2-7 IPトレースバックシステムの数学モデルと実証実験

2-7 The Mathematics Models and an Actual Proof Experiment for IP Traceback System

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
SUZUKI Ayako, OHMORI Keisuke, MATSUSHIMA Ryu, KAWABATA Mariko,
OHMURO Manabu, KAI Toshifumi, and NISHIYAMA Shigeru

要旨

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。IPトレースバックシステムの性能は、主に、トレース時間とトレース結果の誤り率によって評価できる。本論文では、代表的なIPトレースバック方式であるICMP方式、IPPM方式、Hash方式、新たに提案されているUDP方式、AS間トレースバック方式の数学モデルを提案し、トレースバック時間の予測を行う。また、誤検知率を信頼性の指標とし、信頼性特性を分析する。そして、実際の大規模検証ネットワークを使用した実測により、予測の妥当性を裏付ける。

IP traceback is a technique that searches DDoS attackers. There are many kinds of IP traceback methods. The performance of IP traceback system can mainly evaluate using a trace time and the error rate of the trace result. In this paper, we propose mathematical models of typical IP traceback methods, which are ICMP, IPPM, Hash, and an UDP and AS traceback method newly proposed. And, we estimate the time required to trace. And, we analyze reliability features of these. False positive rate are evaluation parameters of the reliability. And, we analyze mathematical models. Then we compare the predicted value with the measured values using the actual large network for verification.

[キーワード]
IPトレースバック，AS間トレースバック，UDP方式，数学モデル，FPR分析
IP traceback, Inter AS (Autonomous System) traceback, An UDP method, Mathematical models, Analysis of FPR (False Positive Rate)

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AS内IPトレースバック方式には、ICMP方式[1]、IPPM方式[2]、Hash方式[3]があり、近年、これらを組み合わせたハイブリッド方式（Hash＋新方式のUDP）[4]－[6]が提案されている。また、AS内トレースバックを連携してAS間をトレースバックする技術も提案されている[7]。

IPトレースバックシステムの性能は、主に、トレース時間とトレース結果の誤り率によって評価できる。誤り率とは、IPトレースバック方式が様々な要因のため、完全に攻撃者を特定することができないことに起因する。誤り率を表す指標として、誤検出率FPR（False Positive Rate）がある。本論文ではこれを信頼性指標と呼ぶ。IPトレースバックの効率的な運用には、IPトレースバックのトレース時間、信頼性特性を認識する必要がある。

そこで、本研究では、ICMP、IPPM、Hash、UDP、AS 間トレースバック方式について、それぞれのトレースバック時間の数学モデルを提案する。また、運用時に想定される利用状況下での FPR の特性を分析する。なお、数学モデルを検証するため、大規模な検証ネットワークでの実測値と比較し、数学モデルの妥当性を得ることができた。以後、**2** では、AS 内、AS 間トレースバックの仕組みと、FPR について概説する。**3** では、各方式における数学モデルを定義する。**4** では、実測のための検証環境の紹介、トレースバック時間の予測と実測比較、FPR 分析を報告する。**5** をまとめとする。

2 IP トレースバック

2.1 IP トレースバックの仕組み

IP トレースバックシステムは、攻撃の発信源を探査するシステムであり、一般的には単一 AS 内を探査する方法である。しかし、DDoS 攻撃では通常、攻撃パケットは複数 AS を通過して犠牲者まで達する。複数 AS で探査を行う場合、AS 内探査とは別に AS 間を連携する仕掛けが必要である[7]。ここでは、前者を AS 内トレースバック、後者を AS 間トレースバックと呼ぶこととする。

2.1.1 AS 内トレースバック

AS 内 IP トレースバックの代表的な方式には、ICMP 方式、IPPM 方式、Hash方式がある。

ICMP 方式、IPPM 方式は、攻撃パケットに対して、確率的にトレースバック情報を生成する。このため、攻撃者のトレースバックパス確定は確率的になり、攻撃者の発見確率は、攻撃ルートの各エッジに関するトレースバック情報の生成確率から算出できる。

Hash 方式は、各ルータのエージェントが、到着するパケットごとに、HASH値を設定する。マネージャから攻撃パケットが通過したか問い合わせてトレースバックパスを設定する。このため、トレースバック時間は、マネージャからの問い合わせ回数に依存する。

