュレーション
－ICMPトレースバック方式のシミュレーション－

山名　正人[†]　平田　勝弘[†]　清水　弘[†]　中谷　浩茂[†]　甲斐　俊文[†]　塚本　克治[‡]

[†]松下電工株式会社 〒571-8686 大阪府門真市門真1048
[‡]工学院大学情報工学科通信システム研究室 〒163-8677 新宿区西新宿 1-24-2

E-mail: [†]yamana@cqad.mew.co.jp, hirata@ertc.mew.co.jp,
{simizu,nakatani,kai}@trc.mew.co.jp, [‡]tsukamoto @tsukaken.jp

あらまし　近年，インターネットの安全性を脅かすDoS攻撃（ネットワークサービス不能攻撃）が社会問題となり深刻化している．このDoS攻撃を防ぐため，攻撃者を探査するIPトレースバック手法が注目されている．このIPトレースバック手法に関する従来の研究は理論計算や確率計算による簡易的なシミュレーションが中心であった．現実のネットワークに対応するために今回，代表的なネットワークシミュレーションソフトであるOPNETを改良してIPトレースバック手法のICMPトレースバック方式を評価するためのシミュレーションソフトを開発した．このソフトを直列型ネットワークとツリー型ネットワークに適用し，有効性を確認したので報告する．

キーワード　DoS攻撃，DDoS攻撃，IPトレースバック手法，ICMPトレースバック方式

Simulation of IP Traceback for the Denial of Service Attack
－Simulation of ICMP Traceback －

Masahito YAMANA[†]　Katsuhiro HIRATA[†]　Hiroshi SHIMIZU[†]
Hiroshige NAKATANI[†]　Toshihumi KAI[†]　Katshuji TSUKAMOTO[‡]

[†]Matsushita Electric Works, Ltd. Kadoma1048, Kadoma-shi, Osaka, 571-8686 Japan
[‡]Multimedia Infomatics Kogakuin Univ. Nishishinjyuku1-24-2, Shinjyuku-ku, Tokyo 163-8677 Japan

E-mail: [†]yamana@cqad.mew.co.jp, hirata@ertc.mew.co.jp,
{simizu,nakatani,kai}@trc.mew.co.jp, [‡]tsukamoto@tsukaken.jp

Abstract Recently, Denial of Service (DoS) Attacks become serious problems. In order to protect DoS Attacks, various kinds of IP traceback methods have been proposed to find the attacking host. Usual studies in this field are mostly the theoretical analysis or the simple simulation based on probability computation. In this paper, we focus on ICMP traceback and develop the simulation method by improving the commercial network simulator code "OPNET". The effectiveness of this method is verified when it is applied to both models of serial network and tree-structural network.

Keyword DoS (Denial of Service) Attack, DDoS (Distributed Denial of Service) Attack, IP traceback, ICMP traceback

1. はじめに

近年，インターネットの安全性を脅かすDoS（Denial of Service）攻撃やDDoS（Distributed Denial of Service）攻撃が社会問題となり深刻化している．2000年2月にはYahoo!，Amazon.com，CNNといった大手のサイトがDDoS攻撃により停止に追い込まれるといった被害が報告されている．DoS攻撃は不正アクセスの1つで攻撃者が大量のパケットを被害者に送りつけることでネットワークの帯域を不正に占有し，被害者のインターネットの使用を妨害するものである．また，複数の攻撃者によるものがDDoS攻撃である．攻撃に用いられるパケットの送信元IPアドレスは一般に偽装されており発信源（攻撃者）探査は非常に困難である．そこで発信源探査技術の1つとしてIPトレースバック手法が研究されている[1]．この手法は送信元IPアドレスの偽装の有無に関わらず発信源を探査する技術である．発信源探査により被害者はDoS攻撃，DDoS攻撃を阻止することが可能となる．

