2004－QAI－13　(1)
2004／10／28

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
－IP マーキング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,
{shimizu,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，攻撃者を追跡するトレースバック（発信源探査）技術が注目されている．このようなトレースバック技術の既存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る．本論文では，代表的なシミュレーションソフトである OPNET をベースとして IP マーキングトレースバック方式のシミュレータを構築し，直列型ネットワーク及びツリー型ネットワークに適用して有効性を確認した．

キーワード　DoS 攻撃，DDoS 攻撃，IP トレースバック手法，IP マーキングトレースバック方式

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

Masahito YAMANA[†]　Katsuhiro HIRATA[†]　Hiroshi SHIMIZU[†]
Hiroshige NAKATANI[†]　Toshifumi KAI[†]　Katsuji 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,
{shimizu,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. The theoretical analysis and the probability computation are generally employed to apply. In this paper, we focus on IP marking traceback and construct the simulator which is based on 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, IP marking 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．2003 年度のインターネット上での情報セキュリティ被害報告では DoS 攻撃などの不正アクセス被害が全体の約 20％を占めている[1]．

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，複数の攻撃拠点（攻撃者という）を設定し，攻撃するのが 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[2]．この手法は送信元 IP アドレスの偽装の有無に関わらず攻撃パケットのパスを構築し，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 IP マーキングトレースバック方式[3]（IP Marking traceback，以下マーキング方式），ICMP トレースバック方式[4]（ICMP traceback，以下 iTrace 方式），Hash トレースバック方式[5]（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ハイブリッド方式を検討中である[6]．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[7]-[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[8],[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．そのため，前報[12]で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[13]をベースとしてICMP トレースバック方式評価のためのシミュレータを構築し，直列型ネットワークで数値解析との比較により定量的に検証を行い，ツリー型ネットワークで定性的に検証し，提案手法の有効性を確認した．

本論文では，前報で有効性を確認した提案手法により IP マーキングトレースバック方式評価のためのシミュレータを構築し，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．

2. IP マーキングトレースバック方式(マーキング方式)

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）をたどってそのパケットのパスを構築する技術である．従って，ルータ（もしくはそれに接続する機器）はパス構築のための情報を被害者側に置かれた攻撃者追跡装置に伝える必要がある．今回はマーキング方式についてシミュレータを構築した．マーキング方式はルータでサンプリングしたパケットの中にパス構築情報を入れ追跡側の機器に伝える方式である．追跡側はパス構築情報入りのパケットを集めて分析し攻撃パスを検出する．

本研究にて評価するマーキング方式は Song と Perrig が提案した AMS II 方式[3]を元にしたものである．ルータで通過パケットに格納されるパス構築情報は以下の 4 つである．

① Start IP
マーキングするルータの 1 つ前のルータの出口側 IP アドレス（図 1）

② End IP
マーキングするルータの出口側 IP アドレス(図 1)

③ distance field
ルータを通過するごとにプラス 1 される数値．マーキングされると初期化して 0 にする．

上記の①～③はリンク情報である．

④ マークフラグメント
AMS II 方式では①～③を 16bit の Identification フィールドに格納するためハッシュ値に変換している．このハッシュ値の衝突を防ぐため，マークフラグメントを定義している．

これらのパス構築情報はパケットの IP ヘッダの 16 ビットの Identification フィールドに格納される．

この方式の特徴について以下に示す．

1．ルータは通過パケットをある確率でサンプリングし，パス構築情報を追加する．サンプリングされたパケットをマーキングパケットと呼び，格納するパス構築情報は前述の Start IP, End IP, distance field, マークフラグメントである．マークフラグメントは 3 ビットの領域に格納するので，0～7 である．

2．被害者側でマーキング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パス構築を行う PC をトレーサーと呼ぶ．