今回提案する UDP 方式は、攻撃パケットが通過したら報告するように近傍のルータに依頼をかけ、攻撃パケットが通過したルータに対し、同じ処理を繰り返す。

2.1.2 AS 間トレースバック

異なる AS 内トレースバックが実装された AS 間で連携探査する方式として、境界探査と内部探査が提案されている。境界探査は AS の境界ルータのみを対象とし、内部探査は AS 内の全ルータを対象に探査する。境界探査と内部探査を有効に組み合わせれば、高速なトレースバックが可能となる。図 1 に境界探査と内部探査の概要を示す。

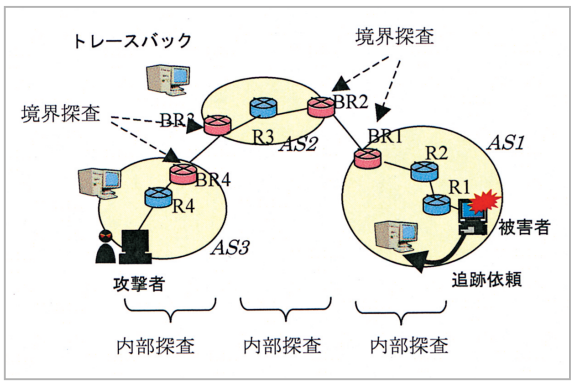

図1 境界探査と内部探査の概要

2.2 信頼性指標 FPR の定義

誤検知率 FPR を式(1)に定義する。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 を予測的に扱うために、式(1)の分母、分子を期待値とする。

FPR＝誤検知攻撃者数／既検知攻撃者数　(1)

FPR＝誤検知数の期待値／既検知数の期待値　(2)

2.3 誤検知率 FPR の発生要因

三つのトレース方式に関して、運用時に想定される誤検知 FP の主な発生要因を表 1 に示す。誤検知要因は四つに分類できる。なお、IP トレースバックシステムのエラー等による要因も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
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	IPPM、HASH方式はHASH値を用いる。HASH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	UDP方式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　数学モデル

3.1　AS 内トレースバックシステム

3.1.1　ICMP 方式

⑴　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。

⑵　攻撃者の発見確率

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(3)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。

$$Pr(ei) = 1-(Np(1-p)^{N-1} + (1-p)^N) \quad (3)$$

⑶　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。

3.1.2　IPPM 方式

⑴　評価システムの処理概要

今回評価した IPPM 方式は、論文[8]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 HASH 値をマーキングする。64 ビットの HASH 値を八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。

⑵　攻撃者発見確率

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。

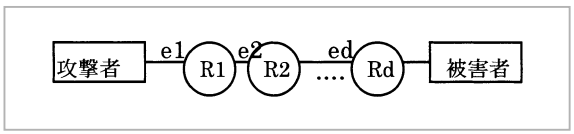

図2　IPPM 方式の数学モデル算出用ルート図

図 2 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 HASH 値を 8 分割したうちのランダムに選択された一つである。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(4)となる。

$$F_d = p(1-p)^{d-1}/8 \quad (4)$$

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(5)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 HASH 値を含むパケットが必要なため 8 乗する。

$$Pr(ei) = (1-(N*F_d(1-F_d)^{N-1} + (1-F_d)^N))^8 \quad (5)$$

(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。

3.1.3 Hash 方式

(1) 評価システムの処理概要

今回評価した Hash 方式は、論文[3]で提案されている SPIE である。各ルータのエージェントが、到着するパケットごとに、HASH 値を設定する。マネージャは、各ルータのエージェントに攻撃パケットが通過したか問い合わせてトレースバックを行う。今回は、HASH サイズが 14 ビットの Hash 方式システムを評価対象とした。

(2) 攻撃者発見確率

攻撃者の発見時間 T は式(6)で定義できる。ここで、n はマネージャが各ルータのエージェントへの問い合わせ総回数。回帰分析により、近似式を求めた。

$$T = 0.004n + 1.2841 \quad (6)$$

(3) FPR

誤検知要因 c が該当するが、今回は評価対象外とした。

3.1.4 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フィックが通過した際、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

