TCP 再送タイマ管理の変更による低量 DoS 攻撃被害緩和の実験評価

細井 琢朗 †　　松浦 幹太 †

† 東京大学生産技術研究所
153-8505 東京都目黒区駒場 4-6-1
{hosoi, kanta}@iis.u-tokyo.jp

あらまし インターネットの重要な通信輻輳制御の一つである TCP 再送タイムアウト機構を悪用することで、TCP 通信に対して低平均通信量での DoS 攻撃が可能になることが既存研究で指摘されている。我々はこの被害を緩和するような再送タイマの管理方法の変更を以前に提案した。また、簡単な攻撃被害のモデルの下でこの提案方式の被害緩和効果を解析的に評価した。本稿ではこの被害緩和効果を実験的に評価した結果を報告する。

Experimental Evaluation of Low-rate DoS Attack Mitigation by Modified TCP RTO Management

HOSOI Takurou†　　Kanta Matsuura†

†Institute of Industrial Science, The University of Tokyo
4-6-1, Komaba, Meguro-ku, Tokyo 153-8505, Japan
{hosoi, kanta}@iis.u-tokyo.jp

Abstract The mechanism of TCP retransmission timeout is essential to the Internet congestion control. But existing research pointed out that this mechanism allows DoS attack with mean low-rate traffic. We proposed a mitigation measure against this attack by changing TCP retransmission timeout management, and evaluated its mitigation analytically under a simple attack damage model. In this paper, we report experimental evaluation results about effectiveness of above attack mitigation.

1　はじめに

インターネットはその通信規約において，通信量が回線容量を超えた場合（輻輳）にその通信パケットの一部を廃棄してネットワークの安定動作を確保する仕組みを備えている．この通信廃棄が TCP において行われた場合，廃棄に対応した通信データを再送信することが TCP の通信規約で決められている [3]．再送信は通信の輻輳が疑われる状況で行われるため，再送パケットが輻輳を強めることのないように，一定の待ち時間の後に行われる．この輻輳制御には二つの時間尺度がある．まず，正常に送られた通信への応答は RTT（round trip time，～数十ミリ秒）程度で送信側に返ってくる．輻輳などの理由により応答の一部が返ってこない場合，再送タイムアウト（RTO : retransmission timeout，推奨最小値 = 1 sec [2]）だけ待ってからパケットを再送信する．

低量 DoS（Denial-of-service）攻撃 [1] は，RTT の時間尺度の間だけ続くバースト通信を一定周期で繰り返し送信することで，この二つの時間尺度の違いの分だけ低い平均攻撃通信量でサービス妨害が可能になる DoS 攻撃である．この時

間尺度の違いは，輻輳制御に重要な役割を担っているためそのままにしておく必要がある．また RTT はネットワーク環境やネットワークの利用状況で決まるため，送信側で操作することは難しい．この二つの理由から，低量 DoS 攻撃対策は再送タイマへの工夫により実現できることが望ましい．文献 [1] では RTO の最小値（minRTO）を一定の幅の中でランダムに選ぶことで，TCP の各通信が DoS 状態に入り難くする対策を試している．この方法では，対策が無い場合に較べて攻撃が最も強く働くパラメータ設定（バースト通信の周期が RTO の最小値 minRTO と同じ）での平均回線容量は改善する．しかしこの対策では，バースト通信の周期を minRTO からランダム変化の幅の分だけずらしたところで対策前と同程度の攻撃被害が発生するという実験結果になった．そのためこの対策の実行に気付いている攻撃者にとっては最強攻撃パラメータ設定の位置が少しずれるだけとなり，有効な対策とはなっていない．

我々は，TCP 再送タイマの長さ（RTO）が連続するタイムアウト毎に二倍される [4] 点がこの DoS 攻撃の被害を深刻にしていることに着目した．再送タイマの増加が整数倍で行われると，一度低量 DoS 攻撃に捕まった通信はそこから抜け出すことが難しく，平均回線容量が低いままに抑えられてしまう．この点を改良するべく，我々は文献 [5] で再送タイマの長さを連続するタイムアウト毎に $(1+u)$ 倍（$0 < u < 1$）するという TCP 再送タイマの管理方法の変更を提案した．また，文献 [6] でその被害緩和効果を簡単なモデルの下で解析的に評価した．本稿では，シミュレーション実験によりこの方式の被害緩和効果を実験的に評価した結果を報告する。

