社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2006－ＡＶＭ－55（15）
2006／12／15

帯域利用状態に着目したパルス型DoS検知の誤検知と観測コストの低減

荒井健二郎† 角田 裕† 和泉 勇治† 根元 義章†

† 東北大学大学院情報科学研究科 〒980-8579 宮城県仙台市青葉区荒巻字青葉 6-6-05
E-mail: †{kenji,tsuno,wai,nemoto}@nemoto.ecei.tohoku.ac.jp

あらまし パルス型 DoS 攻撃は，低レートな攻撃トラヒックを使用する巧妙かつ検知困難な攻撃である．パルス型 DoS 攻撃に対する既存の検知手法の多くは攻撃トラヒックを構成するパルス列の周期性を検知指標としているが，攻撃者は攻撃トラヒックの送信タイミングを制御することでこれらの検知を回避可能である．筆者らはこれまでに攻撃者による攻撃トラヒックの制御に対応可能な検知手法として，帯域利用状態に着目した PDoS 検知手法を提案している．しかし，この従来手法では誤検知を回避するためにフロー単位での高コストなトラヒック観測が必要であった．そこで，本稿では攻撃時にバーストトラヒックが発生することを利用し，バーストトラヒック発生時にのみ帯域利用状態の解析を行うことでフロー単位での観測を行わずに，誤検知を削減できる低コストな検知手法を提案する．そして，シミュレーションを通して提案手法の検知性能の評価を行う．

キーワード パルス型 DoS 攻撃，検知，帯域利用状態，トラヒックのバースト性

Reducing False Positive and Observation Cost in Bandwidth Usage-based Pulsing DoS Detection Schemes

Kenjiro ARAI†, Hiroshi TSUNODA†, Yuji WAIZUMI†, and Yoshiaki NEMOTO†

† Graduate School of Information Sciences, Tohoku University 6-6-05, Aramaki-Aza-Aoba, Aoba-ku, Sendai,980-8579 Japan
E-mail: †{kenji,tsuno,wai,nemoto}@nemoto.ecei.tohoku.ac.jp

Abstract Pulsing Denial-of-Service (PDoS) attacks seriously degrade the throughput of TCP flow and consequently pose a grave concern to networks. The fact that they generate less traffic than traditional flood-based attacks makes PDoS detection more difficult. Although most of the conventional PDoS detection schemes observe the periodical pattern of the pulse trains, attackers can easily evade the detection system by merely controlling the timing of pulse transmission. The bandwidth usage-based detection scheme, which the authors previously proposed, is robust to the control of attack traffic by attackers. However, the conventional method needs high observation cost because the flow-based traffic analysis is required for reducing false positives. In this paper, we propose a new bandwidth usage-based detection method taking into account the burstiness of traffic which is the principal feature of PDoS attacks. The proposed method can drastically decrease the number of false positives without complicated flow-based traffic analysis. Since the proposed method monitors only aggregated flows, the observation cost is also reduced as compared with the conventional method. Through various simulations, we demonstrate the effectiveness of the proposed method.

Key words Pulsing Denial-of-Service Attacks, Detection, Bandwidth Usage Condition, Burstiness of Traffic

1. はじめに

大量のパケットを標的に対して送りつけることで，ネットワークの帯域やメモリなどのリソースを消費させる Flooding 型 DoS(Denial of Service) 攻撃 [1] は現在のインターネットにおいて深刻な問題となっている．さらに近年ではパルス型 DoS 攻撃 (Pulsing DoS，以下 PDoS) と呼ばれる巧妙な DoS 攻撃の脅威が報告されており [2] [3]，実際に PDoS を行う zombie も発見されている [4]．PDoS の攻撃トラヒックは従来の Flooding 型 DoS 攻撃と異なり平均レートが低く，高レートな攻撃トラヒックが継続的に観測されることを前提とした従来の DoS 攻撃検知方式 [5] [6] では検知が困難である．このことから，PDoS へ