攻撃者の発見時間 T は式(7)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。

$$T = \sum_{i}^{hop-1} \frac{1}{Ai} + \frac{2}{Ae} \quad (7)$$

(3) FPR

誤検知要因 a、b、e が該当する。図 7 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二つ送出するまで 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 ではトラフィックの合流が発生しているため、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(7)を用いて算出することができる。

表 2 に、AS 内トレースバック各方式のトレースバック時間の数学モデルをまとめた。

3.2 AS 間トレースバックシステム

通常の DDoS 攻撃の場合、攻撃パケットは、複数 AS を通過して犠牲者まで達する。攻撃者を特定するには、それぞれの AS を管理している ISP 間の連携が必要となる。このような AS 間を連携支援する機能として、境界探査と内部探査が提案されている。境界探査は AS の境界ルータのみを対象に探査し、内部探査は AS 内の全ルータを探査する。境界探索と内部探査を有効に組み合わせれば、高速なトレースバックが可能となる。

探査方法は AS ごとに指定可能である。連携システムの探査順序は境界→内部であり、探査は各 AS で独立して動作可能である。よって、攻撃者を特定する場合、AS1 境界探査→ AS2 境界探査→ AS3 境界探査→ AS3 内部探査の順に探査が行われる。境界探査時間は AS 数分加算さ

表2　AS内トレースバック時間の数学モデル

方式	数学モデル
ICMP	$Pr(ei) = 1-(Np(1-p)^{N-1}+(1-p)^{N})$ $Pr(\prod Aj) = \prod Pr(ei)$ ここで、pは各エッジでのiTraceパケットの生成確率、Nは攻撃パケット数。 パケット数を変化させ、確率が95%になるトレースバック時間を算出する。
PPM	$F_d=p(1-p)^{d-1}/8$ $Pr(ei) = (1-(N*F_d(1-F_d)^{N-1}+(1-F_d)^{N}))^{8}$ $Pr(\prod Aj) = \prod Pr(ei)$ ここで、pは各エッジでのiTraceパケットの生成確率、Nは攻撃パケット数、dは犠牲者からのホップ数。 パケット数を変化させ、確率が95%になるトレースバック時間を算出する。
Hash	$T = 0.004n+1.2841$ ここで、nはマネージャが各ルータのエージェントへの問い合わせ総回数。 回帰分析により、近似式を求めた。
UDP	$T = \sum_{i}^{hop-1}\frac{1}{Ai}+\frac{2}{Ae}$ ここで、Aiは、各エッジの平均攻撃パケット量、hopは、攻撃パスの中で、最長のホップ数。Aeは、攻撃端末の平均攻撃パケット量。最長ホップ数の攻撃パスのトレースバック時間から算出する。 境界探査の場合、境界ルータに対して適用できる。

れ、内部探査時間は攻撃者の存在するAS数でだけ加算される。

複数の攻撃者をトレースバックする場合、その処理は、並列に行われるため、トレースバック時間Tは、最長ホップASの攻撃者のトレースバック時間に依存する。内部探査にUDP方式を用いた場合、トレースバック時間Tは式(8)で定義できる。

T＝MAX(ASnの内部探査完了時間)
＝MAX(ASnまでの境界探査時間＋ASnの内部探査時間)

$$=\frac{1}{Aj}+\sum_{i}^{hop-1}k\times\frac{1}{Ai}+\frac{2}{Ae} \qquad (8)$$

ここで、Ajは境界ルータの各エッジの平均攻撃パケット量、Aiは各エッジの平均攻撃パケット量、hopはAS内攻撃ルートのうち最長ホップのルータ数、Aeは攻撃端末の平均攻撃パケット量である。kは攻撃ルートが合流した場合2とし、合流がない場合1とする。

4　実証実験

4.1　検証環境の構成

(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

表3　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4 検証ツール

検証ツール	構成	トラヒック種別	仕様
攻撃トラヒック生成ツール	マネージャ 攻撃トラヒック擬似端末	Synflood	・攻撃速度、攻撃時間可変 ・送信元IPアドレス偽装 ・最大25000pps ・最大10pps(仮想)
擬似トラヒック生成ツール	マネージャ 正常トラヒック擬似端末	HTTP request	・リクエスト速度可変 ・最大25request/s

