情報処理学会論文誌 Vol. 52 No. 2 610–620 (Feb. 2011)

事後確率評価を利用したDDoS攻撃に対する統計的フィルタリング手法

三島大季[†1] 安達直世[†2] 滝沢泰久[†2]

DDoS（Distributed Denial of Service）攻撃は，各地に分散された多数のノードから，大量の不正トラヒックを攻撃対象とするサーバに送りつけることにより，ユーザに対するサービス提供を不可能にする不正アクセスの 1 つである．DDoS による攻撃トラヒックの判別・破棄は一般的に困難なものであるが，インターネットの信頼性・安全性を脅かす一因であり，その対策はますます重要となっている．そこで本研究では DDoS 攻撃が発生していない時点におけるパケットの到着レート分布および観測によって得られるパケット属性値の分布を用い，パケットが DDoS 攻撃を目的としたものである事後確率の評価を行うことによって，パケットの破棄を行うフィルタリング方式を提案する．シミュレーション結果より，提案手法は攻撃パケットのビットレートが低い場合においても，攻撃パケットだけを選択的に破棄することが可能であることが分かった．

Statistical Filtering Method against DDoS Attacks by Evaluating Posterior Probability

Taiki Mishima,[†1] Naotoshi Adachi[†2] and Yasuhisa Takizawa[†2]

DDoS (Distributed Denial of Service) is one of the illegal accesses. The attackers send a high volume of attack packets from a large number of machines distributed over various location to target server, and make it impossible to perform services for legitimate users. It is generally difficult to detect or reject of DDoS attack packets, but DDoS is one of the threats to reliability and security of the Internet. In this paper, we propose packet filtering method against DDoS attack. In our method, we calculate and evaluate the posterior probability of the event that an arrival packet belongs to DDoS traffic with inter arrival distribution and distribution of packet attribute. Numerical examples show that the proposed method effciently detects attack packets among a large number of normal packet streams.

1. はじめに

DDoS（Distributed Denial of Service）攻撃は，インターネット上に分散する多数の攻撃ノードから，大量の不正トラヒックを攻撃対象とするサーバに送りつけ，ユーザに対するサービス提供を不可能とする不正アクセスの 1 つである．2000 年には Yahoo! や amazon などの大手 Web サイトに対して[1]，2003 年にはルート DNS への攻撃[2] によってサービスが停止する事態となった．このように DDoS 攻撃は，インターネットの信頼性・安全性を脅かす一因であり，その対策はますます重要となっている．

攻撃者は不正に侵入した複数のノードに攻撃用プログラムを待機させ，攻撃指令に従っていっせいにパケットを攻撃対象に向けて送信する．攻撃パケットの送信元アドレスやパケットフラグなどは，多くの場合において身元を隠すため偽装されており，これらの情報をもとに攻撃元を追跡することは困難なため，攻撃者を特定し潜在的な攻撃者の通信を阻止することは困難である．また，DDoS 攻撃の約 90%に該当する[3] TCP SYN Flooding では，接続確立時の 3-way handshake における仕様の不備を悪用した攻撃であるため，通常のコネクション確立要求との区別を行うことが困難であり，攻撃に関するパケットのみを破棄することは難しい．根本的な解決策としては，現在のインターネットプロトコル自体を修正する必要があるが，現実的な解としては非常に困難である[4),5)]．

DDoS 攻撃に対する防衛手法は，大きく 4 つに分類される[6),7)]．

(1) 攻撃の予防（attack prevention）
(2) 攻撃検知（attack detection）
(3) 攻撃元の特定（attack source identification）
(4) 攻撃への対処（attack reaction）

攻撃の予防は，攻撃がターゲットに届く前に食い止める手法である．攻撃の送信元で偽称されたパケットをフィルタリングする方法であり，偽称したパケットを用いる DDoS 攻撃に対して最も効果のある防衛法の 1 つである．攻撃検知は発生した DDoS 攻撃をすばやく正確に検知することを目的としており，攻撃を受けた後の行動を指示するための重要な手続きとなる．攻撃元の特定は，送信元アドレスのフィールドに，間違った情報が含まれている

†1 関西大学大学院理工学研究科
Graduate School of Engineering, Kansai University
†2 関西大学環境都市工学部
Faculty of Environmental and Urban Engineering, Kansai University

© 2011 Information Processing Society of Japan

かどうかにかかわらず攻撃元を特定する手法であり，潜在的な攻撃者の通信を阻止して攻撃の被害を少なくする．攻撃への対処は，攻撃の影響を取り除くか削減する手法である．以下では攻撃検知と攻撃への対処の既存の防衛手法について説明する．

一般に DDoS 攻撃の検知技術は大きく 2 つに分類される．1 つ目は DDoS 攻撃の特徴に基づいた特定によって検知を行う手法である．もう 1 つは正当なトラヒックの振舞いをモデル化し，例外を報告する手法である．攻撃の特徴に基づく手法には Gil らによって提案された MULTOPS[8] という手法がある．この手法は UP リンクと DOWN リンクの両方のパケットレートを観測することで DDoS 攻撃を検知する．2 つのホスト間の UP リンクと DOWN リンクのパケットレートは，通常時に比例すると仮定しており，DDoS 攻撃が発生すると UP リンクと DOWN リンクのパケットレートの不釣り合いな状態になる．この状態を検知することで DDoS 攻撃の検知を行う．そのほかにも SYN Flood 攻撃を検知するために，FIN・RST パケットに対する SYN パケットの割合を用いて攻撃を検知する手法などが提案されている[9]．これらの手法は観測されたトラヒックが既知の特徴と一致すれば攻撃を特定することができる．しかし，攻撃者はシステム固有の脆弱性を狙う必要がないため，攻撃トラヒックの種類や内容を変更して攻撃を行うことは比較的容易である．そのため，攻撃の特徴によって DDoS 攻撃を正確に検知することは困難である．

これらの問題に対し，既存の攻撃トラヒックパターン固有の特徴を用いることなく，DDoS 攻撃の検知・フィルタリングを試みる研究が行われている[10),11)]．文献 10) では，SYN パケットの到着間隔分布に着目し，DDoS 攻撃が発生していない時点での SYN パケット到着間隔分布のモデル分布と観測トラヒックの SYN パケット到着間隔分布との乖離を調べることによって攻撃検出を行う．この手法により，比較的攻撃トラヒックのレートが低い場合においても，高精度な攻撃検出率を達成している．文献 11) では，DDoS 攻撃が発生していないときにあらかじめ計測したパケットの属性値（送信元 IP アドレス，ポート番号，TTL，パケットサイズなど）に関する分布を求めておく．得られた分布を用い，観測した各パケットが正常である事後確率を求めることによってパケットの異常性を検証し，DDoS 攻撃の可能性があるパケットだけを破棄することを可能としている．