の効果的な対策の確立が急務となっている．

PDoS の効果は TCP フローのスループット低下としてあらわれる．PDoS の攻撃者は，ルータのキューを溢れさせるために，図 1 に示すような短期間の高レートな攻撃トラヒック，即ちパルス状の攻撃トラヒックを間欠的に連続して送信する．PDoS の攻撃パルスがルータに到着するとルータのキューは溢れ，ルータを通過する TCP フローのパケットが破棄されてしまう．パケットロスが発生した TCP フローの送信者は輻輳制御 [7] を行い，その転送レートに相当するウインドウサイズを減少させる．攻撃パルスが到着するたびに TCP フローのウインドウサイズが低下するので，PDoS 時にはルータを通過する TCP フローは小さなウインドウサイズでの通信を強いられ，スループットが大きく低下してしまう．

PDoS が及ぼす影響はパルス列のパラメータによって異なり，文献 [2] では 1 秒周期のパルス列による PDoS が最も効果的であることが指摘されている．TCP の再送タイムアウト (RTO:Retransmission Time Out) の最小値は 1 秒にすることが推奨されており [8]，1 秒周期のパルス列による PDoS は，攻撃が TCP フローの再送タイミングと同期し，多くの TCP フローの再送パケットを破棄することができるため，効率的に TCP フローのスループットを低下させることができる．

1 秒周期のパルス列による攻撃が最も効果的であることから，文献 [9] [10] [11] では攻撃パルス列の周期性に着目した PDoS 検知手法が提案されている．しかし，ランダムな周期のパルス列であっても PDoS は攻撃として成立するため [12]，攻撃者は攻撃パルスの送信タイミングを制御することで，これらの周期性に基づいた検知を容易に回避できる．従って，攻撃パルスの周期性などといった攻撃者による攻撃トラヒックの制御に対応可能な検知手法が必要である．

攻撃者による攻撃トラヒックの制御に対応可能な検知手法として，筆者らはこれまでにリンクの帯域利用状態を分析し PDoS が原因で引き起こされた輻輳を発見することで PDoS を検知する手法 [13] を提案している．しかし，この検知手法ではフロー単位での観測が必要であるために観測コストが高いという課題がある．また，観測している TCP フローが帯域を使い切れない状況では誤検知が発生する問題がある．

そこで，本稿では PDoS 時に発生するバーストトラヒックが観測されたときにのみ帯域利用状態の解析を行うことで，フロー単位での観測を行わずに誤検知を削減できる低コストな手法を提案する．さらに，TCP のスループット低下，即ち TCP フローの通信品質が劣化したことを正しく判断することで，TCP フローが帯域を使い切れない状況で発生する誤検知を削減する．

以下，2. では帯域利用状態に着目した検知手法とその課題について述べる．3. では 2. で指摘した課題に対して，トラヒックのバースト性を評価し，さらに TCP フローの通信品質が劣化したことを正しく判断することで，課題を解決する手法を提案する．4. ではシミュレーションを通して提案手法の検知性能を評価する．5. は本稿のまとめである．

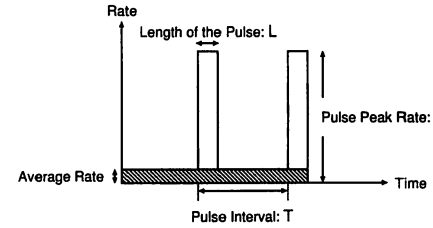

図 1　PDoS の攻撃トラヒックのモデル

2. 帯域利用状態に着目した従来の検知手法

本節では筆者らが提案している帯域利用状態に着目した PDoS 検知手法の概要について述べ，次いでその課題について述べる．

2.1 従来手法の概要

PDoS による輻輳時は通常トラヒックの増大による輻輳時と同様に TCP フローのスループット低下が観測される．従来手法では集約した TCP フロー (以下，集約 TCP フロー) のリンク帯域を基準とした帯域利用率と，全帯域利用率のバランスを評価することで，PDoS による輻輳のみを検知する．以下，従来手法の詳細について述べる．