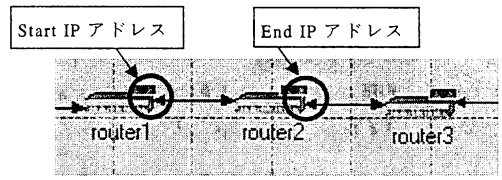

図 1 マーキングパケットに格納するリンク情報

3. 提案手法

前報[13]と同様に OPNET をベースとしてシミュレータを構築した．OPNET の特徴に TCP/IP プロトコルを階層的にモジュールとして構成していること，パケット送受信等の契機をトリガーとするイベントドリブンであることがある．これらを利用してパケット単位でのシミュレーションを行うこととしてマーキング方式をモデル化し，アルゴリズムを作成した．以下に提案手法におけるマーキング方式のモデル化とパス構築の動作確認を示す．

3.1. マーキング方式のモデル化

提案手法ではクライアント（攻撃者または普通の送信者），ルータ，コレクタをモデル化する．マーキング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までのパスを構築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．また，IP パケットに Start IP, End IP, distance field, マークフラグメントと Temp IP の情報を持たせる．また，本来は Start IP, End IP, distance field, マークフラグメントはハッシュ値を求めて Identification フィールドに分割して入れるが，シミュレーション上では簡単のためそのまま書き込む．ただし，実験上問題は無い．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）

既存モデルのワークステーションに全パケットの Temp IP に自身の IP アドレスを格納し，distance field

を０として送信するプロセスを追加する．

２．ルータ

既存モデルのルータに以下のプロセスを追加する．通過パケットのサンプリング判定値をＳとすると，ルータは通過パケットごとに１～Ｓの乱数を振り，１の場合にマーキングする．このとき，通過パケットのサンプリング確率は１／Ｓとなり，これをマーキング確率と呼ぶ．

(a) 通過パケットをマーキングする場合

Temp IP を Start IP に代入する．自身の出口側 IP アドレスを End IP に格納し，distance field を０とする．また，０～７の乱数を振り，マークフラグメントを決定する．また，ルータ名も格納する．

(b) 通過パケットをマーキングしない場合

Temp IP に自身の出口側 IP アドレスを格納し，distance field に１を加える．

３．コレクタ

既存モデルのサーバーにマーキングパケットに格納されたパス構築情報を出力するプロセスを追加する．

3.2. パス構築の動作確認

提案手法により構築したシミュレータのパス構築情報出力が正しいことを確認する．図２にホップ数３のツリー型ネットワークを示す．図２は攻撃者（attacker）４台，被害者（victim）１台，ルータ（router）７台のネットワークである．コレクタは被害者に並列に接続されている．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，Start IP，End IP，distance field，マークフラグメント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へのパスを構築するトレーサーにより実機のパス構築プロセスを再現できる．

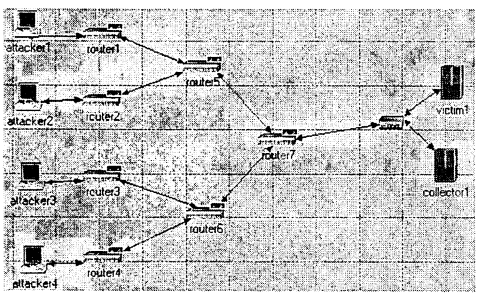

図２　ツリー型ネットワーク（ホップ数３）

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	192.0.2.1	router1
attacker2	192.0.3.1	router2
attacker3	192.0.4.1	router3
attacker4	192.0.5.1	router4
router1	192.0.2.2	attacker1
	192.0.6.2	router5
router2	192.0.3.2	attacker2
	192.0.7.2	router5
router3	192.0.4.2	attacker3
	192.0.8.2	router6
router4	192.0.5.2	attacker4
	192.0.9.2	router6

ノード名	IPアドレス	接続先
router5	192.0.6.1	router1
	192.0.7.1	router2
	192.0.11.2	router7
router6	192.0.8.1	router3
	192.0.9.1	router4
	192.0.10.2	router7
router7	192.0.11.1	router5
	192.0.10.1	router6
	192.0.1.1	collector1
collector1	192.0.1.2	router7