しかし，文献 10) の手法は攻撃の検知を目的としており，攻撃性の疑いがあるパケットだけを選択的に破棄することができない．一方，文献 11) では，攻撃トラヒックのレートが低い場合（正常トラヒックと同程度のレート）に，攻撃パケットの破棄に失敗するという結果が示されている．

そこで，本研究では攻撃トラヒックのレートが低い場合においても，攻撃パケットを選択的に破棄する手法を提案する．本研究における攻撃パケットとは，DDoS 攻撃を目的としたパケットのみで構成されているものとする．提案手法では，あらかじめ観測によって得られた到着レートの分布と，正常時における到着レート分布のモデルとの比較により評価を行う．ここで正常時とは，DDoS 攻撃以外のトラヒックもまったく含まれていない通信状況を意味している．加えて，各パケットに記されている属性値（送信先ポート番号とパケットサイズ）を用い，事後確率を評価することによってパケットの異常性の検証を行う．以下，2 章では本提案手法の詳細について述べる．3 章では本提案手法の有効性をシミュレーションによって評価を行う．最後に 4 章でまとめと今後の課題について述べる．

2. トラヒックの統計的分析と DDoS トラヒックのフィルタリング手法

提案手法では，フィルタリングを行う際にパケットから以下の情報を取得する．

(1)　T_i：パケットの到着間隔

(2)　P_{size}：パケットサイズ

(3)　D_{port}：送信先ポート番号

上記データのうちパケットサイズ・送信先ポート番号を用いて，フィルタリング対象となるパケットの観測属性値を $\boldsymbol{x} = (P_{size}, D_{port})$ として用いる．パケットの観測属性値としては様々な組合せを考えられるが，様々な属性値を用い検証を行った中で誤通過率・誤遮断率が最も低かったパケットサイズと送信先ポート番号を属性値の要素として選択した．フィルタリングを行う際に，観測したパケットは攻撃を目的としたパケットであるか，あるいは攻撃を目的としない通常のデータ通信に関するパケットのいずれかである．

次に，観測した各パケットに対して，フィルタリングによって受理（accept）・拒否（reject）を判定するために，次のような条件付き確率の比を計算する．

$$R(\boldsymbol{x}) = \frac{P(I|\boldsymbol{x})}{P(L|\boldsymbol{x})}. \tag{1}$$

ここで，I（Illegal）は観測したパケットが DDoS 攻撃を目的としたパケットであること（以後，攻撃パケット）を意味し，L（Legal）は観測したパケットが DDoS 攻撃を目的としたパケットでないこと（以後，正常パケット）を表す．式 (1) における，$P(I|\boldsymbol{x})$，$P(L|\boldsymbol{x})$ はそれぞれ，フィルタリングを行う際に観測した属性値が $\boldsymbol{x}$ であったとき，観測したパケットが正常パケットである確率，攻撃パケットである確率となる．$P(I|\boldsymbol{x})$（あるいは $P(L|\boldsymbol{x})$）は観測によって収集したパケットデータからなる母集団のうち，観測状態が $\boldsymbol{x}$ となる正常パケット（攻撃パケット）の個数によって求められるが，フィルタリングの作業中にはこれ

© 2011 Information Processing Society of Japan

ら母集団中の正常パケット，攻撃パケットの数は不明であるため，直接 $P(I|\boldsymbol{x})$（あるいは $P(L|\boldsymbol{x})$）を求めることができない．

そこで，式 (1) より式 (2) が得られるが，$P(\boldsymbol{x}|I)$ を計算する必要がある．これは，観測パケットが DDoS 攻撃によるものだった場合の観測属性値 $\boldsymbol{x}$ の分布である．しかし，$\boldsymbol{x}$ は DDoS 攻撃の手法によって異なるし，DDoS に対する対処法の発展にともなっても異なるものである．したがって，$\boldsymbol{x}$ に対する分布をあらかじめ知ることは困難であるし，また仮に分布を得られたとしても，未知の攻撃が出現した場合には対応できず，再び分布の導出を行う必要がある．

$$R(\boldsymbol{x}) = \frac{P(I|\boldsymbol{x})}{P(L|\boldsymbol{x})} = \frac{P(\boldsymbol{x}|I)P(L)}{P(\boldsymbol{x}|L)P(I)}. \tag{2}$$

そこで式 (2) を，攻撃パケットに対する $\boldsymbol{x}$ の分布を必要としない，式 (3) に変形する．条件付き確率の比であるので，式 (3) の値が 1 より大きいときは観測パケットを攻撃パケットと判別し reject，1 より小さいときには観測パケットは正常パケットと判断し accept とする．

$$\begin{aligned} R(\boldsymbol{x}) = \frac{P(I|\boldsymbol{x})}{P(L|\boldsymbol{x})} &= \frac{P(I \cap \boldsymbol{x})}{P(\boldsymbol{x}|L)P(L)} \\ &= \frac{P(\boldsymbol{x}) - P(L \cap \boldsymbol{x})}{P(\boldsymbol{x}|L)P(L)} \\ &= \frac{P(\boldsymbol{x})}{P(\boldsymbol{x}|L)P(L)} - 1. \end{aligned} \tag{3}$$

式 (3) において，$P(\boldsymbol{x})$ は随時更新される観測パケットの直近の履歴から頻度分布を用いて計算を行う．一方 $P(\boldsymbol{x}|L)$ は正常パケットが持つ属性値 $\boldsymbol{x}$ の分布，$P(L)$ は何ら条件を与えられていないときに観測パケットが正常である確率である．この $P(\boldsymbol{x}|L)$ の導出については，2.1 節で詳細を述べる．また，$P(L)$ は 2.2 節で詳細を述べる．

2.1　$P(\boldsymbol{x}|L)$ の導出

式 (3) において，$P(\boldsymbol{x}|L)$ は DDoS 攻撃が発生していない時点でのトレースデータから得られる頻度分布で与えられる．しかし，この分布を作成する期間に 1 度だけ作られるような分布ではトラヒックの特徴の代表としては不十分である可能性がある．このような状況を避けるために，分布を作成する期間を複数の期間に分割しておき，その分割された期間ごとにそれぞれの割合が観測された中から代表する割合を選択する．提案する手法では，分布の中よりも高い属性値の割合を持つパケットを遮断することが目的である．したがって，

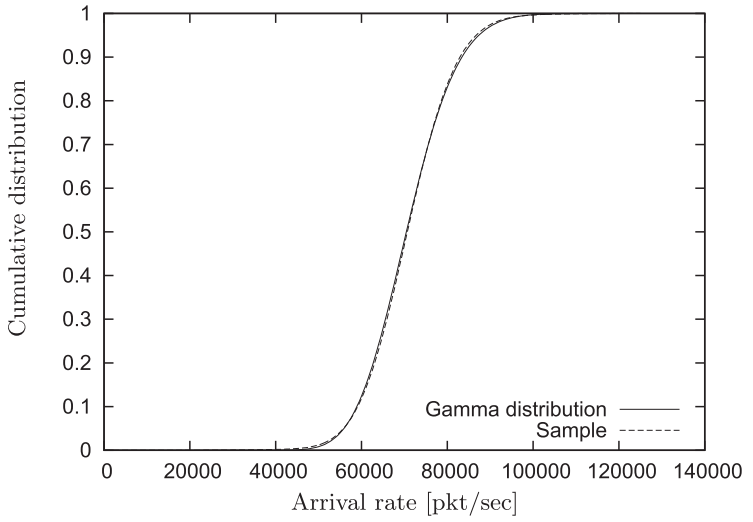

図 1　到着レートの累積確率分布
Fig. 1　Cumulative distribution of arrival rate.

