高品質インターネット　4－2
(2002. 7. 26)

IPトレースバック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

澤井　裕子†　大江　将史†　飯田　勝吉†　門林　雄基†

† 奈良先端科学技術大学院大学 情報科学研究科
〒 630-0101 生駒市高山町 8916-5
E-mail: †{yuko-sa,masafu-o,katsu,youki-k}@is.aist-nara.ac.jp

あらまし　サービス妨害攻撃への対策技術としてIPトレースバック逆探知パケット方式がある．本方式では，攻撃経路の情報を格納したパケットをある生成確率にしたがって生成し被害ノードに送出する．送出されたパケットを受け取った被害ノードはパケットに含まれる経路情報をもとに攻撃経路を再構成する．この方式は生成確率の値によって攻撃経路の検出性能が変化し，逆探知パケット方式の性能指標である攻撃経路の検出時間とネットワーク帯域への負荷が生成確率の値によるトレードオフの関係にある．しかし，これまでの研究ではトレードオフの関係や性能指標への影響は論理的に示されていない．本研究では逆探知パケット方式のひとつであるIPオプショントレースバックのモデル化をおこない，モデルの数学的解析によって性能指標の相関関係を明らかにする．この解析により性能指標の関係をグラフから割り出し，サービス妨害攻撃を検出可能にする条件下での性能指標の最適値を明示できた．
キーワード　逆探知パケット方式，IPオプショントレースバック，サービス妨害攻撃

Performance Evaluation of the Amount of Trace Traffic and the Time to Re-compose Attack Path in Passive Detection Method of IP Traceback

Yuko SAWAI†, Masafumi OE†, Katsuyoshi IIDA†, and Youki KADOBAYASHI†

† Graduate School of Information Science, Nara Institute of Science and Technology
Takayama-cho 8916-5, Ikoma-shi, Nara, 630-0101 Japan
E-mail: †{yuko-sa,masafu-o,katsu,youki-k}@is.aist-nara.ac.jp

Abstract　IP traceback is a technique to find the true sources of Distributed Denial of Service (DDoS) attack. In this paper, we focus on Passive Detection Packet (PDP) method of IP traceback. There is a trade-off between the amount of trace traffic and the time to detect the attacking route with using PDP method. But no analysis is made yet. We mathatically analyze this trade-off with a model which consider an AS as a node for inter-domain route re-composition.
Key words　Passive Detection method (PDP), IP Option Traceback, Denial of Service attack (DoS)

1. はじめに

インターネットの急速な普及に伴い，不正アクセスによる悪質な犯罪が増加している．その不正アクセスのひとつにサービス妨害攻撃 (Denial of Service attack : DoS attack) がある．サービス妨害攻撃は，攻撃の発生源（攻撃ノード）から大量のトラヒック（攻撃フロー）をネットワークやホストへ送信し，帯域や資源を不正に占有することで正規のユーザによるサービスの利用を妨害する．攻撃フローに用いられるパケット（攻撃パケット）の送信元IPアドレスは一般に偽装されており，送信元IPアドレスを手がかりとした攻撃ノードの特定は困難である．攻撃ノードを特定する技術としてIPトレースバックが研究されている．IPトレースバックはパケットから攻撃フローの通過した経路（攻撃経路）の情報を取得し，送信元IPアドレスの偽装の有無に関わらず攻撃ノードを特定する技術である．

IPトレースバック技術のひとつに逆探知パケット方式がある．この方式は，ネットワーク上を流れるパケットに対し追跡用のパケット（トレースパケット）をある確率で生成し，被害

ノードへ生成したトレースパケットを送信する．被害ノードはトレースパケットを収集し，トレースパケットの持つ情報から攻撃経路を特定し攻撃ノードを特定する．逆探知パケット方式は，トレースパケットを生成する確率（生成確率）を高くすることで被害ノードの受信するトレースパケットの数が増加し攻撃経路検出時間は短縮するがネットワーク帯域への負荷が高くなる．2つの性能指標，攻撃経路検出時間とネットワーク帯域への負荷のバランスは生成確率の値によるトレードオフの関係にある．Bellovin [1] は，トラヒックの増加率は 0.1% 以下でなければならないとし，生成確率の妥当な値として 0.5×10^{-4} を定義している．しかし，この数値の理論的な導出過程は示されていない．

逆探知パケット方式は，パケットを付加的に生成する方式であり，ネットワークへの影響は考慮されなければならない．また，生成確率は逆探知パケット方式の性能を決定する．よって，生成確率がネットワークトラヒックと検出時間へ与える影響が，明らかにされなければ実ネットワークへの導入は難しい．逆探知パケット方式を実用化するためには，生成確率の妥当な値や各性能指標の相関関係の理論的な証明が必要である．