2 TCP 再送タイムアウトと低量 DoS 攻撃

この節では RFC6298 [4] で規定されている再送タイマの管理方法と，その性質を利用する低量 DoS 攻撃 [1] について簡単に説明する．

2.1 TCP 再送タイムアウト

RTT が計測済みの場合，パケットを $t = 0$ に送信する際，RFC6298 [4] によって RTO の最初の値が次の式で設定される．

$$\begin{aligned}\mathrm{RTO} = \max\{&\mathrm{minRTO},\\ &(\text{smoothed RTT})\\ &+ \max[(\text{clock granularity}),\\ &\quad 4(\text{RTT vairation})]\}\end{aligned} \tag{1}$$

ここで minRTO は RTO の最小値で，RFC6298 [4] が 1 秒にすることを推奨している．多くの場合，最初の最大値比較の中の第二項は第一項に較べて小さい（RTT の時間尺度は RTO の時間尺度よりずっと小さい）．そこでこれ以降は RTO は最初に minRTO に設定されるものとして議論する．

$$\mathrm{RTO}_1 = \mathrm{minRTO} \tag{2}$$

送信されたパケットが無事に宛先に届き，その返信が RTT 程度で送信側に到着した場合は，そのまま通常の通信が続く．しかし輻輳などによりパケットが宛先に届かない，もしくは返信が到着しない場合，送信側は RTO だけ待ってから，送信に失敗したパケットの内の最初の一個を再送信する．その際 RTO の値を次の式で再設定する（exponential backoff phase）．

$$\mathrm{RTO}_i = 2\mathrm{RTO}_{i-1} \tag{3}$$

ここで添字の i は RTO の（再）設定回数を表しており，当該パケットの送信に $i-1$ 回連続して失敗し，i 回目の（再）送信を行っていることを示す．

この新しい RTO の間にパケットが宛先に届き，その返信が送信側に到着した場合は，RTO の値はそのままで，先程送信に失敗したパケットの内の次の二個を再送信する．このパケット送信と返信が無事にできれば，RTO は (1) 式で再計算される（minRTO に初期化される）．一方，再送信した一個のパケットの送信とその返信が (3) 式の RTO の間にできなかった場合，先程と同様，RTO の値を (3) 式の通りに増やし，送信に失敗したパケット一個を再送信する．

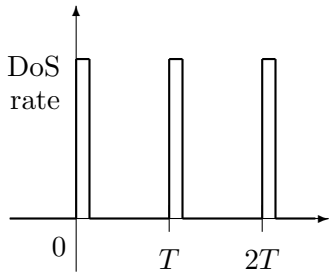

図 1: 矩形波状の DoS 攻撃通信.

以下これを繰り返す．ただし RTO の値には上限値（60 秒以上）が付けられており [4]，それを超える場合はこの上限値が使われる．

2.2 低量 DoS 攻撃

文献 [1] で指摘された，2.1 節の再送タイムアウトの仕組みを利用した低量 DoS 攻撃の概略を説明する．

攻撃通信には図 1 のような，RTT の時間尺度程度続く短時間のバーストとその後の無通信が周期 T で繰り返される矩形波状のものを考える．以下では簡単のため，短時間のバーストは他の通信ができない程に通信帯域を消費する強度と長さを持つ理想的なもののみを考える．

この攻撃通信が始まると，まず最初のバースト通信により,（ほとんど）全ての TCP 通信が失敗し，再送タイムアウトを待つ．2.1 節で解説した通り，この際の RTO は全ての通信で一律に minRTO に設定される．そのため（ほとんど）全ての通信が同期して再送タイムアウトを待つことになる．