正規のトラヒックが持つ属性値の割合の不定期な高まりに対応するために，複数の期間の中から最も高い割合を選択する．これにより正常なトラヒックには安全な範囲を提供しつつ，攻撃トラヒックに対しては小さいペナルティを与えることが可能となる．

2.2　$P(L)$ の導出

$P(L)$ は観測したパケットが正常である確率を表しているが，これは何ら条件が与えられていない状況下においては直接求めることができない．文献 10) では，SYN パケットの到着レートに注目した DDoS 攻撃の検出手法の提案が行われている．正常時における SYN パケットの到着レートは正規分布あるいはガンマ分布に従うことが示されており，観測トラヒックの到着レートの分布と，正規分布の乖離度を調べることによって DDoS 攻撃の検出が可能であることが示されている．この結果をもとに，我々は実験で用いる実トラヒックデータである MAWI のトレースデータにおける全パケットに対して，直近 m 個のパケットから求められる平均到着レート（これを本手法における到着レートの算出方法とする）について調べた．その結果，到着レートの分布は，ガンマ分布に従うことが判明した（**図 1**）．これはサンプルポイントや観測日時が異なる場合においても同様の結果になることも確認

© 2011 Information Processing Society of Japan

済みである．なおここで，調査を行った MAWI のトレースデータには，コネクションごとの振舞いやシーケンス番号の振舞いなどを調べ，攻撃パケットと思われるような記録がないデータであることをあらかじめ確認を行っている．ガンマ分布の累積分布関数 $F(x)$ および確率密度関数 $f(x)$ は，式 (4) で与えられる．ここで α，β はそれぞれ，形式母数（$\alpha > 0$），尺度母数（$\beta > 0$）と呼ばれるパラメータ，Γ は不完全ガンマ関数である．

$$F(x) = \frac{\gamma(\alpha, x/\beta)}{\Gamma(\alpha)}$$
$$f(x) = x^{k-1}\frac{e^{-x/\beta}}{\Gamma(\alpha)}. \tag{4}$$

ガンマ分布の平均，分散はそれぞれ，$\alpha\beta$，$\alpha\beta^2$ である．よって，観測トラヒックの到着レートの平均・分散を得ることができれば，正常パケットの到着レートが従うべき分布を決定することができる．

これらの結果をふまえ，提案手法では観測したパケットから直近の到着レート履歴を用いて得られる到着レート分布と，DDoS 攻撃が行われていないときの到着間隔分布との乖離度 d（$0 \leq d \leq 1$）を求め，この値を $P(L)$ として式 (3) で用いる．ガンマ分布と実際の観測結果から得られるパケットの到着レートの分布を用いて，乖離度 d を次のように定義する．

$$d = \frac{\sum_i f(r_i)g(r_i)}{\sqrt{\sum_i f(r_i)^2 \sum_i g(r_i)^2}} \quad (0 \leq d \leq 1). \tag{5}$$

ここで，$g(r_i)$ を観測トラヒックから得られる頻度分布とし，r_i（$i \geq 1$）を頻度分布を作成する際に用いる到着レートに対する各階級とする．観測トラヒックから得る分布は直近 n 個の到着レートを用いて求める．また，$f(r_i)$ を観測トラヒックのビットレートを確率変数とするガンマ分布の確率密度関数とし，計算を行う際には頻度分布で用いる階級に合わせて離散化を行う．式 (5) で定義した乖離度 d は，分布関数 $f(x)$，$g(x)$ の内積を正規化したものに相当し，これによって関数 $f(x)$，$g(x)$ 間における乖離の度合いを 0〜1 の値で表現することができる．

3. 提案手法の性能評価

本章では，実トラヒックデータをもとにしたシミュレーションにより，提案手法の評価を行う．以下，3.1 節ではシミュレーションによる評価を行う際の条件について述べる．次に 3.3.1 項で乖離度 d の振舞いについて述べ，3.3.2〜3.3.5 項において提案手法によるフィルタリング結果について示す．なお，3.3.4，3.3.5 項で，到着レート分布作成および到着レート算出に用いるキューの影響について調べるが，ここで用いるキューとは，ノードに到着したパケットを直接格納するバッファとしてではなく，到着レートや観測属性値の分布を計算する際に必要となる，直近のパケットから得られる観測情報（ノードへの到着時間や Dport，Psize）を管理するために用いるものである．したがって，パケットそのものはキューに格納されないため，ノードを通過する様々な End-to-End のトラヒックにおける個々のパケットそのものの流れに影響を与えるものではないことに注意されたい．

3.1 シミュレーション設定

実トラヒックデータとして MAWI [12] のインターネットトレースアーカイブを用いた．その中で 900 sec の間記録されたトレースデータを使用することにし，観測日によってどのような差異が存在するのかを調べるために異なる 3 日のトラヒックデータを用意した．このトラヒックデータ 3 つをそれぞれ A，B，C とする．このトレースデータ中には DDoS 攻撃が含まれていないことがあらかじめ確認済みであるため，人工的に生成した攻撃トラヒックを付加し評価を行う．

付加する攻撃トラヒックデータは，使用するトレースデータの最初のパケットレコードから 120 sec 後に開始し，60 sec の間継続されるものとする．Web サーバに対する DDoS 攻撃を想定し，攻撃パケットのパラメータとして送信先ポート番号は Web サーバのポートとして用いられる 80 番とし，パケットサイズは 100 byte とした．攻撃パケットの到着間隔は指数分布で決定するものと，一様分布で決定するものの 2 つのパターンを用意する．ここで一様分布を仮定する理由としては，本提案手法においては攻撃トラヒックの到着分布について分布や前提知識を仮定とする必要がないため，到着分布における事前情報がない場合でのフィルタリング性能を評価するためである．

攻撃のビットレートの違いによる比較を行うために，正常トラヒックのレートの 1 倍，1/2 倍，1/5 倍，1/10 倍，1/30 倍の 5 つの攻撃パターンを用意した．一例として，到着間隔が指数分布に従い，正常トラヒックに対して 1/10 倍のトラヒックレートを持つ攻撃を付加した場合のビットレートの変動を**図 2** に示す．横軸はトレースデータに含まれるパケットの最初の到着時間からの経過時間を表しており，縦軸はビットレートを表している．