現在まで複数のIPトレースバック手法が提案されているが，我々はICMPトレースバック方式[2]（ICMP traceback，以下iTrace方式），IPマーキングトレースバック方式[3]（IP Marking traceback，以下Marking方式），Hashトレースバック方式[4]（Hash traceback，以下Hash方式）に着目し，実用化に向け実装技術を開発し実機評価を行っている．また，これらの方式の問題点を解決する組み合わせ方式を検討中である[5]．ただし，実機評価では大規模ネットワークでの評価が難しい．従って，シミュレーションによる評価が必要と

なるが，従来の研究では理論計算や確率計算による簡易的なシミュレーションが中心であった[6]-[9]．また，ネットワークシミュレーションソフト NS2[10]を使用した報告[6],[11]もあるが実機をモデル化したシミュレーションの報告例はほとんど見当たらない．そこで本研究では代表的なネットワークシミュレーションソフトであるOPNET[12]を改良しiTrace方式評価のためのシミュレーションソフトを開発した．

本論文では，簡易モデルとして直列型ネットワークに，応用モデルとしてツリー型ネットワークに適用し本手法の有効性を確認したので報告する．

2. IP トレースバック手法

IP トレースバック手法は，あるパケットが通過してきた経路（ルータ）をたどって発信源を探査する技術である．従って，ルータ（もしくはそれに接続する機器）は発信源探査のための情報を被害者側の攻撃者を追跡する機器に伝える必要がある．この情報の伝え方により複数の IP トレースバック手法が提案されており，以下に各方式について紹介する．今回はこれらの方式の内，iTrace 方式についてシミュレーションソフトを開発した．

2.1. ICMP トレースバック方式（iTrace 方式）

ルータで ICMP パケット（iTrace パケット）の中に逆探知情報（リンク情報やサンプリングしたパケットの情報）を入れ，追跡側の機器に伝える方式である．追跡側は逆探知情報入りのパケットを集めて分析し攻撃経路を検出する．

2.2. IP マーキングトレースバック方式（Marking 方式）

ルータでサンプリングしたパケットの中に逆探知情報を入れ追跡側の機器に伝える方式である．追跡側は逆探知情報入りのパケットを集めて分析し攻撃経路を検出する．

2.3. Hash トレースバック方式（Hash 方式）

ルータ側で通過するパケット全ての Hash 値を記録しておく方式である．追跡側は探査したいパケットの Hash 値の有無を各ルータに問い合わせて経路を検出する．

3. モデル化

実機評価と同等のシミュレーションを行うためには，実機の動作及び逆探知情報出力を再現する必要がある．そのためには実機をモデル化し，ネットワーク上でシミュレーションできるソフトが必要となる．そのソフトとして市販ソフト“OPNET”をもとに改良した．まずOPNETについて紹介した後，iTrace方式のモデル化について説明する．

3.1. OPNET

OPNET はパケット単位でのネットワークシミュレーションを行うことが可能なソフトとして広く使用されている．その OPNET について図１～３にて説明する．図１は OPNET のネットワークモデルを，図２はサーバーの内部構造を示している．各ノードは実際のネットワークのように層構造（OSI 参照モデル）に従って構築され，各層はモジュール単位で構成されている．各モジュールは図３のように機能がプロセス化されており，各プロセスのソースを改良可能である．今回の iTrace 方式のモデル化は OPNET 標準モデルのワークステーション，ルータ，サーバーのネットワーク層とデータリンク層の界面にある arp モジュールにソースを追加して行った．

