IPトレースバックの数学モデルと検証

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[*]

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、IPトレースバック技術がある。IPトレースバック方式は各種方式が提案されている。新しい方式の検討にあたっては、従来方式との性能比較が必要である。本論文では、ICMP、IPマーキング、ハッシュ方式の数学モデルを提案する。提案する数学モデルは、任意のネットワークトポロジに適用でき、新しい方式の性能評価に利用できる。数学モデルは、約600ノードの検証ネットワークでの実測値と比較することで検証した。

Mathematical Models of IP Traceback Systems and their Verification

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

Abstract IP traceback is the technology to specify DDoS (Distributed Denial of Service) attackers. Various IP traceback systems have been proposed. When a new system is developed, performance comparison with the conventional system is necessary. In this paper, the mathematical models of ICMP, IP marking, and hash system are proposed. The mathematical models to propose can be applied to arbitrary network topology, and can be used for a performance evaluation of a new system. The mathematical models is verified by comparing them with the actual measurement value on the verification network of about 600 nodes.

1. まえがき

分散型サービス妨害攻撃 (Distributed Denial of Service Attack ; DDoS攻撃) は、ワームやウィルスを利用して猛威を振るっている。このようなセキュリティ侵害への対処方法や再発防止などの対策を行うことを可能にするセキュリティ運用の仕組みの研究開発が急務であるとの認識も高まってきている。

ＩＰトレースバックは、送信元が偽造した攻撃パケットの転送経路を特定することができ、DDoS攻撃に対して、極めて有効な手段であると考えられている。代表的なＩＰトレースバック方式には、ICMP方式[1]、IPマーキング方式[2]、 ハッシュ方式[3]がある。また、これらを組み合わせたハイブリッド方式[4]も提案されている。

ＩＰトレースバック方式の性能を評価する方法としては、数学モデルによる方法[5]、ネットワークシミュレータ、ネットワークによる方法[6]がある。

新しい方式を検討する場合、従来の代表的なIPトレースバック方式の性能評価が必要となる。従来方式のＩＰトレースバックシステムを稼動させて、性能評価するのが理想的だが、現実的には困難を伴う。このため、現実的には、数学モデルによる性能推定が有効に

* 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 システム開発ユニット
+ NTT Advanced Technology Corp, Core Networks Bussiness Headquarters System Development Unit
** 松下電工株式会社 システム技術研究所
++ Matsusita Electric Works, Ltd. Systems Technology Research Laboratory

なる。従来の数学モデルによる方法は、解析的な手法を用いてリニアや2分木等の簡単なトポロジに対して分析しており、任意のネットワークトポロジに適用できなかった。

そこで、本研究では、代表的なトレースバック方式であるICMP方式、IPマーキング方式、ハッシュ方式について、任意のネットワークトポロジに適用可能な数学モデルを提案する。また、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た。

以後、2章では、IPトレースバックの数学モデル、3章では、検証方法と検証ネットワーク、4章では実測と理論値の比較、5章では、まとめと今後の課題を述べる。

2. IPトレースバックの数学モデル

2.1 IPトレースバックの概要

まず、IPトレースバックの概要を説明する。IPトレースバックは、DDoS攻撃を受けている犠牲者から、分散している攻撃者を特定する。IPトレースバックシステムは、各ルータに配備され、攻撃パケットがどのルータを通過したかを示すトレースバック情報を生成する。これらのトレースバック情報は、コレクタに蓄えられ、これらの情報を元にトレースバックする。

図1にトレースバックの例を示す。Vは犠牲者、A1, A2, A3, A4は攻撃者を示す。攻撃者A1, A2, A3, A4は、ルータR1からR6を経由して、犠牲者Vを攻撃している。例えば、攻撃者A1の攻撃パケットは、ルータ間のエッジe6, e3, e1を経由して犠牲者に到達しているため、攻撃者A1を特定するためには、e1, e3, e6に関するトレースバック情報が生成されているとトレースバックが可能となる。

ICMPトレースバック方式、IPマーキング方式は、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。例えば、A1, A2, A3, A4の攻撃者4人の発見確率 $Pr(A1 \cap A2 \cap A3 \cap A4)$ は、犠牲者から4人の攻撃者に至る各エッジのトレースバック情報生成確率 $Pr(ei)$ から、式(1)より求めることができる。

$$Pr(A1 \cap A2 \cap A3 \cap A4) = \prod_{i=1}^{9} Pr(ei) \qquad (1)$$

ハッシュ方式は、各ルータのエージェントが、到着するパケット毎に、ハッシュ値を設定する。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。ICMP方式、IPマーキング方式のように確率的にトレースバック情報を出す方式とは異なる。

