Vol.2011-DPS-146 No.8
Vol.2011-CSEC-52 No.8
2011/3/10

事後確率を用いた DDoS 攻撃に対する統計的フィルタリング手法の評価

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一つである．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わかった．

Statistical Filtering Method against DDoS Attacks With 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，これらの情報を元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

†1 関西大学大学院 理工学研究科 〒 564-8680 大阪府吹田市山手町 3-3-35
Graduate School of Engineering, Kansai University 3-3-35 Yamate-cho, Suita-shi, Osaka, 564-8680 Japan
†2 関西大学 環境都市工学部 〒 564-8680 大阪府吹田市山手町 3-3-35
Faculty of Environmental and Urban Engineering, Kansai University 3-3-35 Yamate-cho, Suita-shi, Osaka, 564-8680 Japan

Vol.2011-DPS-146 No.8
Vol.2011-CSEC-52 No.8
2011/3/10

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る舞いをモデル化し，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時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) の手法は攻撃の探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. 提案手法

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使用し，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

Vol.2011-DPS-146 No.8
Vol.2011-CSEC-52 No.8
2011/3/10

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．従って，$\boldsymbol{x}$ 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．

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

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時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，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．

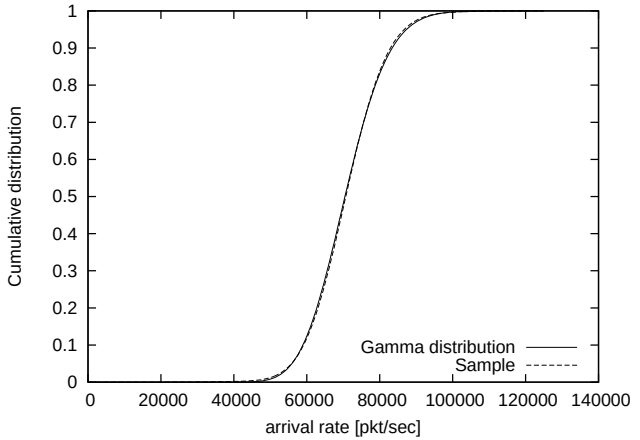

図 1 到着レートの累積確率分布．

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[12] 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は確認済みである．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無

Vol.2011-DPS-146 No.8
Vol.2011-CSEC-52 No.8
2011/3/10

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．

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

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) にて用いる．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．

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

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．

以上が $P(L)$ の導出方法になるが，このとき 3 つのパラメータを設定しなくてはならない．それは平均到着レート算出個数，ヒストグラム作成個数，階級の幅である．これらの値が変化すると結果に影響を与えると考えられるので，シミュレーションの際にはパラメータを変えることで結果を調査する．

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 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 で乖離度 d の振る舞いについて述べ，3.3.2 では $P(\boldsymbol{x}|L)$ 算出時のパラメータの調査を行う．最後に 3.3.3 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．

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 のインターネットトレースアーカイブを用いてシミュレーションを行い，提案手法を評価する．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 120sec 後に開始し，60sec 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 100byte 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無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，1/30 倍，1/100 倍の 5 つの攻撃パターンを用意した．

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．

$$\text{誤通過率} = \frac{\text{攻撃パケットが正常判定された数}}{\text{攻撃パケットの総数}}$$
$$\text{誤遮断率} = \frac{\text{正常パケットが異常判定された数}}{\text{正常パケットの総数}}$$

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 の振る舞い

図 2 は，正常トラヒックと同じビットレートを持ち，到着時間間隔が一様分布に従う攻撃トラヒックを加えたデータに対して，パケットの到着毎に式 (5) に従って計算した乖離度