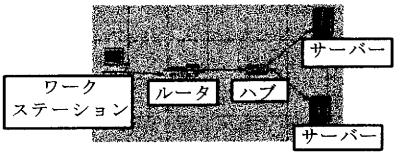

図１ OPNET のネットワークモデル

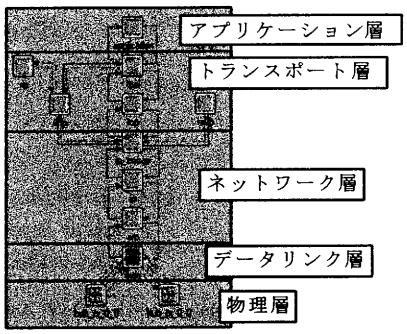

図２ ノードモデルの内部（図はサーバー内部）

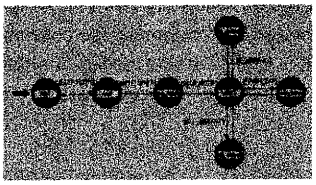

図３ モジュールのプロセスモデル（図は arp 内部）

3.2. iTrace 方式のモデル化

本研究にて評価する iTrace 方式モデルの特徴を以下に示す．

1．ルータは通過するパケット数に従って通過パケットをサンプリングし iTrace パケットを生成する．

2．iTrace パケットに格納する逆探知情報はリンク情報としてIP アドレスとMAC アドレス，サンプリングしたパケット情報としてプロトコルがある．図４にホップ数３の直列ネットワークを示す．Router2

が iTrace パケットを生成した場合に格納される IP アドレスを図4に示している．また，IP アドレス詐称に対応するため IP アドレスと同様に各位置の MAC アドレスも格納する．また，サンプリングしたパケットのプロトコルは攻撃の特定に用いる．

これら以外に iTrace パケットを生成したルータのホップ数を割り出すため，パケットの TTL 値も逆探知情報とする．

3．被害者側で iTrace パケットを収集しデータベースに保存する PC をコレクタと呼ぶ．そのデータベースを参照し逆探知を行う PC をトレーサーと呼ぶ．

シミュレーションではクライアント（攻撃者または普通の送信者），ルータ，コレクタをモデル化して行う．iTrace パケットが生成されコレクタに収集される時間に比べてトレーサーで攻撃者を逆探知する時間は無視できるほど短いのでトレーサーはモデル化しない．以下に個々のモデル化について示す．

1．クライアント（攻撃者または普通の送信者）

OPNET 標準モデルのワークステーションに次のプロセスを追加する．

・全てのパケットの backward up IP に自身の IP アドレスを格納し，サンプリングしたパケットが攻撃か普通かのフラグを立てて送信．

2．ルータ

ルータは通過パケット数に応じて通過パケットをサンプリングし ICMP パケットを生成するが，シミュレーションではサンプリングしたパケットをコピーして iTrace パケットとする．次のモデル化を行う．

(a) 通過パケットが iTrace パケットの場合

① 直前のルータによる iTrace パケット

forward down IP に自身の IP アドレスを格納し送信

② 直前のルータ以外による iTrace パケット

そのまま送信

(b) 通過パケットが iTrace パケットでない場合

iTrace パケット生成判定を行う．iTrace パケット生成確率を p とすると次の手順で iTrace パケット生成判定を行う．

1．前回使用した生成判定数 x を y に代入

2．1～1/p までの乱数 x を生成

3．通過パケットが 1/p－y + x 個通過したとき通過パケットをサンプリングしてコピーし iTrace パケット生成

4．通過パケットカウンターを初期化し1へ

以上の手順により，iTrace 生成確率は平均して p となる．

① iTrace パケットを生成する場合

生成した iTrace パケットの backward down IP に自身の入口 IP アドレスを，forward up IP に自身の出口 IP アドレスを格納