再送タイムアウトが DoS 攻撃のバースト通信に重ならなければ，パケットの再送信は成功することが期待される．そしてそれ以降はほぼ通常の通信が行われた後，次のバースト通信により再度（ほとんど）全ての TCP 通信が失敗し，再送タイムアウトを待つ．これを攻撃が止むまで繰り返すことになる．

再送タイムアウトが DoS 攻撃の次のバースト通信に重なる

$$\mathrm{minRTO} \simeq T \tag{4}$$

と，再送信も失敗し，(3) 式により 2 倍に増やされた RTO だけ待ってから再度再送信を行うことになる．しかしこの再度の再送タイムアウトも (4) 式の条件からバースト通信に重なる．以降，RTO は minRTO の整数倍の値を取り続けるため，再送タイムアウトは全てバースト通信に重なり，攻撃の間は通信が（ほとんど）できない．

バーストにより全ての TCP 通信が送信失敗になる場合の正規化平均回線容量は，文献 [1] により次の式で表せる．

$$\rho = \frac{T - \mathrm{minRTO}}{T} \quad (\text{for } T \geq \mathrm{minRTO}) \tag{5}$$

上式は常に 1 より小さく，その 1 との差（通信回線容量の減少）がサービス妨害の被害に当たる．攻撃のバースト通信の周期 T と再送タイマの最小値 minRTO が等しい（(4) 式）と，回線容量は 0 になり，攻撃の被害が最も大きい．

攻撃からある割合 r で逃れる通信がある場合の正規化平均回線容量は，簡単な考察から

$$\rho' = \frac{T - (1-r)\mathrm{minRTO}}{T} \quad (\text{for } T > \mathrm{minRTO}) \tag{6}$$

と表せる．ただし，DoS 攻撃のバースト通信の周期が再送タイムアウトに同期している場合（$T \simeq \mathrm{minRTO}$: (4) 式）は，再送タイマ別にきちんと取り扱う必要がある．文献 [5] にあるように，

- $t = 0$ から次のバースト通信まで（$t = T$）の間，攻撃を避けた通信の割合 :
  $$r$$
- $t = T$ から次のバースト通信まで（$t = 2T$）の間，攻撃を避けた通信の割合 :
  $$r^2 + (1-r)r = r$$
- $t = 2T$ から次のバースト通信まで（$t = 3T$）の間，攻撃を避けた通信の割合 :
  $$r^2 + (1-r)r^2 = (2-r)r^2$$
- $t = 3T$ から次のバースト通信まで（$t = 4T$）の間，攻撃を避けた通信の割合 :
  $$(2-r)r^3 + (1-r)r^2 + (1-r^2)r$$

のように順次計算できる．この攻撃を避けた通信の割合を平均したものが正規化平均回線容量になる．

3　提案方式の再送タイマ管理

低量 DoS 攻撃が行われると，2.2 節で解説した通り，特に DoS 攻撃のバースト通信の周期が再送タイムアウトに同期している場合（$T \simeq \mathrm{minRTO}$: (4) 式）に大きなサービス妨害が発生する．これは連続して再送信を続ける場合，(1) 式と (3) 式により RTO が minRTO の整数倍に増やされるため，毎タイムアウトが必ず DoS 攻撃のバースト通信と重なることが原因である．文献 [1] では minRTO を一定の幅の範囲でランダムに選ぶことでこの DoS 攻撃への対策を試みたが，TCP 通信の輻輳制御を働かせるためにはこの幅を大きく取れず，大きな被害低減効果は得られなかった．

そこで我々は，(3) 式による RTO の増加方法を以下のように変更することを文献 [5] で提案した．

$$\mathrm{RTO}_i = (1+u)\mathrm{RTO}_{i-1} \quad (0 < u < 1) \tag{7}$$

すると連続した再送信での RTO は

$$\mathrm{RTO}_i = (1+u)^{(i-1)}\mathrm{minRTO} \tag{8}$$

となり，u に有理数を選ぶことで minRTO の整数倍にはならない系列が得られる．この系列を使って RTO を増やせば，低量 DoS 攻撃の一周期内のバーストの回数を増やし続けない限り，再送タイムアウトがバーストと重ならない機会が生まれ，サービス妨害の被害の低減が期待できる．