本研究では逆探知パケット方式を用いた IP トレースバックをモデル化し，そのモデルに対して数学的解析をおこなう．そして，モデルの数学的解析により Bellovin [1] が定義する生成確率 0.5×10^{-4} の妥当性を検証し，生成確率の変動により変化する 2 つの性能指標，攻撃経路検出時間とネットワーク帯域の相関関係を調査する．

この解析によって，性能指標の関係をグラフによって示し，サービス妨害攻撃の検出条件「検出時間 30[min]，トラヒック増加率 0.1%」での性能指標の最適値を明示できた．

第二章では IP トレースバック技術の概要を述べ，その中で逆探知パケット方式を紹介する．第三章で本研究の数学モデル，およびその解析を述べ，第四章で数値結果から性能指標のトレードオフを調査し第 5 章で結論を述べる．

2. IP トレースバック

2.1 IP トレースバック技術

IP トレースバック技術はサービス妨害攻撃の攻撃経路を特定し，攻撃ノードを特定する技術である．サービス妨害攻撃の多くは攻撃パケットの送信元 IP アドレスを偽装しているため，送信元 IP アドレスを手がかりとする攻撃ノードの特定は不可能である．また，インターネット上において図 1 に示すようにノード A から B への送信経路（フォワードパス）と B から A への返信に用いられる経路（リバースパス）が同一である保証は無いため traceroute やルーティング情報を用いた攻撃ノードの特定も難しい．現状の攻撃経路の特定には，ルータのもつフィルタリング機能やサービス妨害攻撃検知機能を用いて攻撃フローが流入しているルータ上のリンクを特定し，リンクをたどりルータを再帰的に検査することで行われている．手作業で行われ多くの労力と時間を要するため，攻撃ノードの特定に至るまでの被害は大きい．

IP トレースバック技術は，送信元 IP アドレスの偽装の有無

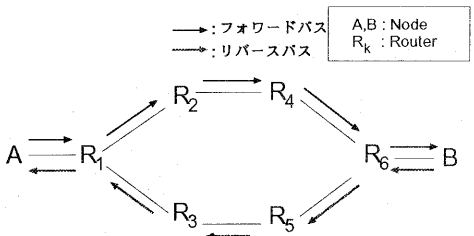

図 1 通過経路の違い

に関わらず短時間で攻撃ノードを特定する技術である．IP トレースバック技術では図 2 のようにフォワードパスを逆にたどる．攻撃経路の特定に用いる情報は攻撃フローが通過した経路の情報であり，攻撃パケットの送信元 IP アドレスの偽装に左右されず攻撃経路および攻撃ノードの特定が可能である．攻撃

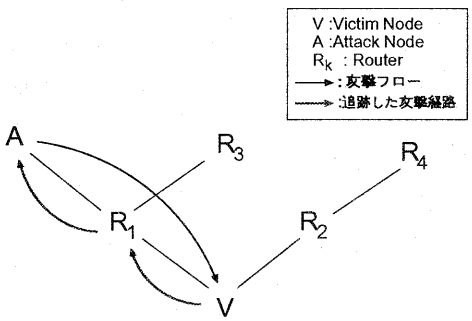

図 2 攻撃経路の追跡

経路の情報を取得する上で様々な方式が提案されているが，ここでは省略する [2]．次に本研究でモデル化する逆探知パケット方式の概要を説明する．

2.2 逆探知パケット方式

2.2.1 ICMP Traceback Messages

ICMP Traceback Messages（iTrace）は Bellovin [1] によって提案された，逆探知パケット方式の基本となる手法である．この手法では，ルータがパケットを転送する際に，攻撃経路情報を格納した ICMP パケット（トレースパケット）をある確率で生成し被害ノードへ送信する．トレースパケットに格納する情報は通過したルータの情報やルータが接続するリンク情報である．被害ノードでは，トレースパケットから攻撃経路情報を取得し，攻撃経路を特定する．iTrace ではトレースパケットはルータ上を通過するパケットに対し無差別に生成され，攻撃フローではないパケットや被害ノードではないノード行きのパケットに対しても生成される．結果として追跡に使用されないトレースパケットがネットワーク上に流れ，ネットワーク帯域に負荷がかかる．Bellovin [1] は生成確率の基準値を 0.5×10^{-4} とし，ネットワーク帯域に影響を与えない生成確率の最大値を 0.1% と定義している．しかし，生成確率の値の妥当性や，生成確率の変動によるネットワーク帯域と攻撃経路検出時間の変