リンク帯域を Bw，スロット幅を Δt とし，スロット t における各 TCP フローの利用帯域を $B_{tcp-i}(t)$，そしてその総和を $B_{tcp-all}(t)$，全利用帯域を $B_{all}(t)$ としたとき，集約 TCP フローが利用可能な帯域 $B_{avail}(t)$ は式 (1) のように求められる．ただし，N_{flow} は TCP フロー数を表す．

$$\begin{aligned} B_{avail}(t) &= Bw - \{B_{all}(t) - \sum_{i=1}^{N_{flow}} B_{tcp-i}(t)\} \\ &= Bw - \{B_{all}(t) - B_{tcp-all}(t)\} \end{aligned} \quad (1)$$

次に，スロット t における帯域 $B_{avail}(t)$ に対する帯域 $B_{tcp-all}(t)$ の割合を集約 TCP フローの実帯域利用率 $R(t)$ として定義し，スロット t における集約 TCP フローの帯域利用状況を評価する．

$$\begin{aligned} R(t) &= \frac{B_{tcp-all}(t)}{B_{avail}(t)} \\ &= \frac{B_{tcp}(t)}{Bw - \{B_{all}(t) - B_{tcp-all}(t)\}} \end{aligned} \quad (2)$$

さらに，スロット t における全帯域利用率を $U_{all}(t)$，集約 TCP フローの帯域利用率を $U_{tcp-all}(t)$ とすると，式 (2) より式 (3) のように表せる．

$$R(t) = \frac{U_{tcp-all}(t)}{1 - \{U_{all}(t) - U_{tcp-all}(t)\}} \quad (3)$$

通常時の輻輳原因となるイベントの発生時にはみられず PDoS 時にのみ見られる現象は，集約 TCP フローの実帯域利用率 $R(t)$ が長期間に渡って低い値になるということである．この現象を捉えるために，式 (4) に示すウインドウサイズ W[slot] 毎の $R(t)$ の移動平均 $R_{avg}(t)$ を検知の基準として使用する．通常時の輻輳原因となるイベントが発生した場合と，PDoS が発生した場合を識別するために，従来手法では $R_{avg}(t)$ に対して

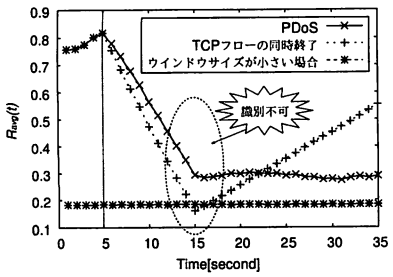

図 2　従来手法において誤検知となる例

閾値を設け，$R_{avg}(t)$ が閾値未満の場合 PDoS として検知する．

$$R_{avg}(t) = \frac{1}{W} \sum_{i=t-W+1}^{t} R(t) \qquad (4)$$

この手法は TCP フローの帯域利用状態に着目しているために，攻撃者による攻撃トラヒックの送信タイミングには影響されず，ランダムな間隔のパルス列による PDoS であっても検知可能であることが大きな特徴である．

2.2　従来手法の課題

2.2.1　観測コストの低減

従来手法では，トラヒックをフロー単位で観測し，個々のフローの帯域利用状態を監視している．これは，フロー数を把握し，TCP フローの終了による集約 TCP フローの実帯域利用率の低下と PDoS による低下を区別するためである．しかし，一般にフロー単位のトラヒック観測は非常に高コストであり，トラヒック流量の異なる様々なネットワークにおいて検知を実施するためには，観測コストの低減が必要である．

2.2.2　誤検知の削減

従来手法では複数の TCP フローが終了した場合には，図 2 のように $R_{avg}(t)$ が PDoS が発生した場合と同程度まで低下してしまうため，PDoS として誤検知してしまうという問題がある．これに対して従来手法では，前述の通りフロー単位での観測によってフロー数の減少を捉え誤検知を回避していた．しかし，観測コスト低減のためには，フロー単位での観測なしでこの誤検知を回避する必要がある．

また，受信者の受信ウインドウが小さい場合や，やりとりするコンテンツのサイズが小さい場合には，TCP フローが帯域を使い切らないために，図 2 に示すように PDoS により低下した場合と同程度に低い $R_{avg}(t)$ が継続し，誤検知してしまうという問題がある．