あらかじめ作成する分布 $P(\boldsymbol{x}|L)$ にも 2 つのパターンを用意し，結果の違いを調査する．検証するトラヒックデータとは異なる日時のデータから 1 日分のトラヒックデータを任意に選択し，分布 $P(\boldsymbol{x}|L)$ を作成しフィルタリングに用いる場合と，異なる日時のすべてのト

© 2011 Information Processing Society of Japan

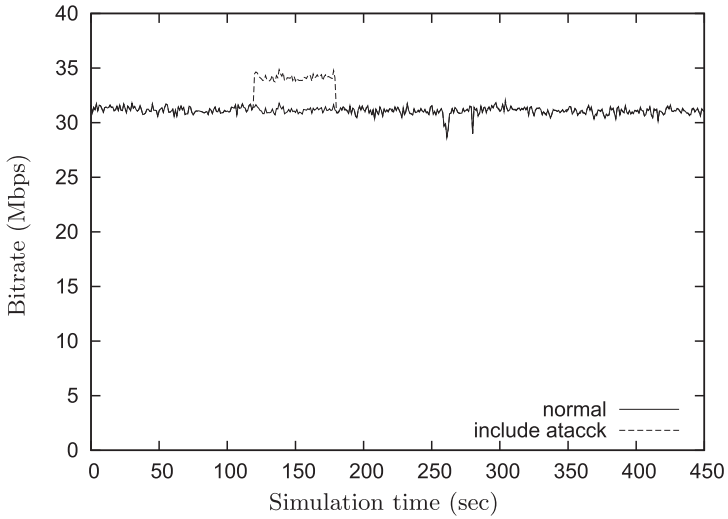

図 2　1/10 倍の攻撃を付加したトラヒックのビットレートの変動
Fig. 2　Traffic behavior with 1/10 intensity attack traffic.

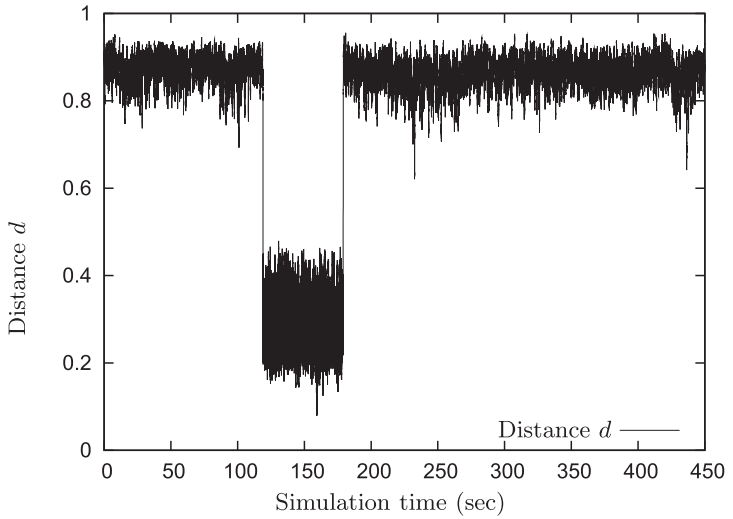

図 3　乖離度 d の変動
Fig. 3　Behavior of distance d.

ラヒックデータを用いて分布 $P(\boldsymbol{x}|L)$ を作成しフィルタリングに用いた場合について考察を行う．通常，事後確率を用いるベイズ推定などでは観測属性の 2 つの情報を独立として扱う場合が多いが，本研究では 2 つの要素を独立として扱わず，$P(\boldsymbol{x}|L)$ を送信先ポート番号とパケットサイズの結合分布として扱う．

3.2　性 能 指 標

DDoS 攻撃のパケットを選択的に破棄する手法においては，攻撃パケットを誤って通過させないことと正規のパケットを誤って遮断しないことが重要になってくる．そこで性能指標として本稿では誤通過率と誤遮断率を定義する．これらはそれぞれ以下の式で与えられる．

$$\text{誤通過率 (False Negative)} = \frac{\text{攻撃パケットが正常判定された数}}{\text{攻撃パケットの総数}}$$

$$\text{誤遮断率 (False Positive)} = \frac{\text{正常パケットが異常判定された数}}{\text{正常パケットの総数}}$$

これら 2 つの指標を用いて提案手法の性能の評価を行うこととする．

3.3　シミュレーション結果

3.3.1　乖離度 d の振舞い

図 3 は，正常トラヒックと同じビットレートを持ち，到着時間間隔が指数分布に従う攻撃トラヒックを加えたデータに対して，パケットの到着ごとに式 (5) に従って計算した乖離度 d の変動を表したものである．横軸はトレースデータに含まれるパケットの最初の到着時間からの経過時間を表しており，縦軸はパケットが到着するたびに計算される，乖離度 d を表している．攻撃トラヒックは，トレースデータの最初のパケットレコードから 120 sec 後に開始し，60 sec の間継続される．

図 3 から分かるように，攻撃が開始する 120 sec の時点から，乖離度 d はおおよそ 0.2〜0.4 の値をとる．一方，攻撃が行われていないそれ以外の部分では，乖離度 d は 0.8〜1.0 の値をとることが分かる．

3.3.2　1 日のトラヒックデータから作成した分布による結果

実際にフィルタリングを行う際には，事前に正常なトラヒックデータからあらかじめパケットサイズと送信先ポート番号を観測属性値とした分布 $P(\boldsymbol{x}|L)$ を作成する必要がある．そのため，検証に用いるトラヒックデータとは異なる 1 日分のデータから分布を作成し，フィル

© 2011 Information Processing Society of Japan

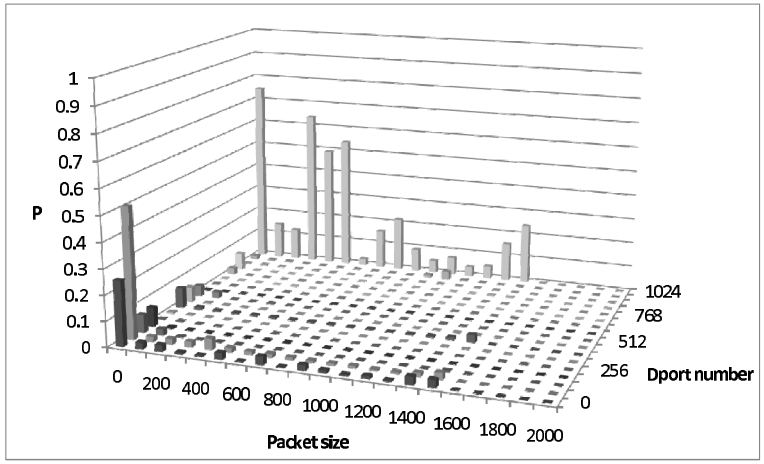

図 4　パケットサイズ，送信先ポート番号による属性値分布
Fig. 4　Distribution of packet property with packet size and destination port number.