② iTrace パケットを生成しない場合

backward up IP に自身の出口 IP アドレスを格納

3．コレクタ

OPNET 標準モデルのサーバーに次のプロセスを追加する．

・iTrace パケットが直前のルータのものかを判定

(a) 直前のルータで生成された場合

forward down IP に自身の IP アドレスを格納した後，逆探知情報を出力

(b) 直前のルータ以外で生成された場合

逆探知情報を出力

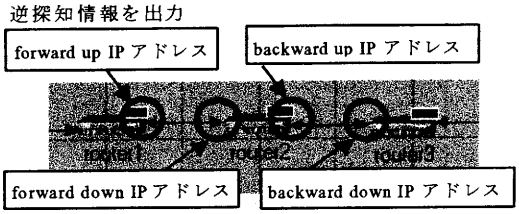

図4 iTrace パケットに格納するリンク情報

3.3. 動作確認

ここで意図した逆探知情報が出力されるかを確認する．図5にホップ数3のツリー型ネットワークを示す．図5は攻撃者（attacker）4，被害者（victim）1，ルータ（router）7台のネットワークである．表1にこのネットワークの IP アドレスを示す．このネットワークにおいて攻撃者4台からパケットを送信したときコレクタにて出力された結果を表2に示す．表2より，4つの IP アドレス，パケット種，TTL 値が正しく出力されていることを確認できる．この出力結果を用いれば攻撃者を逆探知するトレーサーにより実機の逆探知プロセスを再現できる．

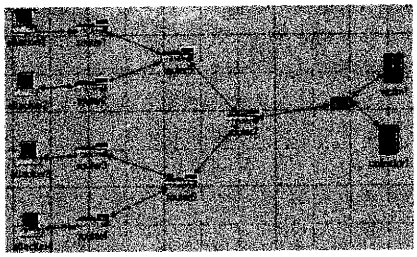

図5 ツリー型ネットワーク（ホップ数3）

表１　図５のネットワークのIPアドレス

ノード名	IPアドレス	接続先
attacker1	192.0.11.1	router1
attacker2	192.0.10.2	router2
attacker3	192.0.9.2	router3
attacker4	192.0.8.2	router4
router1	192.0.11.2	attacker1
	192.0.5.2	router5
router2	192.0.10.1	attacker2
	192.0.4.2	router5
router3	192.0.9.1	attacker3
	192.0.6.2	router6
router4	192.0.8.1	attacker4
	192.0.7.2	router6

ノード名	IPアドレス	接続先
router5	192.0.5.1	router1
	192.0.4.1	router2
	192.0.3.2	router7
router6	192.0.6.1	router3
	192.0.7.1	router4
	192.0.2.2	router7
router7	192.0.3.1	router5
	192.0.2.1	router6
	192.0.1.1	collector1
collector1	192.0.1.3	router7

表２　逆探知情報出力結果

No.	攻撃開始からの時間[秒]	ルータ名	backward-up-IP	backward-down-IP
1	0.04	router7	192.0.3.2	192.0.3.1
2	1.15	router1	192.0.11.1	192.0.11.2
3	1.15	router6	192.0.7.2	192.0.7.1
4	1.17	router4	192.0.8.2	192.0.8.1
5	2.11	router5	192.0.4.2	192.0.4.1
6	3.02	router7	192.0.3.2	192.0.3.1
7	4.13	router7	192.0.2.2	192.0.2.1
8	5.12	router3	192.0.9.2	192.0.9.1
9	5.15	router6	192.0.6.2	192.0.6.1
10	7.07	router7	192.0.3.2	192.0.3.1

No.	forkward-up-IP	forkward-down-IP	パケット種(0:攻撃, 2:普通)	TTL値(初期値255)
1	192.0.1.1	192.0.1.3	2	255
2	192.0.5.2	192.0.5.1	0	253
3	192.0.2.2	192.0.2.1	0	254
4	192.0.7.2	192.0.7.1	0	253
5	192.0.3.2	192.0.3.1	0	254
6	192.0.1.1	192.0.1.3	2	255
7	192.0.1.1	192.0.1.3	0	255
8	192.0.6.2	192.0.6.1	0	253
9	192.0.2.2	192.0.2.1	0	254
10	192.0.1.1	192.0.1.3	2	255

3.4.理論計算と数値解析

今回開発したシミュレーションソフトの検証のため理論計算と数値解析を行う．ただし，理論計算と数値解析は図６に示すような簡易な直列型ネットワークモデルのみに適用することができる．

比較する値は攻撃経路構築までの総パケット数とする．ネットワークの途中でiTraceパケットがロストしてしまう可能性を考慮し，コレクタでiTraceパケットが２個収集されるまでの総パケット数を攻撃経路構築までのパケット数とする．