3.　トラヒックのバースト性評価による帯域利用状態に着目した検知手法の改良

3.1　提案手法の概要

提案手法では，PDoS の検知に際して

- 原因となるバーストトラヒックの存在
- 結果として発生する TCP の通信品質の劣化

の双方を評価し，高性能かつ低コストな検知を実現する．

従来手法では，2.2.1 で述べたように TCP フローの終了を誤検知する可能性があり，その誤検知を回避するためにフロー単位でのトラヒック観測が必要であった．この誤検知は，PDoS の結果として起こり得る，集約 TCP フローの実帯域利用率の低下のみに着目していたことに起因する．そこで，提案手法では図 3 に示すように，PDoS 時に必ず発生する連続的なバーストトラヒックを発見し，その場合にのみ集約 TCP フローの実帯域利用率を評価する．その結果，TCP フローの終了時など，通常時に起こり得る集約 TCP フローの実帯域利用率の低下を PDoS として判断する可能性を大きく低減させることができる．これにより，従来手法で誤検知を避けるために実施していたフロー単位の観測が必要なくなり，提案手法では TCP トラヒックをフローの区別なく観測すれば十分である．

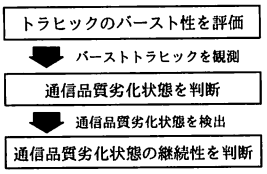

図 3　提案手法の概要

また，2.2.2 で述べたように従来手法では TCP フローが帯域を十分に使い切っていない状況には誤検知するという問題があった．そこで，提案手法では集約 TCP フローの実帯域利用率 $R(t)$ の低下を，前スロットのそれを基準とした相対的な低下として捉えることによりこの誤検知を回避する．集約 TCP フローの実帯域利用率 $R(t)$ が相対的に大きく低下している場合を通信品質劣化状態として定義し，図 3 に示すように，この状態の継続性を判断することで検知を行う．以降ではまず本手法におけるトラヒックのバースト性の評価方法について述べ，次いで通信品質劣化状態の検出方法，および提案検知アルゴリズムについて述べる．

3.2　トラヒックのバースト性の評価方法

提案手法で用いるトラヒックのバースト性の評価指標 $Burstiness$ の算出方法を式 (5) に示す．T_n は n 個のパケットが到着するのに要した時間を表し，S_n は到着した n 個のパケットのサイズの総和を，Bw はリンク帯域を表す．つまり，$Burstiness$ は n パケット単位での bps をリンク帯域 Bw で規格化した値を表す．

$$Burstiness = \frac{S_n}{T_n Bw} \quad (0 < Burstiness \leqq 1) \qquad (5)$$

$Burstiness$ が 0.9 以上の場合，バーストトラヒックが一度観測されたとする．そして，スロット t におけるバーストトラヒックの観測回数 $N_{burst}(t)$ が閾値 Th_{burst} より大きい場合には，短時間のバーストトラヒックが観測されたと判断する．PDoS の攻撃パルスはルータのキューを瞬時に占有することを目的としているため，n をキューサイズと同等に設定し，$Burstiness$ を評価する．

3.3　通信品質劣化状態の検出方法

集約 TCP フローの実帯域利用率 $R(t)$ の低下度合を判断するための相対的な基準 R_c として前スロット $t-1$ における集約

TCP フローの実帯域利用率 $R(t-1)$ を用いる．そして，式 (6) に示すように R_c に対する $R(t)$ の割合を $R_{var}(t)$ と定義する．

$$R_{var}(t) = \frac{R(t)}{R_c} \tag{6}$$

図 4 に示すように，$R_{var}(t)$ が Th_{deg} 未満の場合，スロット t は通信品質劣化状態にあると判断する．そして，スロット t が通信品質劣化状態にある場合には，R_c は更新せずに以降のスロットでも使用する．そして，通信品質劣化状態が一定スロット以上継続しているときに PDoS として検知する．