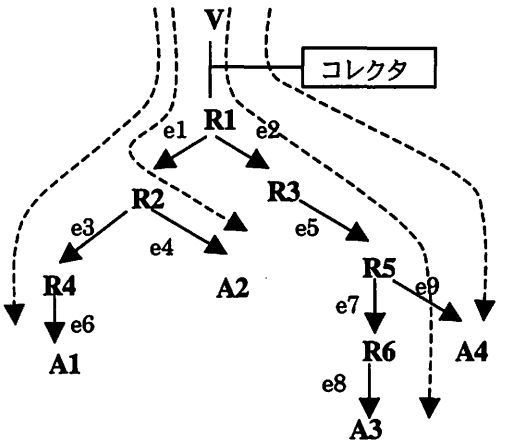

図1. IPトレースバックの例

2.2 IPトレースバックの数学モデル

(1) ICMP方式

(a) 方式概要

各ルータにトレースバック情報を生成するエージェントと犠牲者の直前にトレースバック情報を収集するコレクタを配備する。エージェントは、到着するパケットに対してある確率p(通常は20000分の1)で、トレースバック情報であるiTraceパケットを生成する。コレクタは、iTraceパケットを元にトレースバックを実施する。

(b) 評価システム

通常のICMP方式のトレースバックシステムでは、1個のiTraceパケットでトレースバックを実施する。今回、評価したICMP方式のトレースバックシステムでは、誤検知を少なくするため、2個のiTraceパケットが来た場合、該当エッジのトレースバックが可能となる。

(c) 数学モデル

ルータRkのエージェントがiTraceパケットを2個生成する確率を求める。エッジeiに関するiTraceパケットの生成確率がpで、かつ攻撃パケットがN個パ

ケットきた場合、iTrace パケットを２個以上出す確率は、式(2)となる。

$$Pr(ei) = 1-(Np(1-p)^{N-1}+(1-p)^{N}) \quad (2)$$

ここで、$(1-p)^{N}$ は１個も Trace パケットを出さない確率であり、$Np(1-p)^{N-1}$ は１個の iTrace パケットしか出さない確率である。

全ての攻撃者の発見確率 $Pr(\Pi\ Aj)$ は、攻撃ルートのエッジ ei のトレースバック情報生成確率を使用して、式(3)により求まる。任意の発見確率を求める場合、パケット数の値を変化させ、任意の発見確率になるパケット数を算出する。

$$Pr(\prod_{j=1}^{n} Aj) = \prod_{i=1}^{m} Pr(ei) \quad (3)$$

トレースバック時間は、式(3)で求めたパケット数より算出する。

(d) 適用例

図１に、式(2)、式(3)を使用した例を以下に示す。以下の例では、式(2)を F(N) とする。

図１において、A1, A2, A3, A4 が攻撃パケット量 a (packets/sec) で、DDoS 攻撃を実施しているとする。t 秒後の攻撃者の発見確率算出方法を表１に示す。ここで、(2)式を e1, e2, e5 に流れるパケット量は、合流するため２倍になる。

表１．ICMP 方式の攻撃者の発見確率算出例

エッジ	t 秒後の通過パケット数	各エッジ２個の iTrace 生成確率
e1, e2, e5	2at	F(2at)
e3, e4, e6, e7, e8	at	F(at)
攻撃者 A1, A2, A3, A4 の発見確率		$F(2at)^{3}*F(at)^{5}$

表１で算出した攻撃者 A1, A2, A3, A4 の発見確率に基づきトレースバック時間を算出してみる。例えば、攻撃者の攻撃パケット量は、全て 1000 (packets/sec) とする。発見確率 95%のトレースバック時間はパケット数を変動させて求める。攻撃者 A1, A2, A3, A4 の発見確率が 95%になるトレースバック時間は 96 秒である。

（２）IP マーキング方式

(a) 方式概要

各ルータに通過パケットにマーキングするエージェントを、犠牲者の直前にマークパケットを収集するコレクタを配備する。各ルータで、通過パケットに対してある確率 p（通常は 20 分の１）で、パケットにハッシュ値をマーキングする。コレクタは犠牲者宛てのマークパケットを元にトレースバックパスを算出する。