化は示されていない．

2.2.2 Intention-Driven ICMP Trace-back

Wu [3] が提案する Intention-Driven ICMP Trace-back は，ネットワークに流れる利用されないトレースパケットを生成する iTrace の問題点を生成確率を変化させることで解決している．この手法では，被害ノードの追跡要求をルーティングテーブルと併せてルータ上で保持し，ルータは被害ノードへ転送されるパケットに対してのみトレースパケットを生成する．また，ルーティング情報から判断して，遠方にあるノードからのトレースパケット要求に対してはトレースパケットの生成確率を高める．ルータで生成確率を変化させることで，遠方のルータで生成されたトレースパケットと近隣ルータでつくられたトレースパケットが同じ割合で被害ノードに届くようになる．生成確率はネットワーク全体で Bellovin [1] が定義した 0.5×10^{-4} に収まる範囲内で変動し，ネットワーク帯域への負荷は統計的にみて iTrace と変わらないものとなる．Mankin [4] は Intention-Driven ICMP Trace-back により iTrace と同量のトラヒック増加で攻撃経路検出時間を短縮できることを示している．しかし，生成確率の基準となる Bellovin [1] の提示した値 0.5×10^{-4} の妥当性，生成確率の変化によるトラヒック増加率の変動について詳細な分析はされていない．

2.2.3 IP オプショントレースバック

IP オプショントレースバックでは，AS をひとつのノードとみなして攻撃フローの追跡を行なう逆探知パケット方式を提案している．iTrace では無差別に生成されるトレースパケットから，外部に AS 内部のネットワークトポロジーが流出してしまう問題点が指摘されている．IP オプショントレースバックでは，ルータの持つリンク情報ではなく通過 AS の情報を格納したトレースパケットを AS の境界ルータで生成することで対処している．被害ノードは受信したトレースパケットから AS を単位として攻撃経路を特定し，攻撃ノードの存在する AS を特定する．この特性は運営・管理ポリシの異なる AS の接続により構成される現実のインターネットの構造に適合している．しかし，実インターネットで利用するには，サービス妨害攻撃が収束するまでに攻撃経路の検出できる生成確率の値と，その生成確率におけるネットワーク帯域への負荷の検証が必要である．

3. モデル化と数学的解析

3.1 数学的解析の目的

先行研究ではトレースパケットの生成確率がネットワークトラヒックに与える影響と攻撃経路の検出時間に与える効果について検証が行なわれていない．本研究では逆探知パケット方式の有効性を検証するうえで，生成確率の変動による 2 つの性能指標，攻撃経路検出時間とネットワーク帯域への負荷を用いる．IP オプショントレースバックをモデル化し，数学的解析をおこなう．

3.2 数学モデル

ここでは IP オプショントレースバックの数学モデルを導出する．

モデルでは，$(N_1, \ldots, N_n)$ の n 個の AS を考える．N_1 は N_2 に，また N_2 は N_3 と接続しており，$1 < i < n$ とすると，N_i は N_{i-1} と N_{i+1} と接続する．また簡単のため，経路情報交換の遅延やパケット転送遅延は無く，パケットロスは発生しないとする．

N_n は被害ノードを含む AS を示し，N_1 は攻撃ノードを含む AS を示す．攻撃パケットを送信するノードを含む AS は N_1 のみで，N_1 から送信された攻撃パケットは N_1 から順に被害ノードを含む N_n まで転送される．

各 AS では同じ生成確率 p のもとでトレースパケットを生成する．パケットロスは生じないため，全てのトレースパケットと攻撃パケットは被害ノードを含む AS へ到着する．また，このモデルは各 AS が一列に並んだトポロジを想定しているため，攻撃パケットとトレースパケットは同じ経路を通る．さらに，トレースパケットと他のパケットを区別しないため，トレースパケットに対しても新たなトレースパケットを生成する場合がある．

以下の節で次の 2 つの性能指標を解析する．

- 攻撃経路検出時間：t
- 時間間隔 t で生成される総トレースパケット数：r

t は被害ノードを含んだ AS が攻撃パケットを受信してから攻撃経路上の各 AS で生成されたトレースパケットを全て収集するまでに必要な時間を示す．また，r は時間間隔 t において経路上で生成されたトレースパケットの総数を表す．以降 r をネットワーク帯域への負荷をあらわす指標として用いる．

ここで，攻撃経路検出時間 t の確率分布関数を $G(t)$，攻撃ノードを含む AS：N_1 で攻撃パケットが k 個生成された場合での総トレースパケット数 r の確率分布関数を $H_k(r)$ を定義する．

3.3 生成されるトレースパケット数

ここでは，被害ノードを含む AS が k 個の攻撃パケット数を受信した時の総トレースパケット数の期待値 $E[H_k]$ を解析する．

トレースパケットの生成確率は p であり，N_1 が生成するトレースパケット数の期待値は kp である．この時，次の AS：N_2 で生成されるトレースパケット数の期待値は $(k+kp)p$ となる．よって，AS：$N_i; (1 \leqq i \leqq n)$ から送信されるトレースパケット数は $\sum_{j=1}^{i} xp^j$ となる．よって，総トレースパケット数の期待値 $E[H_k]$ は次の式で表される．

$$E[H_k] = \sum_{i=1}^{n} \sum_{j=1}^{i} xp^j = x \sum_{i=1}^{n} (n-i+1)p^i \quad (1)$$