表２　パス構築情報出力結果

攻撃開始からの経過時間[秒]	ルータ名	Start IP	End IP	distance field	マークフラグメント
0.00033	router7	192.0.10.2	192.0.1.1	0	6
0.00037	router4	192.0.5.1	192.0.9.2	2	6
0.00051	router5	192.0.7.2	192.0.11.2	1	4
0.00055	router7	192.0.11.2	192.0.1.1	0	7
0.00101	router6	192.0.9.2	192.0.10.2	1	7
0.00117	router4	192.0.5.1	192.0.9.2	2	2
0.00119	router5	192.0.6.2	192.0.11.2	1	5
0.00135	router5	192.0.6.2	192.0.11.2	1	4
0.00145	router3	192.0.4.1	192.0.8.2	2	0
0.00157	router7	192.0.10.2	192.0.1.1	0	3
0.00181	router6	192.0.9.2	192.0.10.2	1	7
0.00183	router7	192.0.11.2	192.0.1.1	0	0
0.00199	router7	192.0.11.2	192.0.1.1	0	0
0.00203	router5	192.0.7.2	192.0.11.2	1	0

4. 適用事例

今回構築したシミュレータを単純な直列型ネットワーク及びツリー型ネットワークに適用し，その計算結果を検証する．

4.1. 直列型ネットワークへの適用

図３に計算する直列型ネットワークの例を示す．直列型ネットワークは理論計算が可能であるので，理論計算と本論文のシミュレーション結果を比較し，シミュレーションの妥当性を確認する．検証条件について以下に示す．

１．比較する結果

シミュレーションの全試行の 95%が攻撃パス構築するまでのパケット数について理論計算の結果と比較する．攻撃パス構築までのパケット数はネットワークの途中でマーキングパケットがロストしてしまう可能性を考慮し，コレクタでマーキングパケットが２個収集されるまでの総パケット数とする．攻撃パス上の全ルータの８個のマークフラグメントについてマーキングパケットを２個収集するまでの総パケット数を攻撃パス構築までのパケット数とする

２．マーキング確率

マーキング確率は 1/20 とする．これはネットワークのエンド－エンド間の平均ホップ数が 16[14]であることから最大ホップ数を 20 としたためである．

被害者から攻撃者までのホップ数が 20 の場合，全ルータの中で最もマーキングパケットが届きにくいのは被害者から最も離れた 20 ホップめのルータである．ここで被害者から R ホップめのルータのマーキングパケットがコレクタに到達する確率 U はマーキング確率を p とすると

$$U = p(1-p)^{R-1} \qquad (1)$$

となる．図 4 にホップ数 20 のときのマーキングパケットがコレクタに到達する確率とマーキング確率の関係を示す．この図 4 より，ホップ数 20 のときの最適なマーキング確率が 1/20 であることがわかる．

4.1.1. 理論計算（従来法）による結果

distance field として d をマーキングするルータからあるマークフラグメントを持つマーキングパケットをコレクタが 2 個以上受け取る確率を P_d とする．ルータを通過するパケット数を N，マーキング確率を p，マークフラグメント数を m とすると P_d は次の式（2）となる．

$$P_d = 1 - \left\{1 - \frac{p}{m}(1-p)^d\right\}^N - \frac{Np}{m}(1-p)^d\left(1 - \frac{p}{m}(1-p)^d\right)^{N-1} \qquad (2)$$

distance field の最大値が n のとき，コレクタが全てのルータから全てのマークフラグメントについてマーキングパケットを 2 個以上受け取る確率 Q は

$$Q = P_0 P_1 P_2 \cdots P_{n-1} P_n \qquad (3)$$

となる．図 5 に p=1/20，m=8，Q=0.95 のときの攻撃パス構築までのパケット数とホップ数の関係を示す．ただし，攻撃パス構築までのパケット数は式（3）において p=1/20，m=8，Q=0.95 としたときの N である．また，distance field に 1 を加えたものがホップ数となる．図 5 を見るとホップ数の増加に伴い，攻撃パス構築までのパケット数が増加することがわかる．これはホップ数の増加に伴い，見つけるべきルータが増加するためである．

4.1.2. 提案手法による結果

図 3 のネットワークについて解析する．

(a) 解析条件

- 攻撃速度　50 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 1000 パケット／秒と想定している．
- 攻撃パケットの割合　1.0
  攻撃パケットのみ送信
- マーキング確率　1 / 20
- 試行回数　100 回