Vol.2011-DPS-146 No.8
Vol.2011-CSEC-52 No.8
2011/3/10

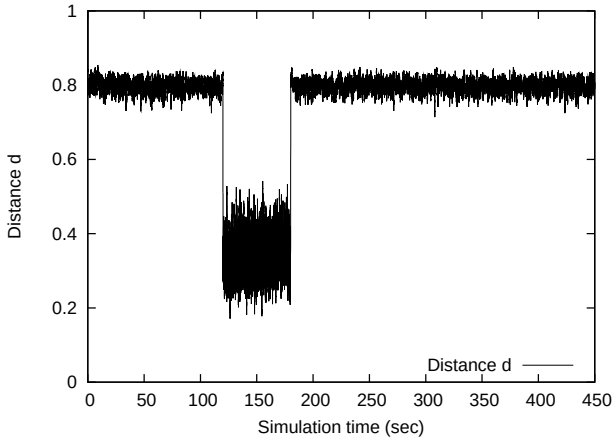

図 2 乖離度 d の変動.

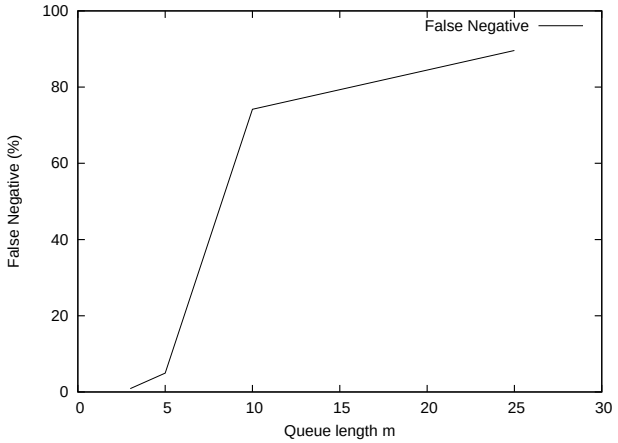

図 3 到着レート算出個数のみを変化させたときの誤通過率の変動.

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わしており，縦軸はパケットが到着する度に計算される，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 120sec 後に開始し，60sec の間継続される．

図 2 から分かるように，攻撃が開始する 120sec の時点から，乖離度 d はおおよそ 0.2 ～ 0.4 の値を取る．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 前後の値を取ることがわかる．

3.3.2 $P(\boldsymbol{x}|L)$ 算出時のパラメータの調整

2.2 で述べたように $P(\boldsymbol{x}|L)$ を算出する際に以下の 3 つのパラメータを設定する必要がある．

(1) 到着レート算出個数 (m)
(2) ヒストグラム作成個数 (n)
(3) 階級の幅 (l)

これらのパラメータの調節を行い，誤遮断率と誤通過率への影響を調べる．それぞれのパラメータを以下に記述するように 4 つずつ用意した．

- m：3，5，10，25
- n：250，500，1000，2000
- l：100，250，500，1000

これらのパラメータを網羅的に設定し，実験を行った．

3.3.2.1 到着レート算出個数の調整

ヒストグラム作成個数を 500，階級の幅を 500 に固定し，到着レート算出個数を変化させたときの誤通過率の変動を**図 3** に，誤遮断率の変動を**図 4** に示す．それぞれ 1/100 倍の攻撃のレートを付加したものをフィルタに適用したときの結果である．

図 3 から到着レート算出個数を減らすと誤通過率が下がる傾向があることがわかる．これは到着レート算出個数が少ないと攻撃パケットが正常パケットに埋もれることを防ぎ，攻撃の特徴を掴みやすいからだと考えられる．図 4 からは到着レート算出個数を減らすと誤遮断率が上がる傾向があることもわかる．これは到着レート算出個数が少ないと正常トラヒックの中での突飛なものの影響を受けるからだと考えられる．

3.3.2.2 ヒストグラム作成個数の調整

次に，到着レート算出個数を 10，階級の幅を 500 に固定し，ヒストグラム作成個数を変化させたときの誤通過率の変動を**図 5** に，誤遮断率の変動を**図 6** に示す．それぞれ 1/100 倍の攻撃のレートを付加したものをフィルタに適用したときの結果である．