3.4 攻撃経路検出時間

ここでは，攻撃経路検出時間 t について解析を行なう．

被害ノードを含む AS が時間 t までに攻撃パケット k 個を受信したとする．このとき，時間 t 内に攻撃経路を検出できる確率 $G(t)$ は，「時間 t 内に k 個の攻撃パケットが発生する事象 A」と，「k 個の攻撃パケットを受信した時に全ノードからのトレースパケットが揃う事象 B」の事後確率として考えることが

できる．

ここで，事象 A，B それぞれをあらわす確率を

（1） $P(A) = F(t)$

（2） $P(B) = P(X = k)$

とする．

3.4.1 確率関数 $P(X = k)$

まず，事象 A の確率関数 $P(X = k)$ について説明する．

今，N_1 から N_n の n 個のノードのうち，任意のノード $N_i(1 \leqq i \leqq n)$ においてトレースパケットを初めて生成したとする．その対象となった攻撃パケットはノード N_1 から生成された X_i 個目の攻撃パケットであるとする．

このモデルではパケット転送遅延やパケットロスは生じないものとしているので，攻撃経路上の全ての AS でトレースパケットが生成されるまでに N_1 が送信した攻撃パケット数 X は

$$X = \max\{X_1, \ldots, X_n\}$$

となる．

また，このときの攻撃パケット数は時間 t までに被害ノード N_n が受信した攻撃パケットに等しいので，$X = k$ となる．

各ノードは確率 p でトレースパケットを生成する．また，トレースパケットの生成は各 AS で独立して行われる．N_i が初めて生成したトレースパケットによって N_n のもとに全ノードからのトレースパケットが揃うのは $X_i = k$ の場合である．その確率 $P(X_i = k); (1 \leqq i \leqq n)$ は，ベルヌーイ過程に従う．つまり，次式が成り立つ．

$$P(X_i = k) = (1-p)^{(k-1)}p; \quad (k \geqq 1,\ 1 \leqq i \leqq n)$$

ここで，$P(X = k)$ を導くために，次式が成り立つことを示す．

$$\begin{aligned} P(X \leqq k) &= P(\max\{X_1, \ldots, X_n\} \leqq k) \\ &= P(X_1 \leqq k, \ldots, X_n \leqq k) \\ &= P(X_1 \leqq k) \cdots P(X_n \leqq k) \end{aligned} \tag{2}$$

また，X_i においても次式が成り立つ．

$$\begin{aligned} P(X_i \leqq k) &= 1 - P(X_i > k) \\ &= 1 - (1-p)^k \\ &= 1 - q^k \end{aligned} \tag{3}$$

ここで $q = 1 - p$ である．

このとき，(2) と (3) から次式が得られる．

$$P(X \leqq k) = (1-q^k)^n \tag{4}$$

同様に，次式も成り立つ．

$$P(X \leqq k-1) = (1-q^{k-1})^n \tag{5}$$

最期に，(4) と (5) から

$$\begin{aligned} P(X = k) &= P(X \leqq k) - P(X \leqq k-1) \\ &= (1-q^k)^n - (1-q^{k-1})^n; \quad (k \geqq 2) \end{aligned} \tag{6}$$

が言える．また，$k = 1$ のときは，

$$P(X = 1) = (1-q)^n$$

が得られるが，(6) はまた，$k = 1$ においても成り立つ．従って，次式が得られる．

$$\begin{aligned} P(X = k) &= (1-q^k)^n - (1-q^{k-1})^n \\ &= \sum_{i=0}^{n} {}_nC_i \left\{(-q^k)^i - (-q^{k-1})^i\right\} \\ &= \sum_{i=1}^{n} {}_nC_i(-1)^i q^{ki}(1-q^{-i}) \quad (k \geqq 1) \end{aligned} \tag{7}$$

3.4.2 $F(t)$ が一般分布関数であるとき

全てのトレースパケットが揃う時間 t までに攻撃パケット k 個が生成される確率は，各攻撃パケットが生成される時間 $t_i(1 \leqq i \leqq k)$ の確率分布関数 $F(t_i)$ の k 階畳み込み積分によって表される．ここでは，$F(t)$ のラプラス - スティルチェス積分を $F^*(t)$ とし，$F^*(t)$ の k のべき乗で表す．

また，前述したように $G(t)$ は各 $F(t_k)$ において $P(X = k)$ との事後確率で表されるため，$G(t)$ のラプラススティルチェス変換 $G^*(s)$ は次の式で表される．

$$\begin{aligned} G^*(s) &= \sum_{k=1}^{\infty} (F^*(s))^k P(X = k) \\ &= \sum_{k=1}^{\infty} (F^*(s))^k \sum_{i=1}^{n} {}_nC_i(-1)^i q^{ki}(1-q^{-i}) \end{aligned} \tag{8}$$

