2004－CSEC－27　(7)
2004／12／20

IP トレースバックシステムの信頼性の特性分析

鈴木　彩子[+]　大森　圭祐[+]　松嶋　竜[+]　川端　まり子[+]
大室　学[+]　甲斐　俊文[++]　西山　茂[+]

[+] 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
[++] 松下電工株式会社 システム技術研究

あらまし　分散型サービス妨害攻撃の攻撃者を特定する技術として、各種の IP トレースバック方式が提案されている。これらの方式を採用した IP トレースバックシステムの運用では、信頼性が問題となる。本論文では、代表的な IP トレースバック方式である ICMP、マーキング、新たに提案されている UDP 方式の信頼性の特性を分析する。信頼性の指標は、未検知率、誤検知率とする。分析方法として、数学モデルにより特性分析を行い、大規模検証ネットワークでの実測により分析を裏付ける。

Reliability Feature Analysis for IP Traceback Systems

Ayako SUZUKI[+]　Keisuke OHMORI[+]　Ryu MATSUSHIMA[+]　Mariko KAWABATA[+]
Manabu OHMURO[+]　Toshifumi KAI[++]　Shigeru NISHIYAMA[+]

[+] NTT Advanced Technology Corp., Core Network Business Headquarters
[++] Matsusita Electric Works, Ltd. System Technology Reasearch Labratory

abstract　IP traceback is a technique that searches DDoS attackers. There are many kinds of IP traceback methods. In a practical use of IP traceback systems, reliability of the systems is very important. In this paper, we analyze reliability features of typical IP traceback methods, which are ICMP, marking, and an UDP method newly proposed.　False negative rate and False positive rate are evaluation parameters of the reliability. First we analyze mathematical models. Then we compare the analysis with measured values using the real large network for verification.

１．　まえがき

分散型サービス妨害攻撃(Distributed Denial of Service Attack；DDoS 攻撃) の攻撃者を特定する技術として、IP トレースバックが研究開発されている。代表的な IP トレースバック方式には、ICMP 方式[1]、マーキング方式[2]、ハッシュ方式[3]がある。また近年、これらを組み合わせたハイブリッド方式[4][5][6]が提案されている。

IP トレースバック方式は、さまざまな要因のため、完全に攻撃者を特定することはできない。このため、IP トレースバックシステムの信頼性を表す指標として、未検出率 FNR(False Negative Rate)と誤検出率

FPR(False Positive Rate)がある。本論文ではこれらを総称して信頼性と呼ぶ。IP トレースバックの効率的な運用には、IP トレースバックの信頼性の特性を認識する必要がある。従来の研究では、各方式において、攻撃者のトレースバックに必要なパケット数の評価が主に行われてきた[7][8]。

そこで、本研究では、代表的な IP トレースバック方式である、ICMP、マーキング、そして新たに提案されたハイブリット方式（ハッシュ＋新方式）のうち新方式である UDP 方式について、運用時に想定される利用状況下での FNR、FPR の特性を分析する。以後、２章では、IP トレースバックの信頼性について概説する。３章では、各方式における FNR,FPR の数学モデルを定義する。４章では、実測のための検証ネットワークを紹介する。５章では、FNR と FPR の特性が顕著にでる利用状況で、理論値と実測値を比較する。第６章で、まとめと今後の課題を述べる。

２． IP トレースバックの信頼性概説

２．１ IP トレースバックの仕組み

（１）ICMP 方式およびマーキング方式

ICMP およびマーキング方式は、ルータ上でトレースパケットを生成するエージェントと、トレースバック情報を収集するコレクタから構成されている。コレクタが攻撃ルート上のエージェントからのトレースバック情報を収集し、この情報を元にトレースバックを行う。