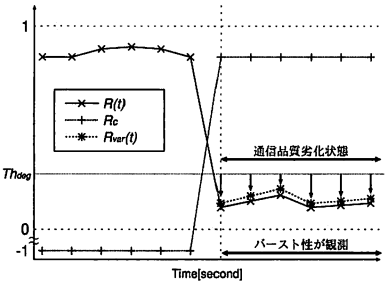

図 4　通信品質劣化状態の検出方法

以上をまとめて図 5 に提案する検知手法のフローチャートを示す．まず，トラヒックのバースト性を評価し，バーストトラヒックの観測回数 $N_{burst}(t)$ が閾値 Th_{burst} より多い場合には通信品質劣化状態検出のフェーズに移る．通信品質劣化状態検出のフェーズでは $R_{var}(t)$ が閾値 Th_{deg} 未満となる通信品質劣化状態が連続しているスロット数 N_d をカウントする．そして N_d が Th_{dur} を上回ったとき，PDoS として検知する．

4. シミュレーションによる検知性能の評価

ns-2 [14] を使用したシミュレーションを通して提案手法の検知性能を評価する．各検知基準の効果を明らかにするために，以下の 3 つの場合について検知性能を評価した．

- $R_{avg}(t)$ を基準とした検知手法
  $R_{avg}(t)$ に対して閾値を設け，閾値未満の場合 PDoS として検知する．
- $R_{var}(t)$ を基準とした検知手法
  $R_{var}(t)$ により通信品質劣化状態を検出し，通信品質劣化状態の継続スロット数が Th_{dur} を上回ったとき，PDoS として検知する．
- トラヒックのバースト性と $R_{var}(t)$ を基準とした提案手法

4.1 シミュレーション環境

シミュレーションのネットワーク構成を図 6 に示す．それぞれ 10 台ずつの FTP Server と Client が，1 本のボトルネックリンクを共有して接続されている．また，Node A と Node B 間では，以下に述べるシミュレーションのシナリオに応じて，PDoS や UDP によるストリーミング通信が行われる．シミュレーションでは，図 6 中の Monitor でのトラヒック観測と観測トラヒックの分析による PDoS 検知を実施する．単位観測時間 Δt は 1 秒とした．また，すべてのリンク帯域は 100Mbps，ルータのキューサイズは 50 パケットとし，すべての通信の RTT は 0.04〜0.1 秒の間でランダムに設定した．各 TCP の送信者のウインドウサイズの最大値は帯域遅延積と等しくなるように設定してあり，シミュレーション開始後 10 秒までに 10 台の FTP Server がランダムに転送を開始する．以降，各シミュレーションの内容について述べる．

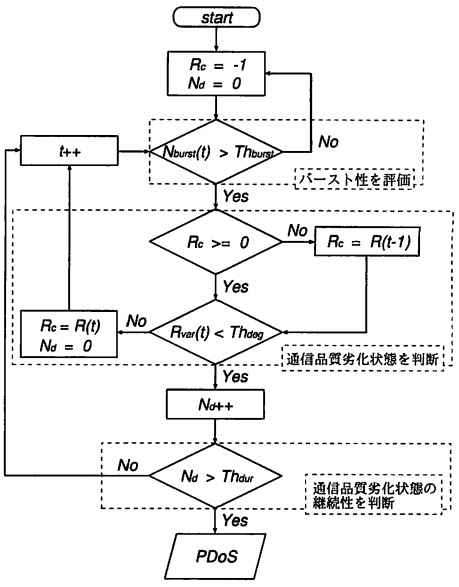

図 5　提案手法の流れ

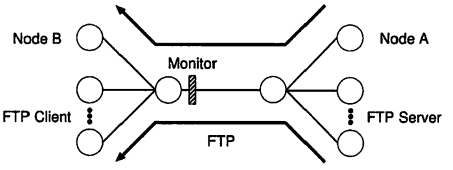

図 6　シミュレーションモデル

(a) PDoS の発生
シミュレーション開始後 30 秒に Node A から Node B へ 64byte のパケットによる PDoS を開始する．ボトルネック部分のルータでの輻輳が PDoS の効果となる．