まず理論計算について示す．１台のルータがiTraceパケットを２個以上生成する確率Pは通過パケット数をN，iTraceパケット生成確率をpとして

$$P = 1-(1-p)^N - pN(1-p)^{N-1} \qquad (1)$$

ホップ数Rのとき全てのルータがiTraceパケットを２個以上出す確率Qは

$$Q = P^R = \left[1-(1-p)^N - pN(1-p)^{N-1}\right]^R \qquad (2)$$

となる．図７にp=1/20000，Q=0.95のときの攻撃経路構築までのパケット数とホップ数の関係を図７に示す．ホップ数の増加に伴い攻撃経路構築までにかかるパケット数の増加は抑えられる．ただし，この理論計算はiTraceパケット生成確率pが厳密なときのみに適用可能である．

今回モデル化したiTrace方式はiTraceパケット生成確率の平均値がpとなるため，式（２）は適用できない．従って，数値解析との比較により検証を行う．この数値解析は今回モデル化した方式のiTraceパケット生成判定を再現している．ルータがその生成判定に沿い何個目のパケットでiTraceパケットを２個出すかを数値解析する．ホップ数Rの場合はR回解析を繰り返してパケット数を算出する．

図８にiTraceパケット生成確率p=1/20000のときの数値解析の結果を示す．この結果は試行回数10000回の結果で全試行の内，攻撃経路構築に95%が成功するときのパケット数とホップ数の関係を示す．

図７と図８の比較より理論計算と数値解析の傾向が一致していることを確認した．この数値解析の結果を用いて今回開発したシミュレーションソフトの検証を行う．

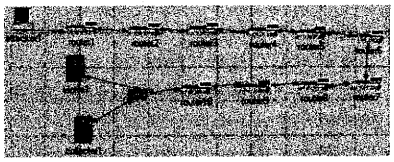

図６　直列型ネットワーク（ホップ数10）

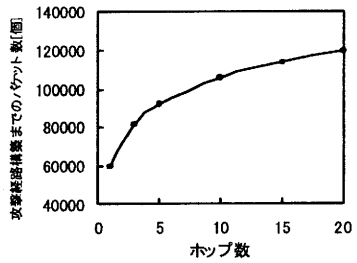

図７　理論計算結果（p=1/20000，Q=0.95）

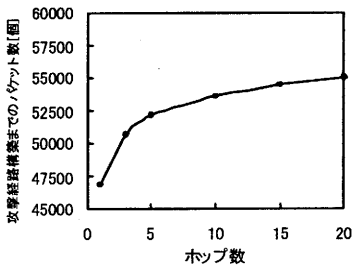

図８　数値解析結果
（p=1/20000，全試行の95%が成功する場合）

4. 結果

今回開発したシミュレーションソフトについて簡易モデルとして直列型ネットワーク，応用モデルとしてツリー型ネットワークに適用して検証を行う．

4.1. 簡易モデル（直列型ネットワーク）

簡易モデルの検証は直列型ネットワークでの結果を数値解析の結果と比較して行う．解析モデルは図6を用いる．解析条件を以下に示す．

・攻撃速度　1250パケット／秒
　これは攻撃者 20 台のとき被害者への攻撃速度を25000パケット／秒と想定している．
・攻撃パケットの割合　0.5555
　（普通パケット速度1000パケット／秒）
・iTrace パケット生成確率　1 / 20000
　この方式ではiTraceパケットを生成するため，トラフィックの増加が問題となる．ネットワーク帯域に負担をかけないトラフィックの増加率は 0.1%以下であり，ホップ数 20 と仮定したときその値を満足するiTraceパケット生成確率は1/20000と報告されている[6]．また，ネットワークのエンドーエンド間の平均ホップ数が16[13]であることからホップ数を20と仮定している．
・比較結果　各試行での攻撃経路構築までのパケット数の平均値．ただし，攻撃経路上の全ルータのiTraceパケットを２個収集するまでの総パケット数を攻撃経路構築までのパケット数とする．

iTrace 方式は数万単位のパケットをシミュレーションする必要がある．そのため，パケット単位のシミュレーションを行う OPNET の計算時間が問題となる．ここで数値解析により有効な試行回数を算出する．図９に前述の解析条件での数値解析の試行回数と精度の関係を示す．試行回数10000回のときを真値とすると図９より試行回数は 50 回で十分（誤差 10%以下）である．