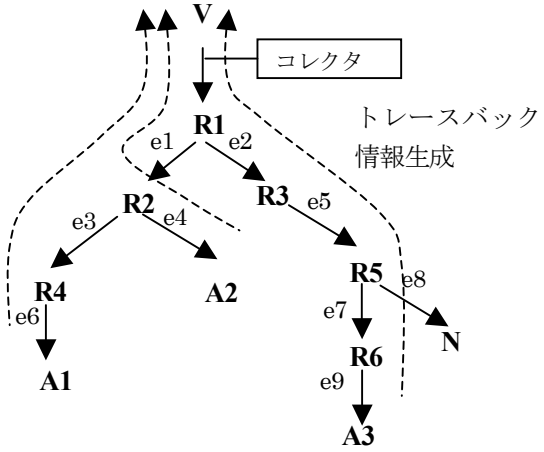

図１．ICMP 方式、マーキング方式の動作例

図１に例を示す。V は被害者、A1,A2,A3 は攻撃者、N は通常の利用者、R1～R6 はルータ、e1～e9 はエッジ（ルータ間のリンク）を示す。攻撃マシンからルータ Ri を経由して、被害者 V を攻撃している。攻撃者 A1 の攻撃パケットは R4,2,1 を経由して被害者 V を攻撃する。R1,2,4 上のエージェントは、エッジ e1,3,6 のトレースバック情報を生成し、被害者 V に送信する。トレースバックシステムは、この情報を元に攻撃者までの経路と攻撃者を特定する。

（２）UDP 方式

本方式は ICMP 方式の改良版であり、各ルータでトレースパケットを生成するエージェントと、トレースバック情報を収集しトレースパスを再構築するマネージャから構成される。ルータ上のエージェントはマネージャが探査パケット情報を設定した後に、エッジに関するトレースバック情報を生成する。

図２に UDP 方式の例を示す。記号などは図１と同一である。まずマネージャは、被害端末に一番近い R1 に探査したいパケット情報を設定する。R1 は設定された攻撃情報に合致するトラヒックが通過した際、マネージャへトレースパケットを送出する。トレースパケットには次に監視すべきルータ情報等が組み込まれている。マネージャでは、R1,2,4 から順次到着するトレースパケットを元に攻撃ルートを再構築し、攻撃者までの経路と攻撃者を特定する。

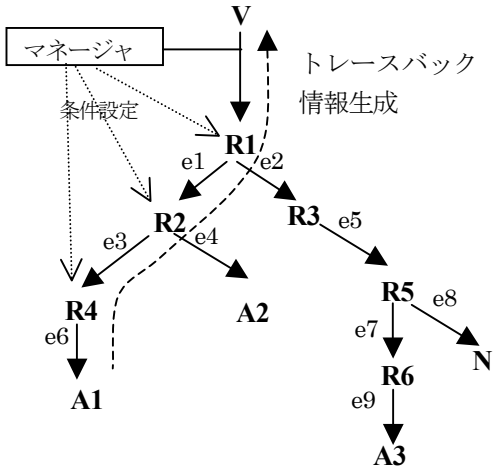

図２．UDP 方式の動作例

２．２ 信頼性指標 FNR,FPR の定義

（１）FNR

未検知率 FNR を式(1)で表す。図１において、任意のトレースバック時間で A1,2 が見つかり、A3 が見つからない場合、FNR は 33%であり式(1)が成立する。

さらに、FNR を攻撃者の発見確率で表現する場合、式(2)で定義できる。攻撃者の発見確率は、被害者から攻撃者に至る経路上に存在する全エッジのトレースバック情報生成確率の積である。この確率は、エ

ッジに流れるパケットの量に依存する。

FNR＝　未知の攻撃者数／全攻撃者数　　(1)
FNR＝　1 - 全攻撃者の発見確率　　(2)

（2）FPR

誤検知率 FPR を式(3)に定義する。図 1 において、任意のトレースバック時間で、A1,2,3,N が全て見つかった場合、FPR は 25%となり式(3)が成立する。

既検知攻撃者数は、任意の時刻にトレースバックシステムが検知した攻撃者数である。その中には誤って検知したものが含まれている。FPR を理論的に扱うために、式(3)の分母、分子を期待値とする。

FNR＝　誤検知攻撃者数／既検知攻撃者数　　(3)
FNR＝　誤検知数の期待値／既検知数の期待値　(4)

２．３　未検知、誤検知の発生要因

3 つのトレース方式に関して、運用時に想定される未検知 FN、誤検知 FP の主な発生要因を表？に示す。未検知要因は 3 つ、誤検知要因は 4 つに分類できた。なお、IP トレースバックシステムのエラー等による要因があるが本稿では考慮しない。