タリング性能について検証を行う．ここで，パケットの観測属性値としてパケットサイズ，送信先ポート番号を用いたときの属性値分布を**図 4** に示す．ここで図 4 から属性値分布の全確率が 1 を超えていることが分かるが，これは 2.1 節で述べたとおり複数の期間に分割したデータから得られる分布の中で，最も高い頻度を用いて分布を作成するためである．

図 5 は，正常トラヒックの 1/10 倍のビットレートを持つ攻撃を付加したトラヒックに対し，フィルタを適用した際のビットレートの変動を表している．横軸はトレースデータに含まれるパケットの最初の到着時間からの経過時間，縦軸はビットレートである．この図から 120〜180 sec の間に加えた攻撃トラヒックを除去し，付加した分のビットレートだけを削除できていることが分かる．次にそれぞれのシミュレーションにおいて，誤通過率と誤遮断率をまとめたものを**表 1**，**表 2**，**表 3**，**表 4**，**表 5**，**表 6** に示す．

これらの表から誤遮断率・誤通過率ともに攻撃のレートによらず，ほとんどの状態で 1% 未満となっていることが分かる．誤遮断率は攻撃のレートが高くなるにつれて高くなる傾向があり，誤通過率は攻撃のレートが低くなるにつれて高くなる傾向がある．

攻撃の到着間隔に関しては一様分布で決定されるものよりも指数分布で決定される方が除去しにくく，攻撃のレートが高いときに差が大きい．これは，正常トラヒックのモデルとしてガンマ分布を選択したが，指数分布はガンマ分布のパラメータが $\alpha = 1$ のときであるた

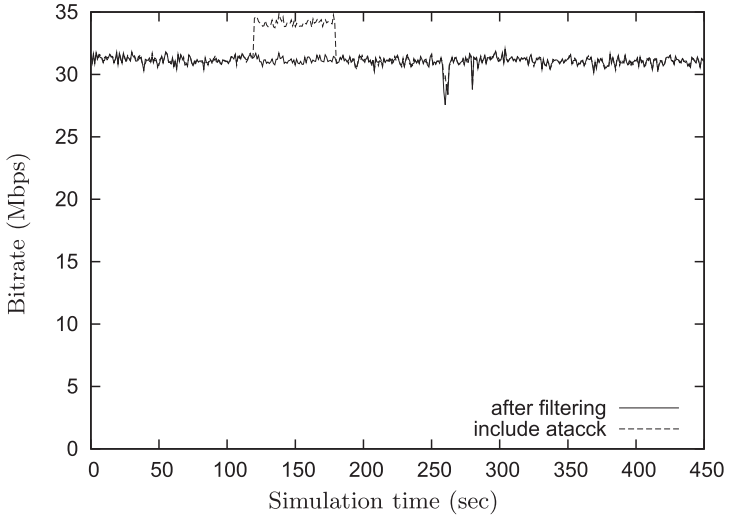

図 5　1/10 倍の攻撃を付加したトラヒックのフィルタリング前後のビットレートの変動
Fig. 5　Filtering result with 1/10 intensity attack traffic.

表 1　指数分布で決定する到着間隔を持つ攻撃を含むトレースデータ A をフィルタリングした結果
Table 1　Filtering result with exponential interarrival attack of trace data A.

	×1/30	×1/10	×1/5	×1/2	×1
正規パケットが正常判定された数	9,716,293	9,716,281	9,716,287	9,716,287	9,586,577
正規パケットが異常判定された数	3,470	3,482	3,476	3,476	133,186
攻撃パケットが正常判定された数	168	180	175	154	159
攻撃パケットが異常判定された数	75,058	224,913	448,118	1,127,311	2,246,830
誤遮断率（%）	0.036	0.036	0.036	0.036	1.370
誤通過率（%）	0.223	0.080	0.039	0.014	0.007

表 2　一様分布で決定する到着間隔を持つ攻撃を含むトレースデータ A をフィルタリングした結果
Table 2　Filtering result with uniform interarrival attack of trace data A.

	×1/30	×1/10	×1/5	×1/2	×1
正規パケットが正常判定された数	9,716,292	9,716,117	9,714,839	9,715,634	9,716,287
正規パケットが異常判定された数	3,471	3,646	4,924	4,129	3,476
攻撃パケットが正常判定された数	176	179	176	177	171
攻撃パケットが異常判定された数	74,825	224,541	450,952	1,131,899	2,222,052
誤遮断率（%）	0.036	0.038	0.051	0.042	0.036
誤通過率（%）	0.235	0.080	0.039	0.016	0.008

© 2011 Information Processing Society of Japan

表 3　指数分布で決定する到着間隔を持つ攻撃を含むトレースデータ B をフィルタリングした結果
Table 3　Filtering result with exponentioal interarrival attack of trace data B.

	×1/30	×1/10	×1/5	×1/2	×1
誤遮断率（%）	0.065	0.041	0.032	0.039	2.256
誤通過率（%）	0.205	0.075	0.037	0.015	0.007

表 4　一様分布で決定する到着間隔を持つ攻撃を含むトレースデータ B をフィルタリングした結果
Table 4　Filtering result with uniform interarrival attack of trace data B.

	×1/30	×1/10	×1/5	×1/2	×1
誤遮断率（%）	0.065	0.040	0.051	0.026	0.016
誤通過率（%）	0.196	0.074	0.038	0.015	0.008

表 5　指数分布で決定する到着間隔を持つ攻撃を含むトレースデータ C をフィルタリングした結果
Table 5　Filtering result with exponential interarrival attack of trace data C.

	×1/30	×1/10	×1/5	×1/2	×1
誤遮断率（%）	0.048	0.048	0.048	0.048	4.703
誤通過率（%）	0.169	0.059	0.034	0.015	0.007

表 6　一様分布で決定する到着間隔を持つ攻撃を含むトレースデータ C をフィルタリングした結果
Table 6　Filtering result with uniform interarrival attack of trace data C.

	×1/30	×1/10	×1/5	×1/2	×1
誤遮断率（%）	0.048	0.050	0.059	0.051	0.048
誤通過率（%）	0.164	0.058	0.027	0.012	0.007

め，分布の乖離度 d に影響を与えにくいと考えられる．従来研究[11] での実験の中で最も小さい攻撃のレートは正常パケットと同じビットレートを持つものであり，その結果は誤遮断率 0.0%，誤通過率は 41.02%である．提案手法の結果はそれ以下の攻撃のレートにおいて，誤遮断率は多少高くはなるが誤通過率に関しては大幅に改善できているといえる．また，任意の時間に攻撃を挿入した場合においても，同様の結果が得られることは検証済みである．

フィルタリングの結果，誤通過させてしまった攻撃パケット数から計算すると，3 pps（Packet/s）程度の攻撃にまで攻撃パケットをレートを減少させることになる．文献 13), 14) では低レートの DoS 攻撃に対する Traceback 手法の提案を行っているが，これらの研究が対象としている低レート DoS として扱っている攻撃トラヒックレートは 20〜100 pps 程度となっており，本提案手法を用いることによってより低い攻撃レートまでフィルタリングできることが分かる．

表 7　指数分布で決定する到着間隔を持つ攻撃を含むデータ A をフィルタリングした結果（複数日）
Table 7　Filtering result with exponentioal interarrival attack of trace data A (5 days samples).