(b) 理論計算との比較

図 6 に攻撃パス構築までのパケット数とホップ数の関係について示す．提案手法と理論計算の結果は定量的にほぼ一致し，提案手法が有効であることが確認できる．

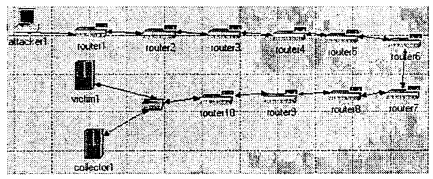

図 3　直列型ネットワーク（ホップ数 10）

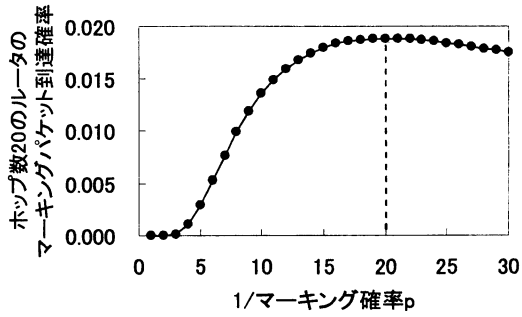

図 4　到達確率（ホップ数 20）とマーキング確率の関係

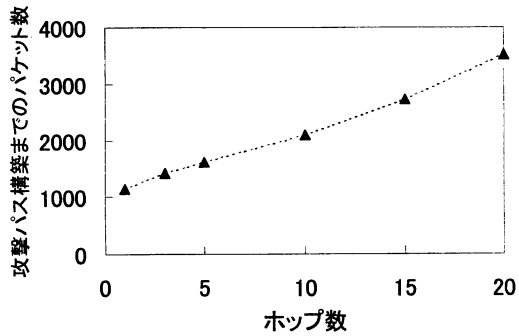

図 5　理論計算結果（p=1/20，m=8，Q=0.95）

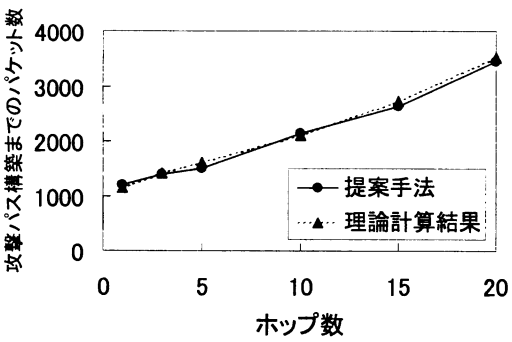

図６　提案手法と理論計算結果の比較

4.2. ツリー型ネットワークへの適用

ツリー型ネットワークでは攻撃者が独立に攻撃する場合を除いて理論解析は不可能である．従って，提案手法のみ適用する．図７のホップ数６のツリー型ネットワークについて解析を行い，クライアントは 32 台，ルータは 63 台である．

(a) 解析条件

・攻撃速度　50 パケット／秒
・攻撃パケットの割合　1.0
・マーキング確率　1 / 20
・攻撃者数は攻撃パス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　100 回

(b) 解析結果

全試行の 95%が攻撃パス構築するまでのパケット数を解析する．ただし，攻撃パス上の全ルータの８個のマークフラグメントについてマーキングパケットを２個収集するまでの総パケット数を攻撃パス構築までのパケット数とする

図８に解析結果を示す．図８より攻撃者の増加に伴い，攻撃パス構築にかかるパケット数は緩やかな増加傾向を示す．これは以下に示す攻撃パス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　図９，10 に攻撃者１台と８台のときの攻撃速度を示す．攻撃者数１台のときの攻撃速度は 50 パケット／秒で一定だが，攻撃者８台のときは下流に向かうにつれ攻撃速度は上がる．つまり，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，マーキングパケットが生成されやすくなる．