(b) ストリーミング通信の発生
シミュレーション開始後 30 秒に Node A から Node B に向けて開始する．また，400byte のパケットを用いる．(a) と同様にボトルネック部分のルータで輻輳が発生する．

(c) 複数 TCP フローの同時終了
シミュレーション開始後 30 秒に，10 本の FTP 通信のうち同時に複数本を終了させる．

(d) TCP フローが利用可能な帯域を使い切らない状況
TCP の送信者のウインドウサイズに対して上限を設定する．上限は帯域遅延積に満たない値とするため，TCP フローが帯域を十分に利用しない状況となる．

表 1 に示すように，各シミュレーションについてパラメータの異なる複数のシナリオを用意し，評価を実施した．

表 1　シミュレーション内容

シナリオ	内容	パラメータ設定
(a)-1	シミュレーション開始後 30 秒に PDoS を開始. T=1 秒とする.	R=50Mbps L=0.05 秒
(a)-2		R=50Mbps L=0.1 秒
(a)-3		R=100Mbps L=0.05 秒
(a)-4		R=100Mbps L=0.1 秒
(b)-1	シミュレーション開始後 30 秒にストリーミング通信を を開始.	R=10Mbps
(b)-2		R=30Mbps
(b)-3		R=50Mbps
(c)-1	シミュレーション開始後 30 秒に複数の FTP 通信を終了.	終了フロー数=8
(c)-2		終了フロー数=9
(c)-3		終了フロー数=10
(d)-1	FTP の送信者のウインドウサイズに上限を設定	最大ウインドウサイズ=10
(d)-2		最大ウインドウサイズ=20

4.2 評価項目

各手法の PDoS 検知性能を，False Positve Rate (FPR), False Negative Rate (FNR), Error Rate (ERR) により評価する．False Positive, False Negative, Error はそれぞれ以下のように定義する．

- False Positive (FP)
  シナリオ (b)(c)(d) のシミュレーションにおいて，ストリーミング通信の発生，複数 TCP フローの同時終了，TCP フローが利用可能な帯域を使い切らない状況を誤って PDoS であると検知した場合

- False Negative (FP)
  シナリオ (a) のシミュレーションにおいて，PDoS を検知できなかった場合

- Error (ER)
  シナリオに関らず，False Positive または False Negative となった場合

4.3 シミュレーション結果

各検知手法が最高の性能が得られるパラメータを設定し，その際の検知性能を比較する．そのために，閾値を変化させながら各シナリオについて 100 回ずつシミュレーションを実施し，各手法の FPR, FNR, ERR を評価した．ただし $R_{avg}(t)$ を算出するウインドウ幅 W は 10 スロットとし，品質劣化状態の継続性を判断する際の閾値 Th_{dur} を 5 スロット，$Burstiness$ の算出に用いる n はキューサイズと同じ 50 パケットとした．

$R_{avg}(t)$ を基準とした手法の検知性能とその閾値の関係を図 7 に示し，$R_{var}(t)$ を基準とした手法の検知性能と Th_{deg} の関係を図 8 に示す．またトラヒックのバースト性と R_{var} を検知基準とした提案手法において Th_{burst} を 10 に固定し，Th_{deg} を変動させたときの検知性能を図 9 に示し，Th_{deg} を 0.6 に固定し，Th_{burst} を変動させたときの検知性能を図 10 に示す．そして，これらの結果から各手法において ERR が最小となるときの各評価項目の値をグラフを図 11 に示し，表 2〜5 にはそのときの各シミュレーションにおけるエラー数を示す．