図10にOPNETでの計算値（50試行）と数値解析結果（10000 試行）の比較を示す．両者の結果はほぼ一致し（誤差 10%以下），今回開発したシミュレーションソフトが有効であることが確認できる．

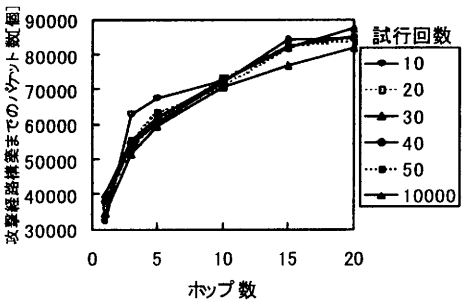

図９　試行回数と精度の関係

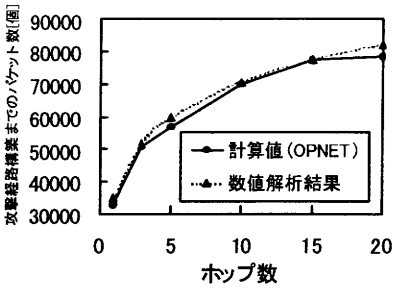

図10　計算値と数値解析結果の比較

4.2. 応用モデル

応用モデルはツリー型ネットワークで計算する．解析モデルは図 11 のホップ数６のツリー型ネットワークでクライアントは32台，ルータは63台である．解析条件を以下に示す．

・攻撃速度　1250パケット／秒
・攻撃パケットの割合　1.0
　時間短縮のため攻撃パケットのみ
・iTrace パケット生成確率　1 / 20000
・攻撃者数は攻撃経路がなるべく重複しないように1，4，8，16，32 台と増加
・試行回数は20回
・比較結果　各試行での攻撃経路構築までのパケット数の平均値．ただし，攻撃経路上の全ルータのiTraceパケットを２個収集するまでの総パケット数を攻撃経路構築までのパケット数とする．

図 12 に計算結果と上記解析条件によるホップ数６のときの数値解析結果を示す．図12より攻撃者１台の計算結果は 43083 パケット，数値解析の結果は 42692 パケットであり誤差0.92%である．従って，攻撃者１台の場合は正しく計算できていることが確認できる．

また，複数の攻撃者の場合はiTraceパケットが生成確率に従って正しく生成されていることを確認する．表３にホップ数８のときの各ルータを通過する総パケット数と各ルータで生成されたiTraceパケット数の平均を示す．この場合，攻撃開始から最後のiTraceパケットがコレクタで収集される時間は 49.186 秒であった．表３より生成されたiTraceパケット数と総パケット数／20000 を比較するとほぼ一致しており，iTraceパケット生成確率に従ってiTraceパケットが生成されていることが確認できる．

図 12 より攻撃者 4 台と８台では攻撃経路構築にかかるパケット数はほぼ一定になっている．また，８台以上では緩やかな増加傾向を示す．これは以下に示す攻撃経路構築までのパケット数の増加要因と減少要因が均衡しているためと考えられる．