以上の結果からツリー型ネットワークにおいて提案手法を定性的に評価できた．

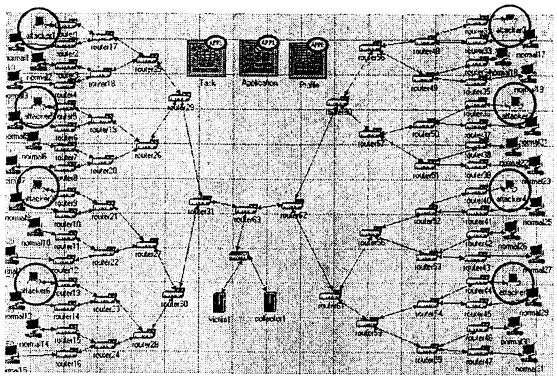

図７　ツリー型ネットワーク
（ホップ数６，攻撃者数８台）

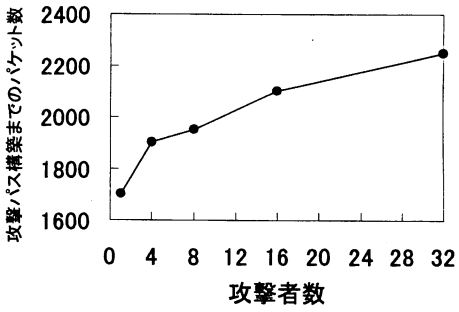

図８　ツリー型ネットワークの結果

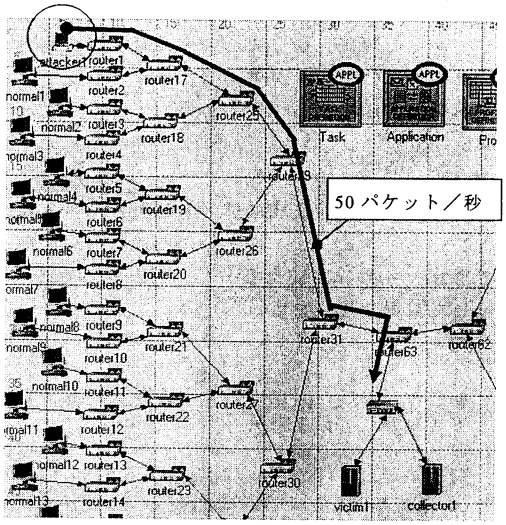

図９　攻撃者１台のときの攻撃速度

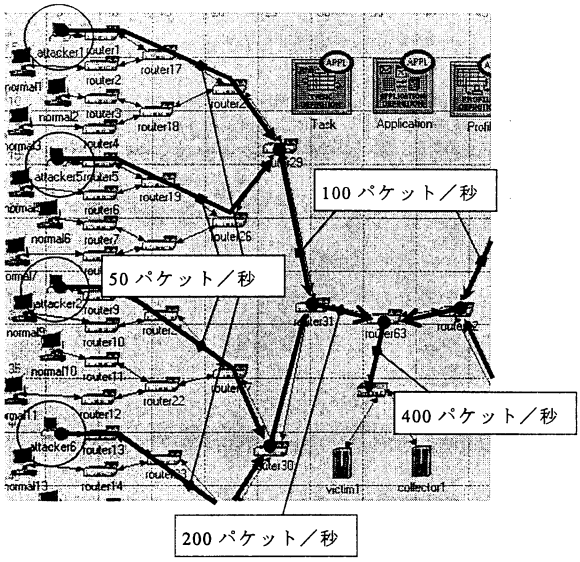

図 10　攻撃者 8 台のときの攻撃速度

5. 結論

構築したマーキング方式のシミュレータを直列型ネットワークに適用して従来法である理論計算との比較により定量的に検証した．また，ツリー型ネットワークに適用して定性的に検証した．以上の直列型ネットワークとツリー型ネットワークによる結果から提案手法の有効性が確認できた．また，今回構築したシミュレータの出力を用いれば実機と同様のパス構築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タの構築が挙げられる．また，我々が考案したハイブリッド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] 警察庁，“平成 15 年度不正アクセス行為対策等の実態調査”，pp. 12-13

[2] 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

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

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

[5] 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

[6] 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

[7] 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

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

[9] 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

[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] 山名正人，平田勝弘，清水弘，中谷浩茂，甲斐俊文，塚本克治，“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－”，信学技報，vol.104，No.173，pp.1-6，2004

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

[14] 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