3.4.3 $F(t)$ が一定到着過程であるとき

ここで，$G(t)$ の明確な式を得るために，攻撃パケットの生成時間間隔を一定にして考える．

$$F(t) = \begin{cases} 0 & \text{if } t < a \\ 1 & \text{otherwise} \end{cases}$$

ここで，F(t) の確率変数を k 回合成した時の確率分布関数を $F^{*k}(t)$ とすると，これもまた $k \geqq 1$ において次式に示すステップ関数となる．

$$F^{*k}(t) = \begin{cases} 0 & \text{if } t < ka \\ 1 & \text{otherwise} \end{cases} \tag{9}$$

これは，すでに導出した $P(X \leqq k)$ から $G(t)$ を導くことができることを意味しており，求める $G(t)$ は次のようになる．

$$G(t) = P\left(X \leqq \lfloor \frac{t}{a} \rfloor\right) = (1-q^{\lfloor \frac{t}{a} \rfloor})^n \tag{10}$$

3.4.4 期 待 値

ここでは，$G(t)$ から期待値 $E[G(t)]$ を求める．$G(t)$ の平均は，$G^*(s)$ の一階微分によって求められる．$G(t)$ の LST(ラプラススティルチェス変換) (9) において，$F^*(s)$ に次式

$$F^*(s) = e^{-sa}$$

を代入することによって求める．3.4.3節の $F(t)$ の LST である．

$$\begin{aligned} G^*(s) &= \sum_{k=1}^{\infty} e^{-sak} \sum_{i=1}^{n} {}_nC_i(-1)^i q^{ki}(1-q^{-i}) \\ &= \sum_{i=1}^{n} {}_nC_i(-1)^i(1-q^{-i}) \sum_{k=1}^{\infty} \left(e^{-sa}q^i\right)^k \end{aligned} \tag{11}$$

$\sum_{k=1}^{\infty}\left(e^{-sa}q^i\right)^k$ は，無限等比級数の和になっており，この値の収束条件は $(e^{-sa}q^i) < 1$ である．

これを $l = k+1$ と置き換えて式変形行なうと

$$\begin{aligned} ppG^*(s) &= \sum_{i=1}^{n} {}_nC_i(-1)^i(1-q^{-i}) \sum_{l=2}^{\infty} \left(e^{-sa}q^i\right)^{l-1} \\ &= \sum_{i=1}^{n} {}_nC_i(-1)^i(1-q^{-i}) \frac{e^{-sa}q^i}{1-e^{-sa}q^i} \end{aligned}$$

が得られる．

$G^*(s)$ は，説明を明確にするために次式のように置き換える．

$$G^*(s) = \sum_{i=1}^{n} {}_nC_i(-1)^i(1-q^{-1}) \frac{\alpha(s)}{\beta(s)}$$

ここで

$$\alpha(s) = e^{-sa}q^i$$

$$\beta(s) = 1 - e^{-sa}q^i$$

であり，微分関数の値は次のようになる．

$$\frac{d}{ds}G^*(s) = \sum_{i=1}^{n} {}_nC_i(-1)^i(1-q^{-i}) \left(\frac{a\alpha^2(s)}{\beta^2(s)} - \frac{a\alpha(s)}{\beta(s)}\right)$$

また，上式は微分関数によって次のように表現できる．

$$\frac{d}{ds}\alpha(s) = -a\alpha(s)$$

$\alpha(0) = q^i$ また，$\beta(0) = 1 - q^i$ より期待値 $E[G]$ は次式によって得られる．

$$\begin{aligned} E[G] &= -\lim_{s\to 0} \frac{d}{ds} G^*(s) \\ &= a\sum_{i=1}^{n} {}_nC_i(-1)^{i+1} \frac{1}{1-q^i} \end{aligned} \tag{12}$$

4. 数値結果と既存研究の検証

4.1 検証目的

本研究で定義する数学モデル上でトレースバケット生成確率を変動させるときのネットワーク帯域への負荷と攻撃経路検出時間を算出し，生成確率 0.5×10^{-4} の妥当性を検証する．ネットワーク帯域への負荷はトラヒック増加率を指標として算出する．そして最適な生成確率の値を調査する．

数値結果による検証を行う上で，トラヒック増加率と攻撃検出時間について目標値を設定する．トラヒック増加率の目標値は，Bellovin [1] の定義に従い 0.1% とする．トラヒック増加率は，トレースバケット数と攻撃バケット数の総和に対するトレースバケット数の割合として算出する．また，攻撃経路検出時間は 30[min] を目標値とする．サービス妨害攻撃が 30[min] 後に収束をはじめ 60[min] 後にほぼ収束するとの CAIDA [5] の報告から，収束が開始する時間を目標値に定めた．