(b) 評価システム

今回評価した IP マーキング方式システムは、64 ビットのハッシュ値を 8 つに分割し、そのうちの 1 つをランダムに選択してマーキングする。コレクタは、2 回、64 ビットのハッシュ値 (16 個のマーキングパケット) が揃った場合、該当エッジのトレースバックが可能となる。

(c) 数学モデル

攻撃者と犠牲者の間に 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 がパケットにマークし、他のルータにより書き換えられない確率を算出する。

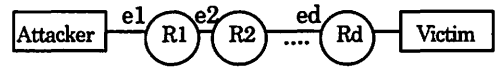

図２．　IP マーキング方式の数学モデル算出用

図２において、R1 でパケット１個をマークし、他のルータでマークされない確率は、$p(1-p)^{d-1}$ となる。ハッシュ値をフラグメントにより 8 分割し、その内の１個をランダムに送出する。このため、マークパケットの生成確率が p/8 となり、１個のマークを生成し、他のルータで書き換えられない確率 F_d は式(4)となる。

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

エッジ ei に対する、フラグメントにより 8 分割したマークパケットが、２個以上到達する確率 Pr(ei) は式(5)となる。

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

ここで、N はパケット数、$N*F_d(1-F_d)^{N-1}$ 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。１から 2 つの値を引くこと

で、マークパケットが2個以上到達する確率を示す。トレースバックには、フラグメントされた8個のパケットが必要なため、8乗している。

任意の攻撃者の発見確率、攻撃トレースバック時間は、ICMP方式と同様に式(3)で求めることができる。

(d) 適用例

図1に、式(5)、式(3)を使用した例を以下に示す。以下の例では、式(5)をG(d, N)とする。ICMP方式との違いは、マーキングするルータと被害者間にあるルータがマークパケットを書き換える場合があるため、ルータの台数dを考慮する必要があるという点である。

A1, A2, A3, A4が攻撃パケット量a(packets/sec)で、DDoS攻撃を実施しているとする。t秒後の攻撃者の発見確率算出方法を表2に示す。

表2．IPマーキング方式の攻撃者の発見確率算出例

エッジ	d	t秒後の通過パケット数	各エッジ2個のiTrace生成確率
e1, e2	1	2at	G(1, 2at)
e5	2	2at	G(2, 2at)
e3, e4	2	at	G(2, at)
e6, e7, e9	3	at	G(3, at)
e8	4	at	G(4, at)
攻撃者A1, A2, A3, A4の発見確率		G(1, 2at)^2*G(2, 2at)*G(2, at)^2*G(3, at)^3*G(4, at)	

例えば、攻撃者の攻撃パケット量は、全て25(packets/sec)とした場合、攻撃者A1, A2, A3, A4の発見確率が95%になるトレースバック時間は65秒である。

（3）ハッシュ方式

(a) 方式概要

各ルータのエージェントが、到着するパケット毎に、ハッシュ値を設定する。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。

(b) 評価システム

ハッシュサイズが14ビットのハッシュ方式システムを評価した。

(c) 数学モデル

トレースバック時間Tとすると

$$T = nT_{ask} + k \quad (4)$$

ここで、nは問い合わせ回数であり、下位ルータに一斉に問い合わせるので、最大ホップ数となる。T_{ask}は1回当りの問い合わせ時間である。kは定数である。

(d) 適用例

図1を用いて、攻撃者毎の最大ホップ数の例を表3に示す。ここで、R1はVに直接、接続されているので、R1のホップ数はカウントしていない。

表3．ハッシュ方式では最大ホップ数の例

攻撃者	問い合わせルータ	最大ホップ数
A1, A2	R2, R3, R4	2
A1, A2, A3, A4	R2, R3, R4, R5, R6	3

3．検証方法と検証ネットワーク

3．1 検証方法

実測値により数学モデルの妥当性を検証する。このため、ノード数が約600台の検証ネットワークを構築し、各種トレースバック方式のトレースバック時間を測定する。攻撃者と犠牲者間のホップ数、ランダムに配置した攻撃者数をパラメータとした検証項目を設定する。検証ネットワークを使用した実測では、FN(False Negative)率、FP(False Positive)率が、それぞれ5%以内になる時のトレースバック時間を測定する。

3．2 検証ネットワークの構成

（1）検証ネットワークの仕様

検証ネットワークの仕様は以下の通りである。

- 規模 サーバ数が300台、全ノード数600台
- 使用OS Linux
- NW速度 100Mbps
- DoS/DDoSアタッカ数 1～100台
- 1台あたりのアタック速度 最大25000packet/sec
- NWトポロジ　コア部はメッシュ
  その他はTree型