図 5 からヒストグラム作成個数を減らすと誤通過率が下がる傾向があることがわかる．これは到着レート算出個数と同様に，ヒストグラム作成個数が少ないと攻撃パケットが正常パ

Vol.2011-DPS-146 No.8
Vol.2011-CSEC-52 No.8
2011/3/10

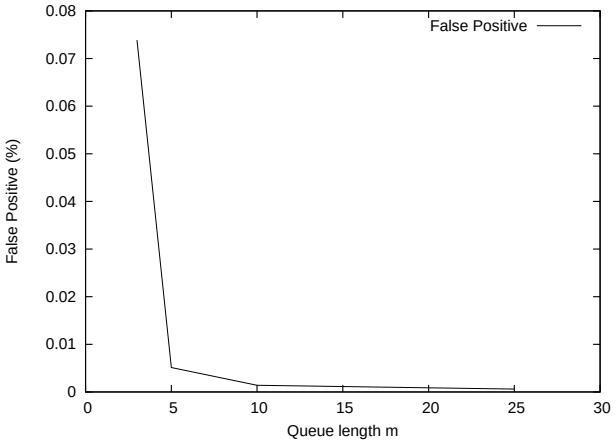

図 4 到着レート算出個数のみを変化させたときの誤遮断率の変動.

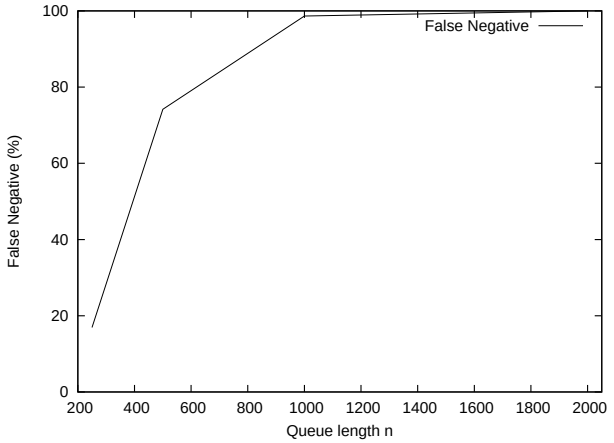

図 5 ヒストグラム作成個数のみを変化させたときの誤通過率の変動.

ケットに埋もれることを防ぎ，攻撃の特徴を掴みやすいからだと考えられる．図 6 からは到着レート算出個数を減らすと誤遮断率が上がる傾向があることもわかる．これは着レート算出個数と同様に，到着レート算出個数が少ないと正常トラヒックの中での突飛なものの影響を受けることや，荒い分布になることから乖離度が全般的に低ってしまうことなどが原因だと考えられる．

3.3.2.3 階級の幅の調整

次に，到着レート算出個数を 10，ヒストグラム作成個数を 500 に固定し，階級の幅を変化させたときの誤通過率の変動を**図 7** に，誤遮断率の変動を**図 8** に示す．それぞれ 1/100 倍の攻撃のレートを付加したものをフィルタに適用したときの結果である．

図 7 から階級の幅を狭くすると誤通過率が下がる傾向があることがわかる．これは階級の幅を狭くすることによって階級数が多くなり，攻撃トラヒックによる到着レートと正常トラヒックによる到着レートとの区別がつきやすくなるということが考えられる．図 8 からは階級の幅を狭くすると誤遮断率が上がる傾向があることもわかる．これは区別がつきやすくなった分，同じ階級に属しているパケットの遮断が増加しているということが原因だと考えられる．

以上のことからパラメータの調節を行うことにより，その傾向に従って誤通過率と誤遮断率の調整を行うことができることがわかる．

3.3.3 提案手法のパラメータ調整を踏まえた評価

前項では到着レート算出個数，ヒストグラム作成個数，階級の幅の 3 つのパラメータを調節による調査を行った．今回行った実験の中で一番良い結果であると考えられるものを示す．パラメータの設定は以下の通りである．

- m = 5
- n = 500
- l = 250

これらのパラメータの設定での，誤通過率と誤遮断率をまとめたものを**表 1** と**表 2** に示す．

表 1 指数分布で決定する到着間隔をもつ攻撃を含むトレースデータをフィルタリングした結果.