表 3 からわかるように，ストリーミング通信が発生した場合をどの検知手法でも誤検知していないことがわかる．これは，

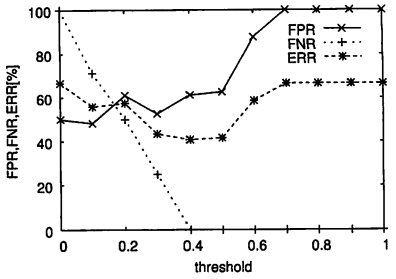

図 7　$R_{avg}(t)$ を基準とした手法の検知性能と閾値の関係

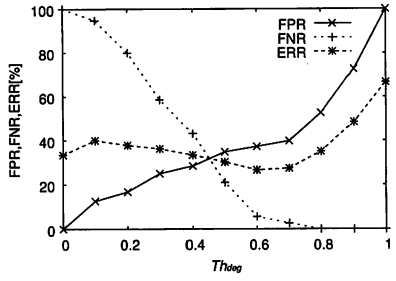

図 8　$R_{var}(t)$ を基準とした検知性能と閾値の関係

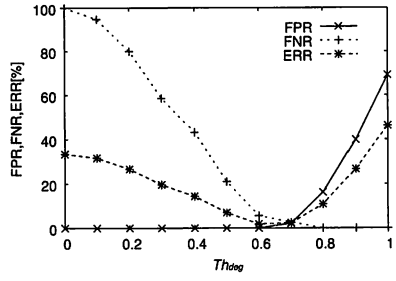

図 9　提案手法の検知性能と Th_{deg} の関係 ($Th_{burst} = 10$)

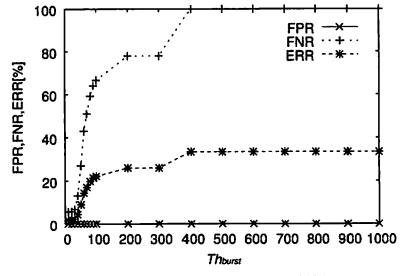

図 10　提案手法の検知性能と Th_{burst} の関係 ($Th_{deg} = 0.6$)

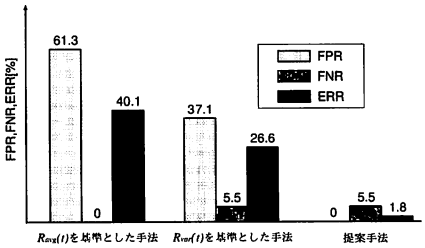

図 11　各手法において ERR が最小となるときの各評価項目の値

帯域利用状態に着目することで輻輳原因がPDoSか否かを識別可能であることを示している．

表5において検知基準が$R_{avg}(t)$の場合と$R_{var}(t)$の場合を比較すると，$R_{avg}(t)$を検知基準としたときには，TCPフローが利用可能な帯域を十分に使い切らない状況を多く誤検知していたが，$R_{var}(t)$を検知基準とすることで誤検知をしていないことがわかる．つまり，集約TCPフローの実帯域利用率の値自体ではなく，前スロットからの相対的な低下度合を評価することで，誤検知を低減できていることがわかる．

さらに，表4において検知基準が$R_{var}(t)$の場合と提案手法の場合を比較すると，$R_{var}(t)$のみを検知基準とした場合には，TCPフローの同時終了が発生した場合を多く誤検知していたが，トラヒックのバースト性を加味することで，誤検知をしないことがわかる．つまり，バーストトラヒックが発生した場合にのみ帯域利用状態の解析を行うことで，誤検知を低減できていることがわかる．

図11からわかるように，提案手法は最もERRが低くなっており，提案手法によりフロー単位での観測なしで誤検知の削減ができ，さらにフロー単位での観測を必要としないため，従来手法と比較して検知に必要な観測コストの低減が可能となったといえる．

しかし，表2から提案手法においても未検知となる場合が存在していることがわかる．これは，PDoSが小規模であるため，TCPフローのスループットの大幅な低下がみられなかったためである．

表2 PDoSのシミュレーションにおけるエラー数

シナリオ	パラメータ設定	検知基準		
		R_{avg}	R_{var}	$Burst+R_{var}$
(a)-1	R=50Mbps L=0.05秒	0	20	20
(a)-2	R=50Mbps L=0.1秒	0	2	2
(a)-3	R=100Mbps L=0.05秒	0	0	0
(a)-4	R=100Mbps L=0.1秒	0	0	0

表3 ストリーミングのシミュレーションにおけるのエラー数

シナリオ	パラメータ設定	検知基準		
		R_{avg}	R_{var}	$Burst+R_{var}$
(b)-1	R=10Mbps	0	0	0
(b)-2	R=30Mbps	0	0	0
(b)-3	R=50Mbps	0	0	0