表１．　誤検知の発生要因

分類		要因
未検知要因	a	トレースバック時間が不十分な場合、攻撃経路ルータを攻撃者と見なし、真の攻撃者を検知できない
	b	ネットワーク障害で、リンク断線等のネットワーク障害が発生した時、攻撃者に到達できない
	c	uTraceは攻撃経路上のルータにTimeOut値を設定する。トレースパケット生成前にTime Out値を超えた場合、追跡途中のルータを攻撃者と見なし、真の攻撃者を検知できない
誤検知要因	a	トレースバック時間が不十分な場合、攻撃経路ルータを攻撃者と見なす
	b	攻撃パケットと通常パケットが同じ種類の場合、通常の利用者と攻撃者を区別できないため、通常の利用者を攻撃者と見なす。
	c	マーキングはハッシュ値を用いる。ハッシュの衝突がおきた場合、実際には攻撃していない端末を攻撃者と見なす。
	d	uTraceは攻撃経路上のルータにTimeOut値を設定する。トレースパケット生成前にTime Out値を超えた場合、攻撃経路ルータを攻撃者と見なす

３．　各方式における FNR、FPR の数学モデル

３．１　ICMP 方式

（1）評価システムの処理概要

今回評価した ICMP 方式は、論文[1]で提案されている iTrace である。各ルータを通過するパケットに対して確率 20000 分の 1 で、iTrace パケットを生成する。今回は誤検知を抑えるため、コレクタにて同一ルータから 2 個の iTrace パケットを収集した場合に、エッジを確定することとした。

（2）攻撃者の発見確率と FNR

任意ルータがエッジ ei の iTrace パケットを 2 個生成する確率 Pr(ei)を求める。攻撃パケットが N 個通過した場合、iTrace パケットの生成確率を p とすると、求める確率 Pr(ei)は式(5)となる。ここで、$(1-p)^N$ は 1 個も iTrace パケットを送出しない確率、$Np(1-p)^{N-1}$ は 1 個送出する確率である。

$$Pr(ei)= 1-(Np(1-p)^{N-1}+(1-p)^N) \qquad (5)$$

攻撃者の発見率は攻撃経路の全エッジの生成確率の積で求まるため、FNR は式(6)となる。ここで、m は攻撃ルート上に存在するエッジ数を表す。未検知要因 a は、式(6)で時間的な変化を算出できる。

$$FNR = 1- \prod_{i}^{m} Pr(ei) \qquad (6)$$

（3）FPR

誤検知要因 a,b が該当する。誤検知要因 a については、単一の攻撃ルートに着目した場合、被害者に最も近いルータの発見確率から、攻撃者の発見確率を減算した値が誤検知率となる。複数の攻撃者の誤検知率も、近似解として、最も早く見つかるルータの発見確率から複数の攻撃者の発見確率を減算した値とすることができる。

誤検知要因 b については、誤検知の攻撃者数の期待値は、通常パケットによるエッジのトレース情報生成確率により算出できる。

３．２　マーキング方式

（1）評価システムの処理概要

今回評価したマーキング方式は、論文[9]で提案されている AMS-Ⅱである。各ルータを通過するパケットに対して確率 20 分の 1 で、パケットにハッシュ値をマーキングする。64 ビットのハッシュ値を 8 つのパケットに分割して、パケットにマーキングする。

今回は誤検知を抑えるため、コレクタにて同一ルータから 16 個のマーキングパケットを収集した場合、エッジを確定することとした。

（2）攻撃者発見確率と FNR

攻撃者と被害者の間に d 台のルータがリニアに結ばれているとする。まず、任意のルータ Ri がパケットにマーキングし、他のルータにより書き換えられない確率 F_d を算出する。

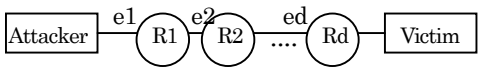

図3.　マーキング方式の数学モデル算出用ルート図

図３において、R1 でエッジ e1 を通過したパケット１個をマーキングし、他のルータでマーキングされない確率は、$p(1-p)^{d-1}$ となる。マーキング値はハッシュ値を 8 分割したうちのランダムに選択された 1 つである。このため、マーキングパケットの生成確率は p/8 となる。よって、求める確率 F_d は式(7)となる。