本モデルでの検証には，次の 2 式の性能指標を用いる．

$$E[H_k] = k\sum_{i=1}^{n}(n-i+1)p^i \tag{13}$$

$$G(t) = (1-q^{\lfloor \frac{t}{a} \rfloor})^n \tag{14}$$

$E[H_k]$ は攻撃バケット k 個を送信するときのトレースバケット数 r との割合が確率分布関数 $H_k(r)$ にしたがっている場合の期待値である．確率 p の変動によるトレースバケットの増減を示す．

$G(t)$ は時間 t で攻撃経路を検出する確率の関数であり，攻撃経路検出の成功率である．検証では，成功率 90%未満は非実用的であるとし，検出成功率は約 90%以上を目標とする．

4.2 検証条件

検証には，以下の条件を用いる．

（1） データ転送率： $480k[bit/sec]$

検証には，現在広く普及している $512K[bit/sec]$ の帯域幅をもつ ADSL からの攻撃を想定する．$512K[bit/sec]$ の帯域幅のうち $480k[bit/s]$ を攻撃に用いられる帯域とする。

（2） パケット長： $1400[bytes]$

ADSL におけるパケット最大サイズは $1454[bit/pkt]$ である．本検証におけるパケットサイズは $1400[bytes/pkt]$ とする．

（3） 攻撃パケットが通過する AS の設定値： 8

CAIDA [5] の報告によればほとんどのパケットが通過する AS の数は 5 ～ 8 であり，検証には 8 を攻撃パケットが通過する AS の設定値とする．また，変数 n は $1 \leqq n \leqq 30$ の範囲で値をとる．

以上の目標値と検証条件から導出される目標検出時間 t，攻撃パケットの生成時間間隔 a，時間 t 内に生成される攻撃パケット数 k の算出結果は以下の通りである．

$$t = 30[min] = 1800[sec]$$

$$a = \frac{1400[bytes/sec]\times 8[bit/byte]}{480K[bit/sec]} = 0.023[sec]$$

$$k = \lfloor \frac{t}{a} \rfloor = 77143[pkt]$$

4.3 検証方法

式 (14) において AS の数 n を一定にした場合に得られた結果を図 3，図 4 に，式 (13) において検出時間 t を一定にした場合に得られた結果を図 6 に示した．

これらのグラフから，各パラメータ間の関係を調査し，第 4 章出述べた条件のもとで、以下の項目を解析する．

（1） Bellovin によって提案された生成確率 0.5×10^{-4} の妥当性

（2） サービス妨害攻撃の収束時間 (30[min]) までに攻撃経路を検出できる生成確率

（3） ネットワークトラヒックの増加率を 0.1% におさえる

ことができる生成確率 p

4.4 数値結果

4.4.1 検出時間 30[min] 以内の生成確率

図 3 は，生成確率 p と攻撃検出時間 t との関係を表す．図 3 はからは，生成確率が高くなるほど攻撃経路を検出時間を短くできることがわかる．その減少率は生成確率が低い値の場合は大きく，生成確率が高い値の場合は小さい．また，$G(t)$ の差による t の差分も生成確率 p を大きくすればほど，小さくなる．これは，図 3 より $G(t) = 0.999$ と $G(t) = 0.990$ の値の差は確率 0.5×10^{-4} と比べて，確率 1.5×10^{-4} では小さいことからも見て取れる．

ここで，$p = 0.5 \times 10^{-4}$ である時の検出時間 t を求めると，図 3 から，$G(t) = 0.999$ の場合は 4133[sec] でり，目標の 30[min] 以内に攻撃パスを検出出来ない。そこで，逆に検出時間が t である時の生成確率を求める．

図 3 より，$30 \times 60 = 1800[sec]$ の場合の生成確率は，検出成功率 $G(t) = 0.999$ において $p = 1.5 \times 10^{-4}$ である．よって，生成確率 $p = 1.5 \times 10^{-4}$ 以上であれば $p = 0.5 \times 10^{-4}$ よりも短時間の検出が可能であり，攻撃が収束しはじめる 30[min] 以内に検出ができることがわかる．

4.4.2 トラヒック増加率 0.1% 以内の生成確率

では，生成確率 1.5×10^{-4} の場合，トレースパケットによるトラヒック増加率はどうか．トレースパケットの増加率を求めるためには，図 4 を用いる．

図 4 は，式 (14) により得られ，生成確率 p が生成されたトレースパケット数の増加率に与える影響を示す．

図 4 では，p の取る値は見易さのため $4.0 \times 10^{-5} \sim 2.0 \times 10^{-4}$ を定義域としているが，図 5 の一部である．図 5 は，$0 \sim 1$ の範囲で p が 1 に近づく程 r/k は指数的に増加する様子が見られる．しかし，Bellovin [1] の定義，「生成確率は 0.001 以上は取るべきではない」という条件の下で行っているため，ここでは，図 4 が示す $4.0 \times 10^{-5} \sim 2.0 \times 10^{-4}$ の範囲で検証を行う．図 4 より，生成確率 p のとる値が低い範囲では，p の増加に従ってトレースパケット数 r の増加率はほぼ比例して増えるとみなせる．