2.2 節の低量 DoS 攻撃と同じ攻撃を考える．再送タイムアウトが攻撃のバースト通信と重ならない場合は，各通信は一回目のタイムアウトの後に通常の通信に戻り，連続してタイムアウト待ちになることはない．RTO の最初の値の設定方法は提案方式と元の再送タイマ管理方法では同じなため，この場合の正規化平均回線容量は提案方式も元の再送タイマ管理方法と同じ (5) 式で表せる．

$$\rho' = \frac{T - \mathrm{minRTO}}{T} \quad (\text{for } T > \mathrm{minRTO}) \tag{9}$$

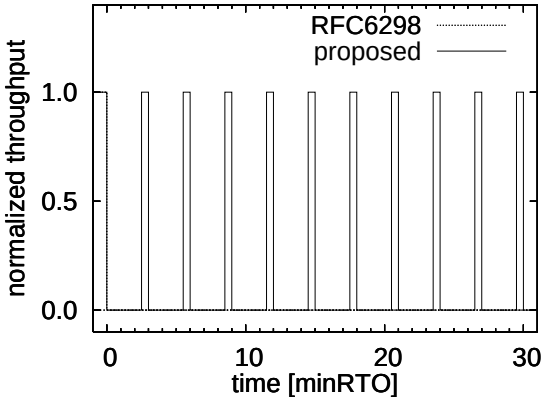

図 2: バーストにより全ての通信が送信失敗になる場合の正規化回線容量の推移．

攻撃のバースト通信の周期が再送タイマの最小値に一致している場合，提案方式では以下のような遷移をする．

- $(t = 0)$
  バーストによりパケットの送信に失敗する．
  （再送タイマ $\mathrm{RTO}_1 = \mathrm{minRTO}$）
- $(t = \mathrm{minRTO})$
  再送タイムアウト．バーストによりパケットの再送信に失敗する．
  （再送タイマ $\mathrm{RTO}_2 = (1+u)\mathrm{minRTO}$）
- $(t = 2\mathrm{minRTO})$
  再送タイムアウトを待つ．
- $(t = (2+u)\mathrm{minRTO})$
  再送タイムアウト．バーストが重ならないため，パケットの再送信に成功する．
- （以下繰り返し.）

この遷移による回線容量の推移をグラフにすると図 2 の実線のようになる．この図からわかる通り，元の再送タイマ管理方法（図中の RFC6298 の破線）では回線容量は 0 のままであるが，提案方式では期間 3minRTO 毎に一回，通常通信に戻る期間ができる．この正規化平均回線容量は簡単に計算でき，以下のようになる．

$$\rho' = \frac{1-u}{3} \quad (\text{for } T = \mathrm{minRTO}) \tag{10}$$

この分だけ，提案方式は元の方式に較べて低量 DoS 攻撃の被害緩和効果がある．

文献 [6] での解析的評価から，攻撃前に正常に通信できていた TCP 通信の正規化平均回線

容量は，(10) 式よりも大きくなることが分かっている．この性質は攻撃回避率 r に依らない．また，この正規化平均回線容量を通常の再送タイマ管理の場合のものと比べると，回避率 r が 0.4 になるあたりで，提案方式の再送タイマ管理の被害緩和効果が高くなることが示された．

4 評価実験方法

評価実験の方法を説明する．

被害緩和効果を評価するためには，実験ネットワーク環境の自由に，大きく変えられることが望ましい．また，提案方式の実験には TCP 再送タイマの管理方式の変更が必要である．これらの要件を実機で達成するのは非常に手間が掛かる．そこで今回の評価実験には，ネットワークシミュレータ ns-3 [7] を用いることにした．