・ 増加要因　攻撃者数の増加に伴い，見つけるべきルータ数が増加する．

・ 減少要因　攻撃者数の増加に伴い，攻撃者１台から下流を見ると攻撃パケットは増加する．そのため，iTrace パケットが生成されやすくなる．

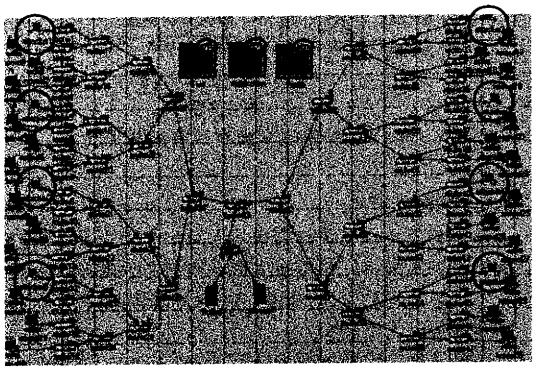

図 11　ツリー型ネットワーク
（ホップ数６，攻撃者数８台）

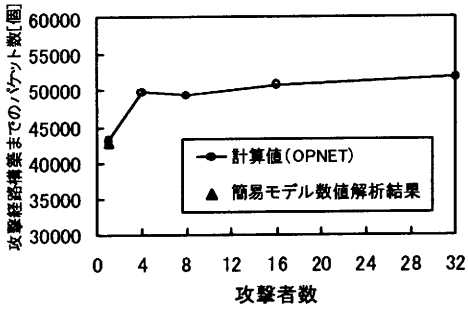

図 12　ツリー型ネットワークの結果

表３　総パケット数と iTrace パケット数の関係

攻撃速度 [パケット/秒]	総パケット数	ルータ名	iTraceパケット数 平均値	総パケット数 /20000
1250	61483	router1,5,9,13,17, 19,21,23,25,26, 27,28,32,36,40, 44,48,50,52,54, 56,57,58,59	2.67	3.07
2500	122965	router29,30,60,61	5.75	6.15
5000	245930	router31,62	12	12.3
10000	491860	router63	24	24.6

5. 結論

簡易モデル，応用モデルの結果から今回開発した iTrace 方式のシミュレーションソフトの有効性が確認できた．また，今回開発したシミュレーションソフトの出力を用いれば実機と同様の逆探知プロセスを再現可能である．

今後の予定としては実機への適用評価，大規模ネットワークでの評価，他方式のシミュレーションソフトの開発が挙げられる．また，我々が考案した組み合わせ方式の性能解析にも適用する予定である．

6. 謝辞

本研究は情報通信研究機構（NICT）から「大規模ネットワークセキュリティの確保に向けた研究開発」として受託（平成 14～16 年度）し，実施中である．ここに記して謝意を表します．

文　献

[1] 門林雄基，大江将史，“IP トレースバック技術”，情報処理，vol.12，no.42，pp.1175-1180，2001

[2] S. Bellovin, M. Leech and T. Taylor, “ICMP Traceback Message”, Internet Draft, draft-ietf-itrace-04.txt, 2003

[3] D. X. Song and A. Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback”, Proc. IEEE INFOCOM2001, pp. 878-886, 2001

[4] A. Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakoutio, S. Kent and W. Straer, “Hash-based IP Traceback”, Proc. ACM SIGCOMM2001, pp. 3-14, 2001

[5] 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 年総合大会

[6] 澤井裕子，大江将史，飯田勝吉，門林雄基，“IP トレースバック技術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”，高品質インターネット，4-2，pp. 4-13，2002

[7] V. Kuznetsov, H. Sanddtrom and A. Simkin, “An Evalution of different IP Traceback approches”, ICICS 2002 Singapore, pp. 1-9, 2002

[8] K. Park and H. Lee, “On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack”, Proc. IEEE INFOCOM '01, pp. 338-347, 2001

[9] A. Habib, M. M. Hefeeda and B. K. Bhargava, “Detecting Service Violations and DoS Attacks”, Proc. NDSS'03, pp. 177-189, 2003

[10] http://www.isi.edu/nsnam/ns/

[11] Henry C. J. Lee, Vrizlynn L. L. Thing, Yi Xu and Miao Ma, “ICMP Traceback with Cumulative Path, an Efficient Solution for IP Traceback”, ICICS 2003, pp. 124-135, 2003

[12] http://www.opnet.com/products/modeler/home.html

[13] 情報処理相互運用技術協会，“平成 12 年度オープンネットワーク化推進のための調査研究報告書”，pp. 70-71