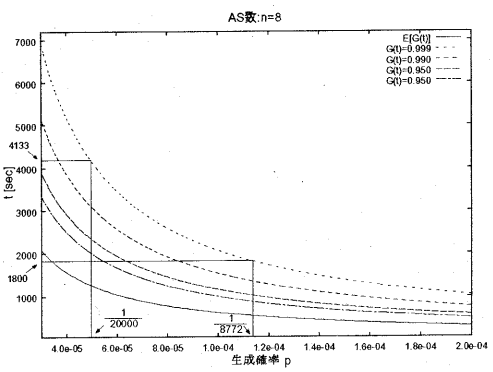

図 3 生成確率 p が検出時間 t に与える影響 (n=8)

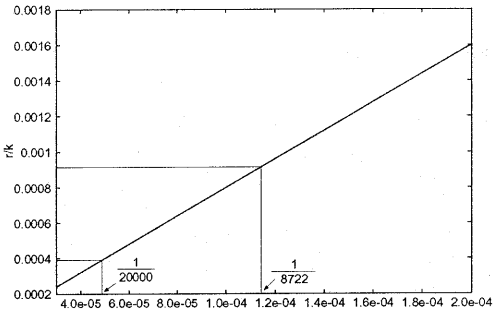

図 4 生成確率 p が逆探知パケット増加率 r/k に与える影響 (n=8)

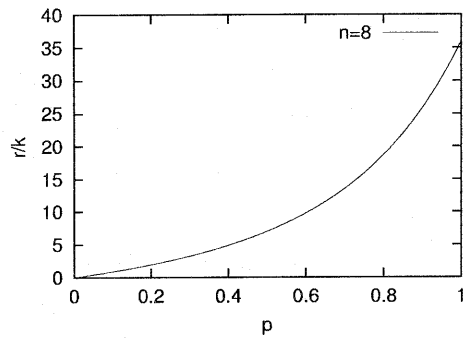

図 5 生成確率 p が逆探知パケット増加率 rk に与える影響
$n = 8 : (0 \leqq p \leqq 1)$

図 4 を用いて生成確率 1.5×10^{-4} のトラヒック増加率が 0.1% におさまるか検証する．その結果，0.033% のトラヒックの増加になることがわかる．この増分は，0.1% 以内におさめるべきという Bellovin [1] の定義を満たしている．同様に，生成確率 0.5×10^{-4} のトラヒック増加量は $r/k = 0.015\%$ であり，検出時間は 30[min] 以内ではないが，トラヒック増加率は 0.1% 内におさめることができる．

逆に，トラヒック増加率が 0.1% におさまる場合の生成確率を求める．図 4 より，トラヒック増加率が 0.1% である生成確率は，$p = 0.5 \times 10^{-4}$ である．よって，生成確率が $p = 0.5 \times 10^{-4}$ 以下の場合はトラヒック増加率に関して問題がないとみなせる．

4.4.3 各成功率における攻撃経路検出時間とトラヒック増加率の関係

4.3 の結果から，各成功率 $G(t) = 0.8000 \sim 0.999$ の条件の中で，生成確率 0.5×10^{-4} と，1.5×10^{-4} の場合におけるアタックパケットの検出時間とトレースパケット増加率を表 4.4.3 に示した．

表 4.4.3 から，生成確率 0.5×10^{-4} では成功率 90% までならば 30[min] 以内で，生成確率 1.5×10^{-4} では成功率 90% までならば 30[min] 以内で検出できることが，明かになった．

4.4.4 生成確率と AS 数の関係

最後に，生成確率 p と成功率 $G(t)$ で検出可能な AS の数 n

表 1　$p = 0.5 \times 10^{-4}$ での $G(t)$ における攻撃経路検出時間

検出の成功率 $G(t)$	検出時間 t ($p = 0.5 \times 10^{-5}$)	検出時間 t ($p = 1.5 \times 10^{-4}$)
0.999	4133[sec] (≒68[min])	1550[sec] (≒25[min])
0.990	3072[sec] (≒51[min])	1147[sec] (≒19[min])
0.980	2750[sec] (≒46[min])	1025[sec] (≒17[min])
0.950	2323[sec] (≒38[min])	867[sec] (≒14[min])
0.900	1994[sec] (≒33[min])	745[sec] (≒12[min])
0.850	1798[sec] (≒29[min])	671[sec] (≒11[min])
0.800	1654[sec] (≒27[min])	616[sec] (≒10[min])