（2）検証ネットワークの実装方法

大規模ネットワークを構築する場合、費用、設置場

所、電源確保、廃熱の問題が生じる。本研究ではこれらの問題を仮想 OS 技術を用いることにより解決を図った。使用 OS が Linux と指定されていたことから UML (User Mode Linux) [7] を用いた。

1 仮想 OS あたり 32 MB を割り当て、サーバについては、仮想数は最大 6 とした。ルータについては、PC の入出力インタフェース速度の制限により、仮想 OS は用いていない。

今回検証に用いた、仮想 OS を用いた検証ネットワークの構成を図 3 に示す。サーバ・クライアント数は 380 台、ルータは 110 台である。ルータは zebra [8] を使用した PC ルータである。括弧の中が実 PC 数である。

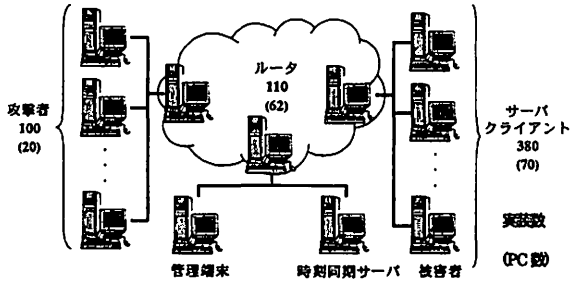

図 3． 検証ネットワークの構成

4． 実測値と理論値との比較

4．1 ホップ数

（1）検証内容

リニアなトポロジで、ホップ数を 1,3,5,10,15,20 と変化させて、トレースバック時間を測定した。測定条件を表 4 に示す。攻撃量は適度なトレースバック時間になるよう設定した。試行回数については、値の変動と試験効率の観点より決定した。

表 4．測定条件

方式	ホップ数	攻撃量	試行回数
ICMP	1,3,5,10,15,20	1250pps	10
IP ﾏｰｷﾝｸﾞ	同上	50pps	100
ﾊｯｼｭ	同上	50pps	5

（2）測定結果

ICMP 方式、IP マーキング方式、ハッシュ方式のシステムについてホップ数とトレースバック時間を検証した。実測値と数学モデルの理論値を図 4 に示す。ほぼ実測値と理論値が一致している。

ハッシュ方式は、ICMP 方式、IP マーキング方式のように確率的にトレースバック情報を生成する方式と異なり、1 パケットでもトレースバックが可能なため、極めて早くトレースバックができている。トレースバック時間は、1～2 秒であるが、ホップ数に伴い増加している。

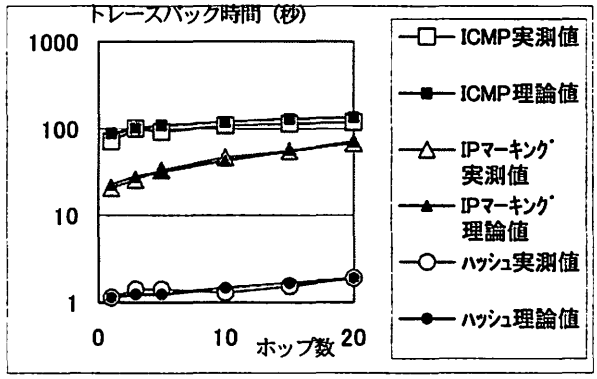

図 4．ホップ数とトレースバック時間の結果

4．2 アタッカ数

（1）検証内容

アタッカ数を変化させて、トレースバック時間を測定した。アタッカ数は、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 に示す。検証 NW トポロジの概要図を図 5 に示す。犠牲者は 1 箇所で、攻撃者数や犠牲者と攻撃者との間のホップ数をパラメータとして評価する。