ネットワーク構造は，一対のルータがボトルネックの回線一本で結ばれているものを元に，一方のルータへ送信側のノードを回線で接続し，もう一方のルータから受信側のノードへ回線を接続した構造とした．この送信側ノードから受信側ノードへ TCP 通信を続けている際に，ルータ間のボトルネック回線へ DoS 攻撃を行う．この攻撃による通信量の減少を観測し，攻撃前の通信速度に対する攻撃後の通信速度を攻撃被害耐性（攻撃後の正規化平均回線容量）の指標とする．通常の再送タイマ管理の場合と提案方式の下での正規化平均回線容量を比べることで，提案方式の攻撃緩和効果を評価する．

DoS 攻撃には，本来であれば文献 [1] で指摘された低量 DoS 攻撃を採用することが最善である．しかし ns-3 を使った予備実験では，2.2 節の低量 DoS 攻撃を安定して発生させることができなかった．そのため今回の実験では，攻撃通信をボトルネック回線に加えるのではなく，DoS の間だけルータがパケットの転送を受け付けないように設定することで低量 DoS 攻撃を模擬することにした．転送の拒否は受信側への TCP 通信ではなく，文献 [1] に倣って，受信側から送信側への返信 ACK パケットの向きに対して作用させる．この手法で，図 3 のように攻撃の無い状態（< 1 sec）に比べて通信は大きく

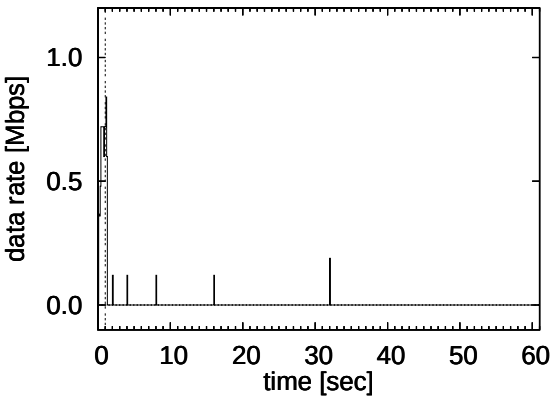

図 3: 攻撃を受けている回線を通過する通信の例．

妨げられる．

ネットワークの各回線は，攻撃箇所をボトルネックとするために，二つのルータ間と受信側は低容量（1.5 Mbps）にし，それに対して送信側を高容量に設定した（1.5，3.0，6.0，12.0 Mbps）．また，RTT が大きくなると実験に支障がでることが予想されるため，回線の遅延は全ての回線で小さい値（6 msec）を設定した．

DoS 攻撃は，通常の TCP 通信を安定させてから加えた（通常通信の開始から 1 sec 後に最初の攻撃）．また，提案方式は DoS 攻撃のバーストの周期が minRTO の場合に被害緩和の効果を発揮することが文献 [6] で示されていることから，バースト通信（パケット転送拒否）の周期は一律に 1 sec とした．バースト通信（パケット転送拒否）の長さは，DoS 攻撃による被害が確実に出るように，長めの値（0.5 sec）を採用した．再送タイマ RTO の上限の最小値は 60 sec であることから [4]，各実験は攻撃を 60 sec 続けた時点で終了させた．

予備実験により，このシミュレーション実験の結果得られる正規化平均回線容量の値は，パケット送信タイミングの僅かの差でかなり変わることが分かった．そこで今回の評価では DoS 攻撃開始時刻を 0.1 sec 刻みに増やした場合のシミュレーションを 10 例試行し，その平均値を使った．

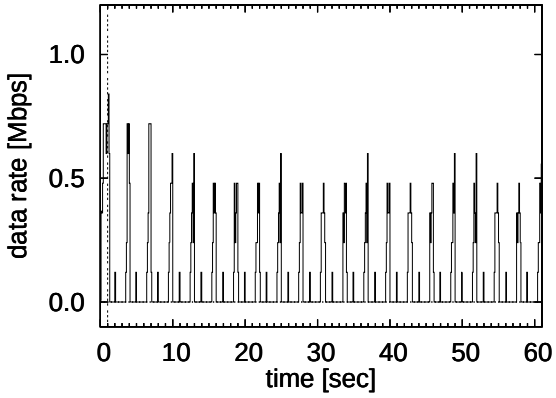

図 4: 攻撃を受けている回線を通過する通信の例（提案方式の RTO 管理の場合）.