	×1	×1/2	×1/5	×1/30	×1/100
正規パケットが正常判定された数	9719172	9719172	9719173	9719178	9719185
正規パケットが異常判定された数	591	591	590	585	578
攻撃パケットが正常判定された数	237	278	301	243	258
攻撃パケットが異常判定された数	2246752	1127187	447992	74983	22173
誤遮断率 (%)	0.0061	0.0061	0.0061	0.0060	0.0059
誤通過率 (%)	0.0105	0.0247	0.0671	0.3230	1.1502

Vol.2011-DPS-146 No.8
Vol.2011-CSEC-52 No.8
2011/3/10

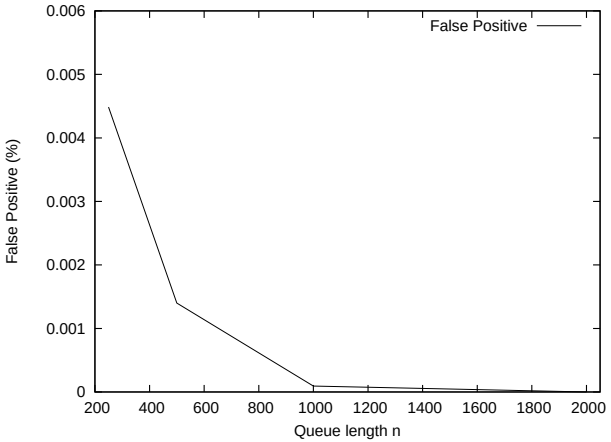

図 6 ヒストグラム作成個数のみを変化させたときの誤遮断率の変動.

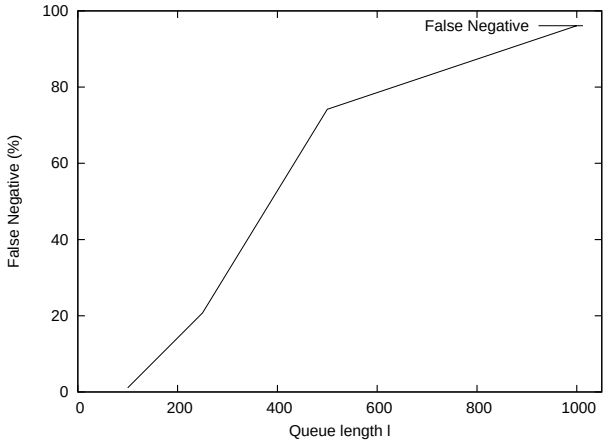

図 7 階級の幅のみを変化させたときの誤通過率の変動.

表 2 一様分布で決定する到着間隔をもつ攻撃を含むトレースデータをフィルタリングした結果.

	×1	×1/2	×1/5	×1/30	×1/100
正規パケットが正常判定された数	9719114	9719172	9719173	9719178	9719184
正規パケットが異常判定された数	649	591	590	585	579
攻撃パケットが正常判定された数	184	209	280	245	232
攻撃パケットが異常判定された数	2222039	1131867	450848	74756	22266
誤遮断率 (%)	0.0067	0.0061	0.0061	0.0060	0.0059
誤通過率 (%)	0.0083	0.0185	0.0621	0.3267	1.0312

表 1，表 2 から 3 つのパラメータの調節を行ったことによって，1/100 倍の攻撃のレートにも対応することができていることがわかる．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．これは攻撃のレートが低くなるほど攻撃と判断しにくくなることが原因であると考えられる．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言える．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，1/100 倍の攻撃のレートでの誤通過させてしまった攻撃パケット数から計算すると，4〜5pps(Packet/s) 程度の攻撃にまで攻撃パケットのレートを減少させることになる．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，これらの研究に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 20〜100pps 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．