$$F_d=p(1-p)^{d-1}/8 \qquad (7)$$

さらに、エッジ ei のマーキングパケットが 2 個以上到達する確率 Pr(ei)は、式(7)を用いて式(8)で定義できる。ここで、N は攻撃パケット数、$N*F_d(1-F_d)^{N-1}$ はマークパケット１個の到達確率、$(1-F_d)^N$ はマークパケットが１個も到達しない確率を示す。トレースパスの再構築には、分割された全ハッシュ値を含むパケットが必要なため 8 乗する。未検知要因 a、b については、ICMP 方式と同様に、式(8)を使用して算出できる。

$$Pr(ei)=\left(1-\left(N*F_d(1-F_d)^{N-1}+(1-F_d)^N\right)\right)^8 \qquad (8)$$

（3）FPR

誤検知要因 a,b が該当する。誤検知要因 a,b の算出方法は ICMP 方式と同じである。

３．３　UDP 方式

（1）評価システムの処理概要

今回評価した UDP 方式は、論文[6]で提案されている uTrace である。マネージャは被害端末に一番近いルータへ探査したいパケットの情報を設定する（IDS 等からの攻撃検知情報が元になる）。ルータは設定された攻撃情報に合致するトラヒックが通過した際、マネージャへトレースパケットを送出する。トレースパケットは UDP パケットで、次に監視すべきルータ情報等が組み込まれている。マネージャは、各ルータから順次到着するトレースパケットを元に攻撃ルートを再構築し、攻撃者までの経路と攻撃者を特定する。なお、探査したいパケットの情報とは、プロトコル種別、ポート番号、パケットの送信先等である。

今回は誤検知を抑えるため、エンドノードのエッジ情報を含むトレースパケットに限って、2 個収集した場合に確定することとした。

（2）攻撃者の発見時間と FNR

攻撃者の発見時間 T は式(10)で定義できる。ここで、d は攻撃経路上のルータ数、A は攻撃速度[packets/sec]である。

$$T = (d+1) / A \qquad (10)$$

未検知要因 a は、単一の攻撃ルートを想定した場合、攻撃者を発見する時刻までは FNR=１、それ以降 FNR=0 となる。各ルータのトレースパケット生成時間は式(10)で求まるため、FNR は式(11)、(12)で表すことができる。

なお、未検知要因 b,c は、マネージャからルータへの設定が妨げられるため、攻撃者を発見できない。

$$FNR = 1 \quad (但し、T < (d+1) / A) \qquad (11)$$
$$FNR = 0 \quad (但し、T \geqq (d+1) / A) \qquad (12)$$

（3）FPR

誤検知要因 a,b,e が該当する。誤検知要因 a,e は、未検知要因 a と同様に算出できる。

図 4 の構成で、誤検知要因 b について考える。被害者に 1 番近いルータ R1 を発見するまでは FPR は 0 である。R1 を発見してから、攻撃者に 1 番近いルータ R10 がトレースパケットを 2 つ送出するまで FPR は 1 であり、攻撃者発見時に 0 となる。その後、R11 が発見された時点から FPR は 0.5 を推移し、それ以下には収束しない。図 4 ではトラヒックの合流が発生している為、合流地点（R1～R6）は他よりも発見時間が早くなる。合流地点の発見時間は、式(10)を用いて算出することができる。

４．　検証ネットワーク

４．１　検証ネットワークの構成

（1）検証ネットワーク構築の目的

前述した各トレースバック方式を、実環境に近いネットワークで検証し**信頼性の特性を明らかにする**為に、検証ネットワークを構築した。**なお、本稿では検証環境の一部を使用するにとどまったが、検証環境全体を使用する項目として、ホップ数、攻撃者数等の検証も実施している。**

（2）検証ネットワークの仕様

構築したネットワークと検証用ツールの仕様を、表２、３に示す。少量のマシンで大規模なネットワークを実現する為に、仮想 OS 技術を用いた。検証対象の各レースバックシステムは全て Linux 上で動作する仕様であった為、OS は Linux を、仮想化技術として UML(User Mode Linux)[10]を選択した。

表 2. 検証 NW ネットワークの仕様

ネットワークの特徴		詳細
AS構成		単一AS
NW規模	サーバ	300台
	クライアント	180台
	PCルータ	110台
トポロジ		ツリー、一部メッシュ (ツリー平均分岐数:2.3、平均深さ:5、フルメッシュ)
最大ホップ数		10 (NW構成変更なし、AS間は直列接続)
ルーチングプロトコル		OSPFv3
実装サーバ		NTPサーバ、WWWサーバ
OS		Linux Redhat7.3
仮想化	仮想化技術	User Mode Linux
	仮想端末	クライアント/サーバ端末、一部のPCルータ