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ために、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3、4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ために、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すべてLinux上で動作する仕様であったため、OSはLinuxを、仮想化技術としてUML(User Mode Linux)[9]を選択した。

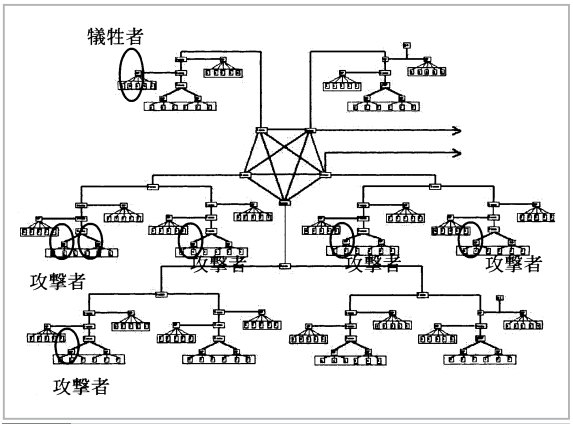

図3 AS内トレースバックの検証NW構成

表5 AS内トレースバックの検証条件

方式	攻撃者数	攻撃者数×攻撃量	試行回数
ICMP	1, 10, 20, 50, 100	25000pps	10
PPM	同上	1000pps	60
Hash	1, 10, 25, 50, 100	50pps	5
UDP	10, 20, 50, 100	100pps	60

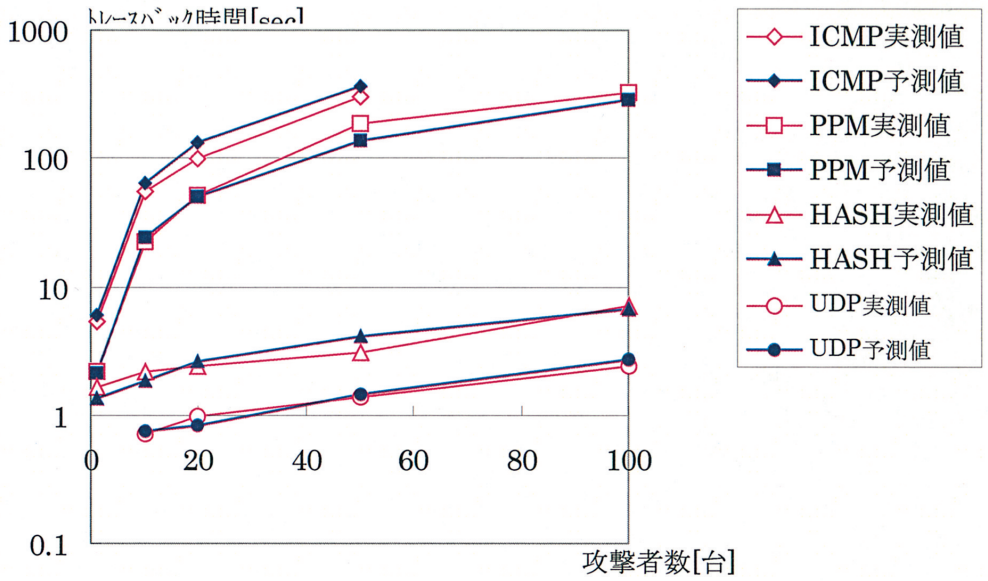

図4 AS内トレースバックのトレースバック時間

4.2 検証結果

4.2.1 トレース時間

(1) AS 内トレース

A）検証内容

攻撃者数を変化させて、トレースバック時間を測定した。

B）検証条件

攻撃者数は、1、10、20、50、100 台とした。今回の評価では、犠牲者の地点での攻撃速度を一定とした。

測定条件を表 5 に、検証NWの構成を図 3 に示す。

C）結果

測定結果を図 4 に示す。実測値と予測値がほぼ一致していること、提案している UDP 方式は他方式に比べて、短い時間でトレースバックができることが明らかになった。ICMP 方式の 100 台に関しては、測定時間制限 10 分を設けており、それ以上となったため、実測値を示していない。

(2) AS 間トレース

A）検証内容

AS 数、攻撃者数、トポロジを変化させて、トレースバック時間を測定した。

B）検証条件

今回の評価では､攻撃者1台の攻撃速度を 10pps で一定とした。測定条件、ネットワーク構成を図 5 に示す。

C）結果

検証結果を図 6 に示す。実測値と理論値がほぼ一致していること、トレース時間は被害者と攻撃者間の最大ホップ数によって決定され、トポロジや攻撃数には影響されないことが明らかになった。