	×1/30	×1/10	×1/5	×1/2	×1
誤遮断率（%）	0.012	0.012	0.012	0.012	0.386
誤通過率（%）	0.459	0.155	0.085	0.027	0.013

表 8　一様分布で決定する到着間隔を持つ攻撃を含むデータ A をフィルタリングした結果（複数日）
Table 8　Filtering result with uniform interarrival attack of trace data A (5 days samples).

	×1/30	×1/10	×1/5	×1/2	×1
誤遮断率（%）	0.012	0.012	0.012	0.012	0.012
誤通過率（%）	0.449	0.139	0.080	0.032	0.018

表 9　指数分布で決定する到着間隔を持つ攻撃を含むデータ B をフィルタリングした結果（複数日）
Table 9　Filtering result with exponentioal interarrival attack of trace data B (5 days samples).

	×1/30	×1/10	×1/5	×1/2	×1
誤遮断率（%）	0.024	0.012	0.011	0.012	1.450
誤通過率（%）	0.520	0.160	0.087	0.030	0.014

表 10　一様分布で決定する到着間隔を持つ攻撃を含むデータ B をフィルタリングした結果（複数日）
Table 10　Filtering result with uniform interarrival attack of trace data B (5 days samples).

	×1/30	×1/10	×1/5	×1/2	×1
誤遮断率（%）	0.021	0.012	0.026	0.016	0.011
誤通過率（%）	0.501	0.146	0.080	0.034	0.017

3.3.3　複数日のトラヒックデータから作成した分布による結果

次に，複数日のトラクックデータから作成した分布 $P(\boldsymbol{x}|L)$ を用いて，フィルタリング性能の検証を行った結果を**表 7**，**表 8**，**表 9**，**表 10**，**表 11**，**表 12** に示す．実際に分布 $P(\boldsymbol{x}|L)$ を作成する際には，検証データと同じサンプルポイントで収集したデータのうち，異なる日に収集された 5 日分のトレースデータを用いた．

これらの結果から，1 日のトラヒックデータから分布 $P(\boldsymbol{x}|L)$ を作成するよりも複数日のトラヒックデータから分布を作成する方が誤通過率は多少上がるが，誤遮断率はそれよりも大きく下がることが分かる．このことから分布を作る方法としては複数日のトラヒックデータから作成する方が良いと考えられる．

3.3.4　到着レート分布作成用のキューの長さ

到着レート分布作成用のキューの長さは長くすればするほど分布の精度は高くなるが，攻

© 2011 Information Processing Society of Japan

表 11　指数分布で決定する到着間隔を持つ攻撃を含むデータ C をフィルタリングした結果（複数日）
Table 11　Filtering result with exponentioal interarrival attack of trace data C (5 days samples).

	×1/30	×1/10	×1/5	×1/2	×1
誤遮断率（%）	0.013	0.013	0.013	0.013	3.326
誤通過率（%）	0.478	0.119	0.081	0.033	0.014

表 12　一様分布で決定する到着間隔を持つ攻撃を含むデータ C をフィルタリングした結果（複数日）
Table 12　Filtering result with uniform interarrival attack of trace data C (5 days samples).

	×1/30	×1/10	×1/5	×1/2	×1
誤遮断率（%）	0.013	0.014	0.018	0.015	0.013
誤通過率（%）	0.483	0.115	0.059	0.023	0.017

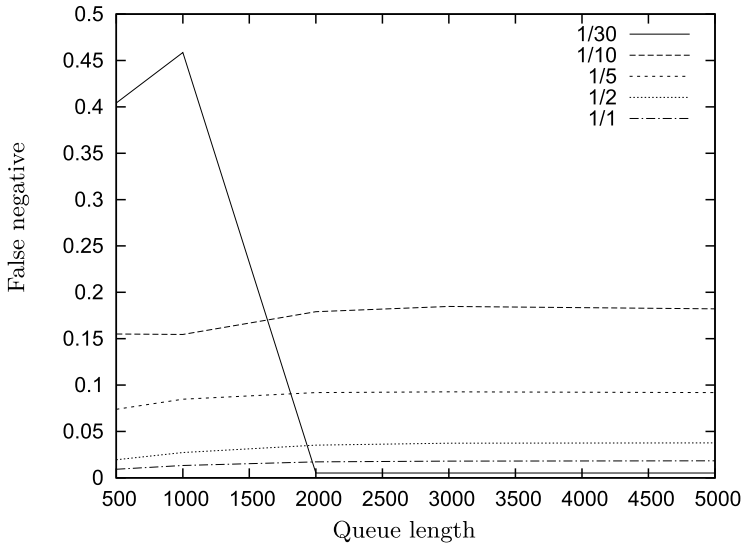

図 6　到着レート分布作成用のキューの長さによる誤通過率の変動
Fig. 6　False negative with queue variation for rate distribution.

撃への反応までの時間が長くなると想定される．そういったことから最適なキューの長さを調べるためにキューの長さを 500，1,000，2,000，3,000，5,000 と変化させ，誤遮断率・誤通過率への影響を調べる．このとき到着レート算出用のキューの長さは固定し，分布は複数日のトラヒックデータから作成したものを使用する．トラヒックデータ A に対してフィルタリングを行った結果を**図 6** と**図 7** に示す．

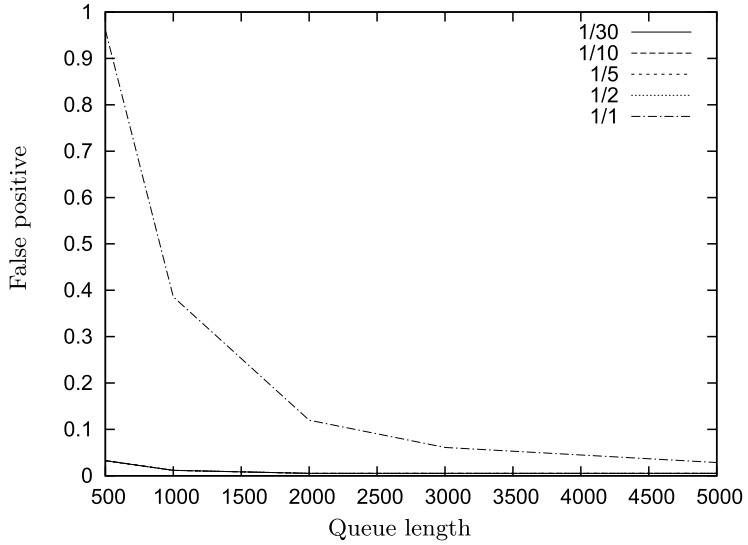

図 7　到着レート分布作成用のキューの長さによる誤遮断率の変動
Fig. 7　False positive with queue variation for rate distribution.