表 3. 検証ツール

検証ツール	トラヒック種別	仕様
攻撃トラヒック生成ツール	Synflood	・攻撃速度可変 ・送信元IPアドレス偽装 ・最大25000pps
擬似トラヒック生成ツール	HTTP request	・リクエスト速度可変 ・最大25request/s

５． 検証

５．１ 検証内容

ICMP、マーキング、UDP 方式によって追跡検知される容疑者は、常に正しいとは限らない。これは攻撃パケット種別と通常パケット種別が同一な場合、前述の各方式ではそれらを区別できないためである。そこで、今回の検証では、攻撃パケットと通常パケットが混在した条件下における FNR、FPR を測定することとした。

５．２ 検証条件

検証ネットワーク構成を図５、検証条件を表４に示す。通常トラヒックとして HTTPRequest を使用する。通常パケット量の括弧内に記述した数字は、１HTTPRequest 中の syn パケット数を示す。

なお、ICMP 方式のトレースバック情報生成確率の推奨値は 1/20,000 であるが、測定時間を短縮するために、1/2,000 とした。

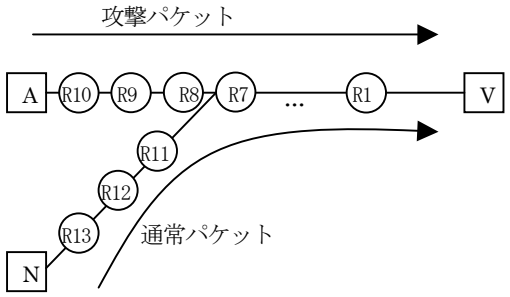

図 4. 攻撃、通常パケットの混在のNW構成

表 4. 検証条件

方式名		ICMP	ﾏｰｷﾝｸﾞ	uTrace
ﾄﾚｰｽﾊﾞｯｸ情報生成確率		1/2000	1/20	–
ﾊﾟｹｯﾄ比率 50%	攻撃ﾊﾟｹｯﾄ量	70pps	25pps	25pps
	通常ﾊﾟｹｯﾄ量	70(10)pps	25(3)pps	25(3)pps
測定回数		3回	60回	50回

（2）FNR の分析

ICMP、マーキング、UDP 方式の FNR の理論値(Teory)と実測値(Measurement)を図５に示す（通常トラヒック割合は 50%)。

ICMP、マーキング方式では、攻撃トラヒックの syn パケット数により攻撃者の発見確率が決まる。攻撃トラヒックと通常トラヒックが合流するルータでは、それぞれのトラヒック中の syn パケット合計数によりトレースバック情報生成確率が決まる。UDP 方式でも同様の方法で、攻撃者、攻撃経路上の各ルータの発見時間が決まる。

マーキング、UDP はほぼ理論通りの推移することが確認できる。一方、ICMP は予測より早い時刻で FNR が 0 に収束している。これは、ICMP の試行回数が少なく、各試行とも理論時に想定していた確率よりも高い確率でトレースパケットが生成された為と考えられる。試行回数を増やし、確率の影響を減らすことで、理論値と同等の結果を得られると予測できる。

（3）FPR の分析

ICMP、マーキング、UDP 方式の理論値と実測値を図６に示す。

ICMP、マーキング方式は、攻撃者 A を発見するまでの時間に、途中のルータを攻撃者として誤検知する。攻撃者の発見確率が増加するに伴い、FPR は一旦減少する。しかし、攻撃者 A を発見した後、通常パケットの中の syn パケットを攻撃パケットと見なし通常利用者 N に至るルータ NR を攻撃者とみなす。NR の発見確率が増加するとともに、FPR が増加していく。UDP 方式でも同様に、攻撃経路上の各ルータの発見時間から FPR が決定する。

マーキング、UDP はほぼ理論通りの推移することが確認できる。一方、ICMP は予測に反しマーキングと同等の推移が見られた。これは、前述した FNR 収束の速さと同じ要因と考えられる。各方式を比較すると、UDP が他の 2 方式に比べ格段に早い時刻で誤検知のピーク（FPR=1）に達することが分かる。