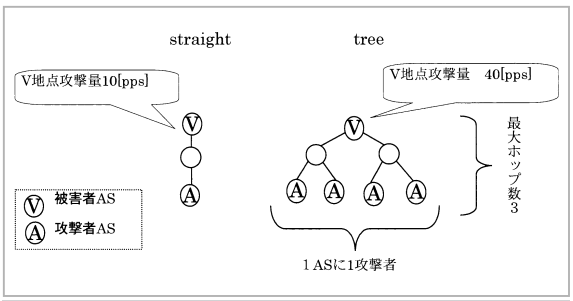

図5 AS 間トレースバックの検証条件、検証 NW 構成

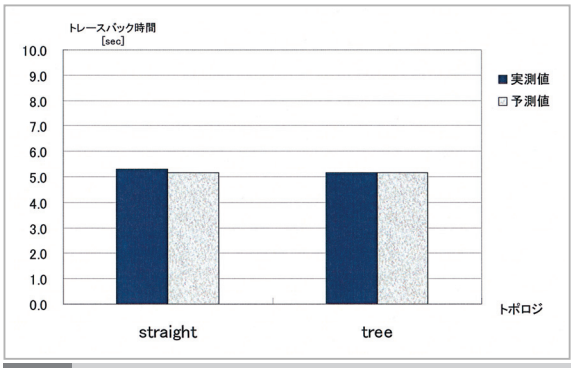

図6 AS 間トレースバックのトレースバック時間

4.2.2 誤り率

A）検証目的

IP トレースバックによって追跡検知される容疑者は、常に攻撃者であるとは限らない。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、十分な時間が経過すれば、パケットにより攻撃者と通常利用者の区別ができないためである。

このため、攻撃パケットと通常パケットの量により、攻撃端末を識別できる可能性を検証した。

B）検証条件

攻撃パケットと通常パケットの比率を変えて、攻撃パケット量により、FPR(False Positive Rate)を検証する。比率は、攻撃パケット割合：通常パケット割合を 50 %：50 %と、10 %：90 %の 2 パターンとした。また、比較する方式は IPPM 方式と UDP 方式とした。なお、図 7 の構成で FPR の推移を測定した。測定条件を表 6 に示す。

C）結果

測定結果を、図 8 に示す。測定結果より、UDP は容疑者の特定が早い反面、攻撃者と通常利用者を攻撃流量やパケット比率で区別することが難しいことが分かる。一方、IPPM は、UDP に比べトレース時間は要するが、攻撃流量、パケット比率の差が FPR に顕著に現れることが分かる。

よって、UDP において FPR を低く抑え、容疑率を高めるためには、閾値を現状の 2 から更に大きく設定する必要があると考える。また、IPPM は、攻撃速度が比較的高速な DDoS 攻撃の場合、攻撃時間を絞ることができれば、FPR

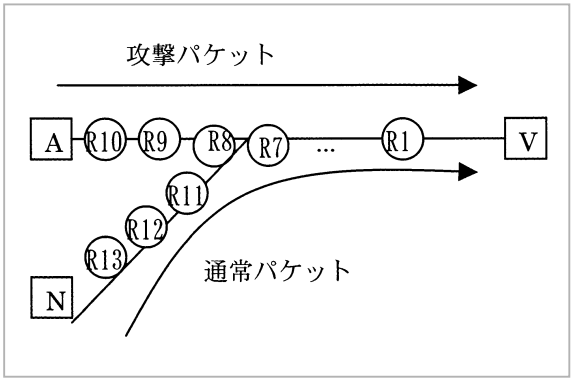

図7 攻撃、通常トラフィック混在の検証 NW 構成

表6 攻撃、通常トラフィック混在の検証条件

		IPPM	UDP
ﾄﾚｰｽﾊﾞｯｸ情報生成確率		1/20	–
通常ﾊﾟｹｯﾄ比率 50%	攻撃ﾊﾟｹｯﾄ量	25pps	25pps
	通常ﾊﾟｹｯﾄ量	25(3)pps	25(3)pps
通常ﾊﾟｹｯﾄ比 90%	攻撃ﾊﾟｹｯﾄ量	5pps	5pps
	通常ﾊﾟｹｯﾄ量	45(9)pps	45(9)pps