図 6，図 7 の横軸はキューの長さを表しており，縦軸は誤通過率もしくは誤遮断率を表している．図 6 より誤通過率は攻撃のビットレートが正常トラヒックのレートの 1/30 倍の場合は，キューの長さが 2,000 以上になるとき大きく下がることが分かる．その他の攻撃のビットレートの場合はキューの長さが長くなるほど誤通過率がわずかに上がる，あるいは一定となる．図 7 より攻撃のビットレートが正常トラヒックのレートと等しい場合はキューの長さが長くなるほど誤遮断率は減少していくことが分かる．グラフでは重なって見えるその他の攻撃のビットレートの場合はキューの長さによる変動はわずかであることが分かる．トラヒックデータ B，C に関しての実験も同様の傾向が見られた．

次に，以下に到着レート分布作成用キューの長さごとの乖離度の動きを**図 8** に示す．横軸はトレースデータに含まれるパケットの最初の到着時間からの経過時間を表しており，縦軸は乖離度を表している．キューの長さが長くなるほど攻撃への反応までの時間が長くかかっていることが分かる．また，キューの長さを短くすると乖離度が安定しないことも分かる．以上のことから誤通過率，誤遮断率，攻撃への反応までの時間などを考慮すると，到着

© 2011 Information Processing Society of Japan

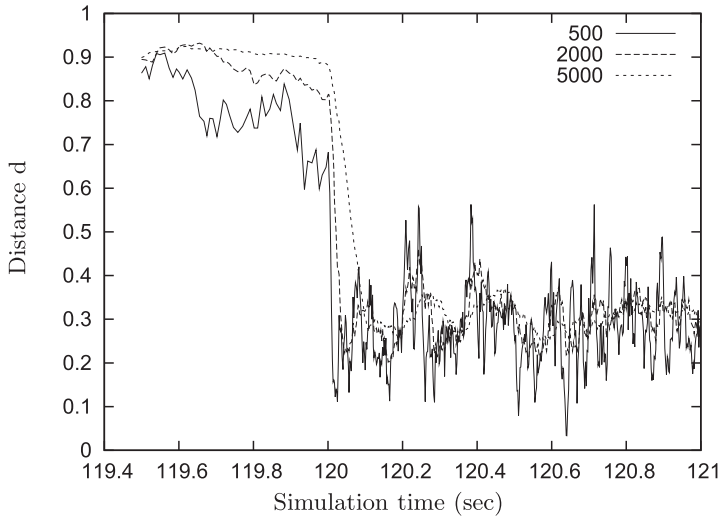

図 8　到着レート分布作成用キューの長さごとの乖離度の変動
Fig. 8　Behavior of distance d with queue variation for avarage rate calculation.

レート分布作成用のキューの長さは 2,000 程度が適当であると考えられる．

3.3.5　到着レート算出用のキューの長さ

次に到着レート算出のキューの長さを調査する．到着レート算出用のキューの長さは短くすればするほど，乖離度の反応が早くなるが，例外的な到着間隔の影響を受けやすくなることが考えられる．そこで，最適なキューの長さを調べるために，キューの長さを 25，50，100，200 と変化させ，誤遮断率・誤通過率への影響を調べる．このとき到着レート分布作成用のキューの長さは 2,000 に固定し，分布は複数日のトラヒックデータから作成したものを使用する．トラヒックデータ A に対してフィルタリングを行った結果を**図 9** と**図 10** に示す．

図 9，図 10 の横軸はキューの長さを表しており，縦軸は誤通過率もしくは誤遮断率を表している．図 9 からはキューの長さが小さいほどすべての攻撃のビットレートにおいて誤通過率が低くなるか一定であることが分かる．図 10 からは攻撃のビットレートが正常トラヒックのレートと等しい場合は小さくするほど誤遮断率は低くなることが分かる．グラフでは重なって見えるその他の攻撃のビットレートの場合は，キューの長さによる変動はわずかであることが分かる．トラヒックデータ B，C に関しての実験も同様の傾向が見られた．

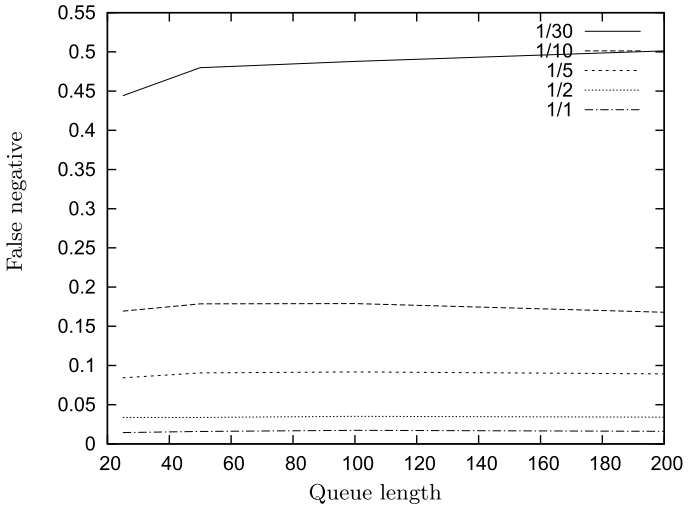

図 9　到着レート算出用のキューの長さによる誤通過率の変動
Fig. 9　False negative with queue variation for arrival rate calculation.

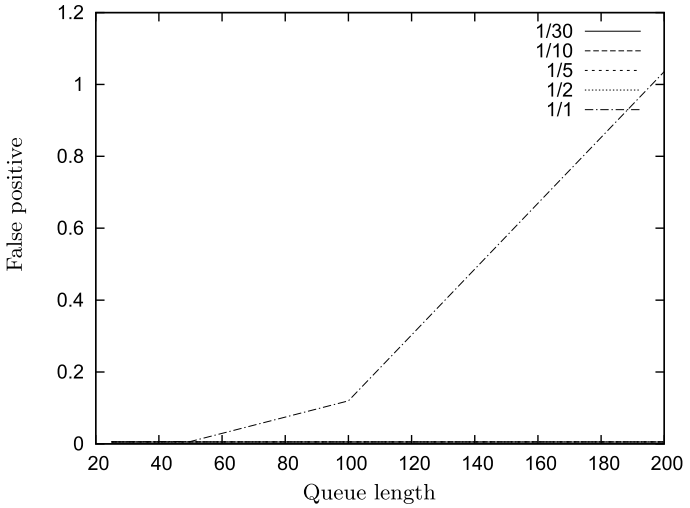

図 10　到着レート算出用のキューの長さによる誤遮断率の変動
Fig. 10　False positive with queue variation for arrival rate calculation.