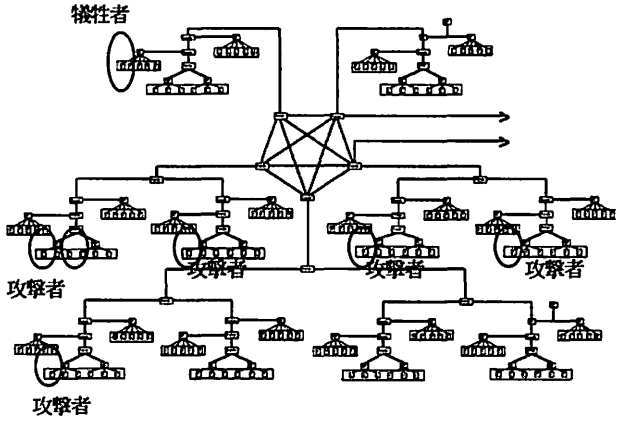

図 5．検証ネットワークのトポロジ

表5．測定条件

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
IPﾏｰｷﾝｸﾞ	同上	1000pps	60
ﾊｯｼｭ	1,10,25,50,100	50pps	5

（2）測定結果

ICMP方式、IPマーキング方式、ハッシュ方式のシステムについてアタッカ数とトレースバック時間を検証した。実測値と数学モデルの理論値を図6に示す。実測値と理論値のほぼ一致している。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。ハッシュ方式では、最大ホップ数は台数によらずほぼ同じなので、トレースバック時間が同じになっている。

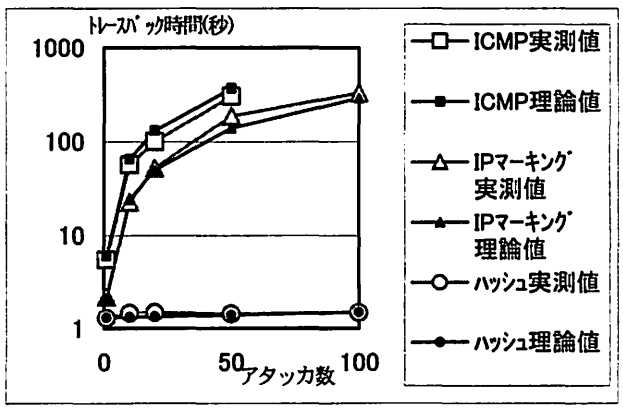

図6．アタッカ数とトレースバック時間の結果

5．まとめと今後の課題

（1）IPトレースバックの数学モデル

ICMP方式、IPマーキング方式、ハッシュ方式の数学モデルを提案した。ICMP方式、IPマーキング方式は攻撃者の発見確率を導出した。パケット数を変動させて任意の発見確率に対応するパケット数を算出する。ハッシュ方式のトレースバック時間は、最も時間のかかるパスに着目し、最大ホップ数の一次式であるとした。これらの数学モデルは、大規模な検証ネットワークを構築して、数学モデルによる理論値が実測値と一致していることを確認した。任意のネットワークトポロジに適用することができ、攻撃パケット速度に依存し、マシンの性能に依存しないので、新しいＩＰトレースバック方式の性能比較で利用することができる。

（2）検証ネットワークの大規模化

数学モデルを検証するために、検証ネットワークを構築して検証した。仮想ＯＳのUMLを使い、仮想的にマシン数を増加することで、150台のＰＣで、約600ノードの検証ネットワークを構築することができた。

（3）今後の課題

今回の検証は、１つのAS(Autonomous Systems)の検証ネットワークで評価を行った。今後は、複数のASを持つ検証ネットワークで、ハイブリッド方式の評価を行う。既に、今回の評価で用いた検証用ネットワークを拡大して、９つのASを持つ、ノード数1100の検証用ネットワークを構築している。

文献

[1] Steven M. Bellovin, "ICMP Traceback Message", Internet Draft: draft-bellovin-itrace-00.txt, submitted Mar. 2000, http://www.research.att.com /~sub/ papers/ draft-bellovin-itrace-00.txt

[2] Dawn Xiaodon Song, Adrian Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback", IEEE INFOCOM 2001, http://vip.poly.edu/kulesh/forensics/docs/ advancedmarking.pdf

[3] Alex C. Snoeren et al., "Hash-Based IP Traceback", Proc. of the ACM SIGCOMM conference 2001, San Diego, CA, Computer Communication Review Vol. 31, No 4, October 2001, http://nms.lcs.mit.edu/~snoeren/papers/spie-sigcomm.pdf

[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] Vadim Kuznetsov, Andrei Simkin, Helena Sandstrom, "An evaluation of different IP traceback approaches", ICICS, 2002, 37-48

[6] 大江将史、門林雄基、" 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

[7] The User-mode Linux Kernel Home Page, http:// user-mode-linux.sourceforge.net

[8] Zebra Home Page, http://www.zebra.org

(注) この研究は、情報通信研究機構から受託(H14～H16年度)して実施している。