表4 TCPフローの同時終了のシミュレーションおけるのエラー数

シナリオ	パラメータ設定	検知基準		
		R_{avg}	R_{var}	$Burst+R_{var}$
(c)-1	終了フロー数=8	90	97	0
(c)-2	終了フロー数=9	100	100	0
(c)-3	終了フロー数=10	100	100	0

表5 TCPフローが帯域を使い切らない状況のシミュレーションにおけるエラー数

シナリオ	パラメータ設定	検知基準		
		R_{avg}	R_{var}	$Burst+R_{var}$
(d)-1	最大ウインドウサイズ=10	100	0	0
(d)-2	最大ウインドウサイズ=20	100	0	0

5. まとめ

従来の帯域利用状態に着目した検知手法では，誤検知を回避するために，フロー単位での高コストなトラヒック観測が必要であるという課題があった．そこで，本稿では攻撃時にはバーストトラヒックが発生することを利用し，バーストトラヒックが観測されたときのみ帯域利用状態の解析を行うことで，フロー単位での観測をせずに，問題となる誤検知を削減する手法を提案した．提案手法では，フロー単位での観測を必要としないために，観測コストの低減が可能となり，さらに，集約したTCPフローの実帯域利用率の低下を，前スロットのそれに対する相対的な低下として捉えることにより，大幅に誤検知を削減することが可能となった．また，ns-2を使用したシミュレーションを通して提案手法の性能評価を行い，その有効性を示した．

文献

[1] R. K. C. Chang. Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial. *IEEE Commun. Mag.*, pp. 42–51, October 2002.

[2] A. Kuzmanovic and E. Knightly. Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephant). *Proc. ACM SIGCOMM'03*, pp. 75–86, August 2003.

[3] A. Kuzmanovic and E. Knightly. Low-Rate TCP-Targeted Denial of Service Attacks and Counter Strategies. *IEEE/ACM Transactions on Networking*, pp. 683–696, August 2006.

[4] M. Delio. New breed of attack zombies lurk, May 2001. `http://www.acm.org/technews/articles/2001-3/0514m.html`.

[5] R. Mahajan, S. Floyd, and D. Wetherall. Controlling High-Bandwidth Flows at the Congested Router. *Proc. ICNP*, November 2001.

[6] D. K. Y. Yau, J. C. S. Lui, and F. Liang. Defending Against Distributed Denial-of-Service Attacks With Max-Min Fair Server-Centric Router Throttles. *Proc. IWQoS*, May 2002.

[7] M. Allman, V. Paxson, and W. Stevens. TCP Congestion Control. *RFC2581*, April 1999. `http://www.ietf.org/rfc/rfc2581.txt`.

[8] M. Allman and V. Paxson. On Estimating End-to-End network path properties. *Proc. ACM SIGCOMM 1999*, 1999.

[9] H. Sun, J. C. Lui, and D. K. Y. Yau. Defending Against Low-rate TCP Attacks: Dynamic Detection and Protection. *Proc. ICNP2004*, pp. 196–205, October 2004.

[10] A. Shevtekar, K. Anantharam, and N. Ansari. Low Rate TCP Denial-of-Service Attack Detection at Edge Routers. *IEEE COMMUNICATIONS LETTERS*, pp. 363–365, April 2005.

[11] Y. Chen, Y. Kwon, and K. Hwang. Filtering Shrew DDoS Attacks Using A New Frequency-Domain Approach. *WoNS2005*, pp. 786–793, 2005.

[12] X. Luo and Rocky K. C. Chang. On a New Class of Pulsing Denial-of-Service Attacks and the Defense. *Proc. NDSS'05*, 2005.

[13] 荒井健二郎, 角田裕, 和泉勇治, 根元義章. 帯域利用状態に着目したパルス型DoS攻撃の検知. 信学技報, CS2006-34, Vol. 106, No. 238, pp. 73–78, September 2006.

[14] S. McCanne and S. Floyd. ns Network Simulator. `http://www.isi.edu/nsnam/ns/`.