© 2011 Information Processing Society of Japan

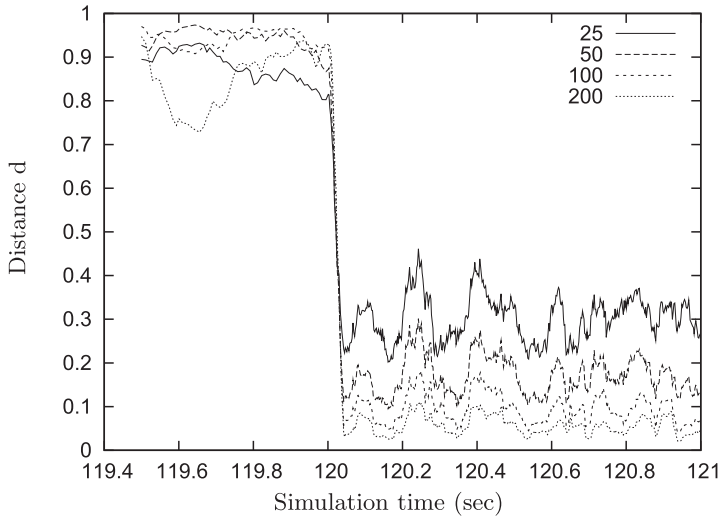

図 11　到着レート算出用キューの長さごとの乖離度の変動
Fig. 11　Behavior of distance d with queue variation for arrival rate calculation.

次に，以下に到着レート算出用のキューの長さごとの乖離度の動きを**図 11** に示す．横軸はトレースデータに含まれるパケットの最初の到着時間からの経過時間を表しており，縦軸は乖離度を表している．攻撃への反応までの時間への影響は少ないことが分かる．

以上のことから誤通過率，誤遮断率，攻撃への反応までの時間などを考慮すると，到着レート算出用のキューの長さは 25 程度が適当であると考えられる．

4. まとめと今後の課題

本研究では，トラヒックの統計的性質を利用した DDoS 攻撃のフィルタリング手法を提案し，シミュレーションによる評価を行った．提案手法では，正常時におけるパケットの到着レート分布と観測パケットから得られる到着レート分布との乖離度に注目した．加えて，観測パケットの属性値分布に着目し，観測パケットが攻撃パケットである事後確率を求めることによって，パケットのフィルタリング手法を設計した．

シミュレーションによる評価により，提案手法が攻撃トラヒックのレートが低い場合においても，攻撃トラヒックを検知して異常パケットを選択的に破棄することができていることが確認できた．さらに設定可能なパラメータについても調査を行い，適切なパラメータを確認することもできた．シミュレーションによる評価では，攻撃トラヒックのレートが正常トラヒックのレートの 1/30 程度まで実験を行っているが，これより低い攻撃トラヒックを加えた場合は，急激にフィルタリング性能が低下することを筆者らは確認している．これは，攻撃トラヒックのレートが低下することによって，通常トラヒックの高い到着レートの間に素の特徴が埋もれてしまい，乖離度 d がほとんど反応しなくなるためと考えられる．

今後の課題としては，このような極端に攻撃トラヒックのレートが低い場合でも，検出可能なフィルタリング手法の開発があげられる．

参 考 文 献

1) Garber, L.: Denial-of-Service Attacks Rip the Internet, *Computer*, pp.12–17 (Apr. 2000).
2) Vixie, P., Sneeringer, G. and Schleifer, M.: Events of 21-Oct-2002 (Nov. 2002). available at http://c.root-servers.org/october21.txt
3) Moore, D., Voelker, G.M. and Savage, S.: Inferring internet Denial-of-Service activity, *Proc. 2001 USENIX Security Symposium*, p.922 (Aug. 2001).
4) Leiwo, J., Nikander, P. and Aura, T.: Towards network denial of service resistant protocols, *Proc. 15th International Information Security Conference* (*IFIP/SEC 2000*) (2000).
5) Handley, M. and Greenhalgh, A.: Steps towards a DoS-resistant internet architecture, *FDNA '04*: *Proc. ACM SIGCOMM Workshop on Future Directions in Network Architecture*, New York, NY, USA, p.4956, ACM Press (2004).
6) Peng, T., Leckie, C. and Ramamohanarao, K.: Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems, *ACM Comput. Surv.*, Vol.39, No.1, pp.1–42 (2007).
7) CERT1996, CERT advisory CA-1996-21 TCP SYN flooding and IP spoofing attacks (Sep. 1996). http://www.cert.org/advisories/CA-1996-21.html
8) Gil, T.M. and Poletto, M.: MULTOPS: A data-structure for bandwidth attack detection, *Proc. 10th USENIX Security Symposium* (2001).
9) Wang, H., Zhang, D. and Shin, K.G.: Detecting SYN flooding attacks, *Proc. IEEE INFOCOM 2002*, Vol.3, pp.1530–1539 (2002).
10) Ohshita, Y., Ata, S. and Murata, M.: Detecting Distributed Denial-of-Service Attacks by Analyzing TCP SYN Packets Statistically, *IEICE Trans. Comm.*, Vol.E89-B, No.10, pp.2868–2877 (2006).
11) Kim, Y., Lau, W.C., Chuah, M.C. and Chao, H.J.: PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks, *IEEE Trans. Dependable and Secure Computing*, Vol.3, No.2, pp.141–155 (2006).

© 2011 Information Processing Society of Japan

12) http://tracer.csl.sony.co.jp/mawi/
13) Kuzmanovic, A. and Knightly, E.: Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants), *Proc. ACM SIGCOMM 2003* (Aug. 2003).
14) 高田友則，中山雅哉：低レート DoS 攻撃の攻撃者特定に有効な改良型 ICMP Traceback，電子情報通信学会論文誌 B，Vol.J91-B, No.10, pp.1203–1210 (2008).

(平成 22 年 5 月 31 日受付)
(平成 22 年 11 月 5 日採録)

三島　大季

2009 年関西大学工学部システムマネジメント工学科卒業．現在，関西大学大学院ソーシャルデザイン専攻都市システム工学分野在籍．ネットワークセキュリティの研究に従事．電子情報通信学会会員．

安達　直世

1996 年立命館大学理工学部電気電子工学科卒業．1998 年奈良先端科学技術大学院大学博士前期課程修了．同年三洋電機（株）入社．2001 年奈良先端科学技術大学院大学博士後期課程修了．同年より同大情報科学研究科助手．2006 年関西大学工学部助手．2007 年関西大学環境都市工学部助教．情報通信システムのモデル化と性能評価に関する研究に従事．博士（工学）．電子情報通信学会，システム制御情報学会各会員．

滝沢　泰久（正会員）

1983 年京都工芸繊維大学工芸学部機械工学科卒業．同年日本ユニシス（株）入社．1990 年住友金属工業（株）入社．1998 年 ATR 環境適応研究所出向．2002 年（株）国際電気通信基礎技術研究所適応コミュニケーション研究所主任研究員．2008 年同研究所上級主任研究員．2009 年関西大学環境都市工学部准教授，ATR 客員研究員．現在，無線ネットワークにおける自己組織化等の研究に従事．工学博士．電子情報通信学会，IEEE，IEEE-CS 各会員．

© 2011 Information Processing Society of Japan