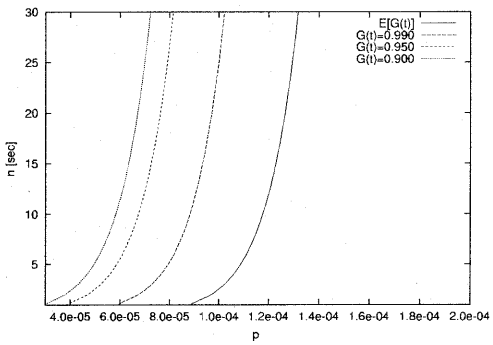

図 6　生成確率 p と AS 数 n との関係グラフ (t=1800s)

との関係を示す．これは，次の図 6 から得られる．

成功率 $G(t) = 0.999$ では，生成確率 0.5×10^{-4} では，成功率 80% で最大 11 の AS までしか検出できないことになる．一方，生成確率を 1.5×10^{-4} まであげると成功率 99.9% 最大 31 の AS まで検出できる．今日のインターネットにおける平均 AS 数は，前述したように 5 ～ 8 であるためどちらの生成確率でも AS の数に関しては有用であるといえる．

5. 考　　察

得られた結果から，本モデルでは Bellovin [1] によって提案された生成確率 0.5×10^{-4} は，成功率 80% において 30[min] 以内の追跡が可能であり，その場合のトラヒック量は 0.1% に抑えられることがわかった．しかし，アタックパス検出の成功率が 99.9 %である場合は検出時間に 60[min] を要し，有用でない．一方，逆に 30[min] 以内に検出が可能な生成確率の値を、図 3 から得られ、その値は、成功率 99.9% で 1.5×10^{-4} であることが導出できた．図 4 より，この場合のトラヒック増加率は 0.1% に満たないことも導出できた．

よって，検出時間 30[min] 以下の条件のもとでは，成功率 99.9% で $p = 1.5 \times 10^{-4}$ が最適生成確率であるといえる．逆に検出時間を考慮せず，トレースパケットの増加率の最大が 0.1% であるという条件のもとで，最適値を求めると，生成確率 1.24×10^{-6} 以下が望ましいといえる．

6. おわりに

本研究では，逆探知パケット生成型トレースバック方式の IP オプショントレースバックの実用化を目的として，この方式のモデル化を行ない，関連研究で提案された生成確率の妥当性と，生成確率により変動する性能指標の関係を数学的見地から考察を行なった．

今回の研究で，逆探知パケット方式のモデル化と数学的解析を行うことで，性能指標間の関係と，関連研究で定義されている生成確率の妥当性を確認した．

結果として，$480K[bit/sec]$ のネットワーク帯域で，AS 数 8 の場合，Bellovin [1] によって提案された生成確率 0.5×10^{-4} でのアタックパス検出は十分可能であることが分かった．また，同じ条件で生成確率 0.001 を取ると，ネットワークトラヒックに影響を与えるとして推奨されていない増加率 0.1% を超える結果となった．

以上より，検出時間が 30[min] という条件下ではこの範囲で最大のトレースパケットを生成することができる生成確率 1.5×10^{-4} が，トラヒック増加率 0.1% という条件下ではこの範囲での最短時間で検出が出来る生成確率 1.24×10^{4} が最適な生成確率といえる．

今後は，実トラヒックを用いた本モデルの検証を行ない，生成確率の変化を利用した新しい手法の提案により，逆探知パケット方式の実用化実現を目指す．また，線形ではなく網状ネットワークのモデルについても考察し，増加率 0.1% より大きな値をとる場合におけるトラヒックに与える影響の明確化も課題の一つである．

7. 謝　　辞

離散確率変数の順序統計量の解析に関して貴重なコメントを下さった三好直人博士，本研究を行うにあたりご協力頂いたインターネット工学講座の皆様に深く感謝いたします．また，本研究の一部は平成１４年度文部科学省科学研究費補助金（若手研究Ｂ）「高信頼大規模インターネットの設計手法に関する研究」（課題番号：13750353）によっています．ここに記して謝意を表します．

文　　献

[1] Steven M. Bellovin, "ICMP Traceback Messages", http://www.research.att.com/ smb/papers/draft-bellovin-itrace-00.txt

[2] 門林，大江，" IP トレースバック技術 " 情報処理 42 巻 12 号，2001

[3] S. Felix Wu, Lixia Zhang, "Intention-Driven ICMP Trace-Back", draft-ietf-itrace-intention-00.txt, May 2002 (expires).

[4] allison Mankin, Dan Massey, Chien-Lung Wu, S. Felix Wu, and Lixia Zhang, "On Design and Evaluation of Intention-Driven ICMP Traceback" Proceedings of IEEE International Conference on Computer Communications and Networks, Arizona, 2001.

[5] David Moore, "Inferring Internet Denial-of-Service Activity", http://www.caida.org/outreach/papers/2001/BackScatter/

[6] R. L. Carter and M. E. Crovella. Dynamic Server Selection Using Dynamic Path Characterization in Wide-Area Networks. In Proceedings of the 1997 IEEE INFOCOM Conference, Kobe, Japan, Apr. 1997.