これは DDoS 攻撃が集まる前の段階においても有効であると思われる．

4. ま と め

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

Vol.2011-DPS-146 No.8
Vol.2011-CSEC-52 No.8
2011/3/10

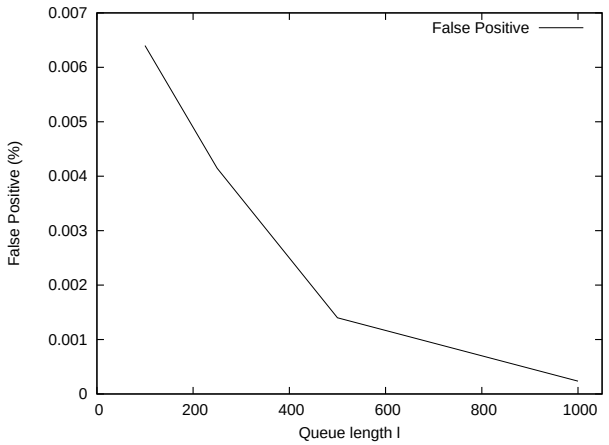

図 8 階級の幅のみを変化させたときの誤遮断率の変動.

が確認できた．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 1/100 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．しかし，今回のシミュレーションの結果からパラメータをより良く調整することによって 1/100 倍の攻撃レートよりも小さな攻撃に対しても対応することができる可能性があると考えられる．

今後の課題としては，極端に攻撃トラヒックのレートが低い場合でも対応できるようなフィルタリング手法の開発，もしくはパラメータの調整などがある．さらにパラメータの調整は本提案手法では手動で行う必要があるため，自動化する方法の模索も課題として挙げられる．

参 考 文 献

1) L. Garber, “Denial-of-Service Attacks Rip the Internet,” Computer, pp. 12-17, Apr. 2000.
2) P. Vixie, G. Sneeringer, and M. Schleifer, “Events of 21Oct2002,” November 2002, available at: http://d.root-servers.org/october21.txt.
3) D. Moore, G. M. Voelker, and S. Savage, “Inferring internet Denial-of-Service activity,” Proceedings of the 2001 USENIX Security Symposium, pp. 922, August 2001.
4) J. Leiwo, P. Nikander, and T. Aura, “Towards network denial of service resistant protocols,” in In Proceedings of the 15th International Information Security Conference (IFIP/SEC 2000), 2000.
5) M. Handley and A. Greenhalgh, “Steps towards a DoS-resistant internet architecture,” in FDNA ’04: Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture. New York, NY, USA: ACM Press, 2004, pp. 4956.
6) T. Peng, C. Leckie and K. Ramamohanarao, “Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems,” ACM Comput Surv, Vol. 39 No. 1, pp. 1-42, April 2007.
7) CERT1996, “CERT advisory CA-1996-21 TCP SYN flooding and IP spoofing attacks,” http://www.cert.org/advisories/CA-1996-21.html, September 1996.
8) T. M. GIL and M. Poletto, “MULTOPS: A data-structure for bandwidth attack detection,” in Proc. Proceedings of the 10th USENIX Security Symposium, 2001
9) H. Wang, D. Zhang and K. G. Shin, “Detecting SYN flooding attacks,” in Proc. IEEE INFOCOM 2002, Vol. 3, pp. 1530-1539, 2002.
10) Y. Ohshita, S. Ata and M. Murata, “Detecting Distributed Denial-of-Service Attacks by Analyzing TCP SYN Packets Statistically,” IEICE Trans. Commun, vol. E89-B, No. 10, pp. 2868-2877, Oct. 2006.
11) Y. Kim, W. C. Lau, M. C. Chuah and H. J. Chao, “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, April-June 2006.
12) http://tracer.csl.sony.co.jp/mawi/
13) A. Kuzmanovic, E. Knightly, “Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants)”, Proc. ACM SIGCOMM 2003, August 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.