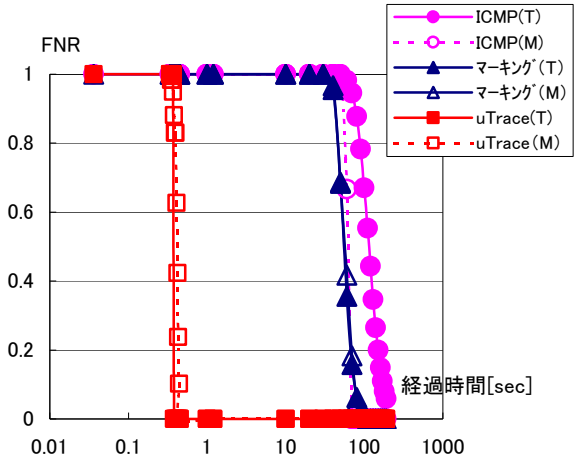

図 5. パケット混合による FNR

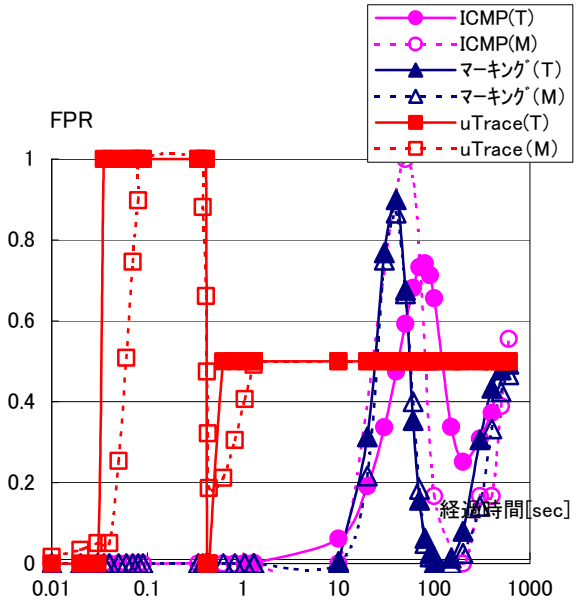

図 6. パケット混合による FPR

6. まとめと今後の課題

ICMP、マーキング方式の攻撃者の発見確率、UDP 方式の攻撃者の発見時間を基に、FNR, FPR の数学モデルを提案した。数学モデルの妥当性については、運用時に想定されるトラヒック混合環境において、FNR, FPR を測定し、数学モデルによる理論値と実測値がほぼ一致していることを確認した。本稿で提案した数学モデルにより FNR, FPR の定量的な予測、特性の検討が可能となった。

今回提示した数学モデルは単一トポロジに対応するモデルであり、今後、多様なトポロジに対応できるモデルを検討する必要がある。

本稿では、単一の AS を想定した検証環境において各方式の評価を行ったが、現在、複数の AS（AS9、ノード 1100）から構成される検証環境を構築し、ハイブリッド方式の評価を実施中である。

参考文献

[1]StevenM. Bellovin, "ICMPTraceback Message", InternetDraft:draft-vellovin-itrace-00.txt, submitted Mar. 2000

[2]S. Savage et al., "Practical Network Support for IP Traceback", Proc. of the ACM SIGCOMM conference, Aug. 2000, Stockholm, Sweden

[3]Alex C. Snoeren et al., "Hash-Based IP Traceback", Proc. of the ACM SIGCOMM 2001 Conf. , SanDiego, CA, Oct. 2001

[4]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

[5]甲斐俊文 他, "DDoS 攻撃に対する高性能発信源探査方式の提案", インターネットコンファレンス 2004 論文集, pp111-118, Oct. 2004

[6]甲斐俊文 他, "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 CSEC 研究会, 2004

[7]Vadim Kuznetsov et al., "An evaluation of differentIPtracebackapproaches", ICICS, 2002

[8]**大江将史 他**, "階層化 IP トレースバック機構の実装と検証", 電子情報通信学会論文誌, vol. J86-B, no. 8, pp. 1486-1493, Aug. 2003

[9]D. Song et al., "Advanced and Authenticated Marking Schemes for IP Traceback" Proc. IEEE INFO-COM, Apr. 2001

[10]http://user-node-linux.sourceforge.net

(注)本研究は、情報通信研究機構からの委託(H14～H16 年度)により実施している。