() 内は、通常パケット内の SYN パケット数

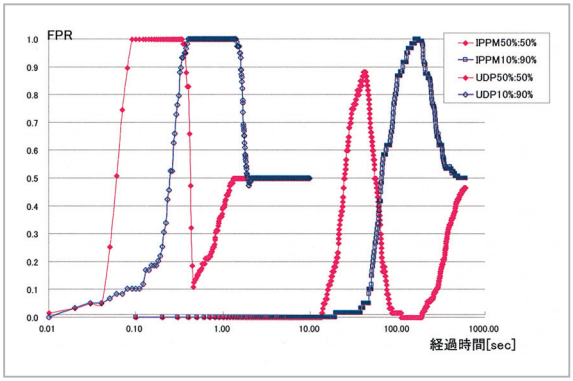

図8 FPR の推移

を下げることが可能と予測される。

D）運用時の提案

トレースシステムの FPR 検証より、以下の 3 点を提案する。

・リアルタイムに Synflood 計測を行い、通常時と攻撃時の区別を判別できるようにする。

・上記により、攻撃が判明したら、トレースシステムにより容疑者リストを生成する。

・容疑者リストを定期的に生成し（例えば攻撃時は毎秒）、常にリストアップされるノードの容疑率を高く設定する。

5 むすび

AS 内トレースバック方式の各方式、ICMP、IPPM、Hash、UDPと、AS 間トレースバック方式について、それぞれのトレースバック時間の数学モデルを提案し、それらを元に、複数攻撃者のトレースバック時間の予測を行った。また、実証実験により実測値を計測し予測値との比較を行った。その結果、AS 内トレースバックでは、実測値と予測値がほぼ一致すること、提案している UDP 方式は他方式に比べて、短い時間でトレースバックができることが明らかになった。AS 間トレースバックは、実測値と予測値がほぼ一致していること、トレース時間は被害者と攻撃者間の最大ホップ数によって決定され、トポロジや攻撃数には影響されないことが明らかになった。

さらに、攻撃トラフィックにノーマルトラフィックが混在する環境における信頼性特性 FPR を分析した。対象は、UDP 方式と IPPM 方式である。その結果、UDP 方式において FPR を低く抑え、容疑率を高めるためには、閾値を現状の 2 から更に大きく設定する必要があること、また IPPM は、攻撃速度が比較的高速な DDoS 攻撃の場合、攻撃時間を絞ることができれば、FPR を下げることが可能と予測できることが分かった。

本稿で提案した数学モデルによりトレースバック時間の予測が可能となり、信頼性指標 FPR の分析より信頼性特性が明らかになった。

謝辞

本研究は、独立行政法人情報通信研究機構における委託研究テーマ「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」によっている。ここに記して謝意を表す。

参考文献

1 StevenM. Bellovin, "ICMPTracebackMessage", 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, Stockholm, Sweden, Aug. 2000.
3 Alex C. Snoeren et al., "Hash-Based IP Traceback", Proc. of the ACM SIGCOMM 2001 Conf., SanDiego, CA, Oct. 2001.
4 福田尚弘ほか，“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 甲斐俊文ほか，“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，pp.111-118，Oct. 2004.
6 甲斐俊文ほか，“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 甲斐ほか，“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.
8 D. Song et al., "Advanced and Authenticated Marking Schemes for IP Trace back", Proc. IEEE INFO-COM, Apr. 2001.
9 http://user-node-linux.sourceforge.net

鈴木彩子（すずきあやこ）
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
ネットワークセキュリティ

大森圭祐（おおもりけいすけ）
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
ネットワークセキュリティ

松嶋　竜（まつしま　りゅう）
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
ネットワークセキュリティ

川端まり子（かわばたまりこ）
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
ネットワークセキュリティ

大室　学（おおむろ　まなぶ）
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
ネットワークセキュリティ

甲斐俊文（かい としふみ）
松下電工株式会社先行技術開発研究所ネットワークセキュリティ

西山　茂（にしやま　しげる）
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担当部長
ネットワークセキュリティ