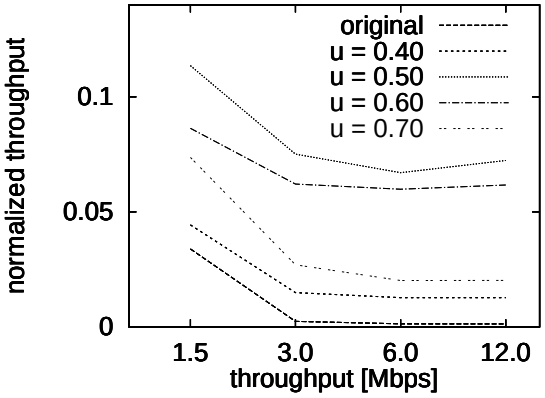

図 5: 攻撃後正規化平均回線容量の測定結果.

5 実験結果

低量 DoS 攻撃の模擬（周期的パケット転送拒否）により，TCP 通信は図 3 のように大きく妨げられる．この図では，時刻 0 sec から 1 sec までは攻撃は行われておらず，通常の TCP 通信が続いている．時刻 1 sec を過ぎると基本的に通信速度は 0 になり，時折少量の通信が行われる状態になる．この少量の通信の中には再送パケットも含まれている．この図の例の場合に攻撃が始まってもすぐには通信が止まらないのは，TCP のウィンドウサイズの分のパケットが遅れて送信されているものや，たまたま最初の DoS を避けた分などが含まれているためである．

提案方式の TCP 再送タイマ管理の下では，図 4 のように，TCP 通信の妨げ（攻撃被害）は元の再送タイマ管理の場合に比べて弱まる傾向にある．攻撃が行われていない間（時刻 0 sec から 1 sec まで）の通信は，提案方式でも元の TCP 再送タイマ管理方式でも変わらない．そこで，攻撃が無い間の通信速度と攻撃後の通信速度を比べることで，攻撃の被害の程度を評価できる．今回の評価実験では，攻撃前の平均通信速度に対する攻撃後の平均通信速度の比を攻撃後の正規化平均回線容量と見做し，攻撃被害耐性の指標とする．また，元の TCP 再送タイマ管理方式の下での正規化平均回線容量に対する提案方式での正規化平均回線容量の差を，攻撃被害の緩和効果の指標として使う．

図 5 は，送信側回線容量設定を変えた場合の，攻撃後正規化平均回線容量の測定結果である．長い破線（”original”）が元の TCP 再送タイマ管理方式での攻撃被害耐性を表す．ボトルネック回線は 1.5 Mbps に容量を設定している．つまりボトルネック回線が実際にボトルネックとして働いている場合には，攻撃の被害が大きい（耐性が小さい）結果になっている．

その他の線（”$u = 0.40$”，”$u = 0.50$”，”$u = 0.60$”，”$u = 0.70$”）は提案方式の TCP 再送タイマ管理の場合（u は (7) 式のもの ; RTO の増分を示すパラメータ）の攻撃被害耐性を表す．これらは全ての場合において元の TCP 再送タイマ管理方式での攻撃被害耐性（”original”）に勝る．即ち，提案した TCP 再送タイマ管理方式には TCP 通信を標的とした低量 DoS 攻撃の被害を緩和する効果があることが判る．また，ボトルネック回線の容量設定が送信側回線容量設定に比べて小さくない場合，攻撃被害が小さい（耐性が大きい）結果になっている点は，元の TCP 再送タイマ管理方式の測定結果と同じである．

文献 [6] での解析的評価によると，正常に通信できていた TCP 通信がこの DoS 攻撃を受けた場合，その正規化平均回線容量は (10) 式よりも大きくなるはずである．各 u の値（$u = 0.4, 0.5, 0.6, 0.7$）を入れると，(10) 式の値はそれぞれ 0.2, 0.167, 0.133, 0.1 と u に対して単調減少する．しかし図 5 はそれとは異なり $u = 0.5$

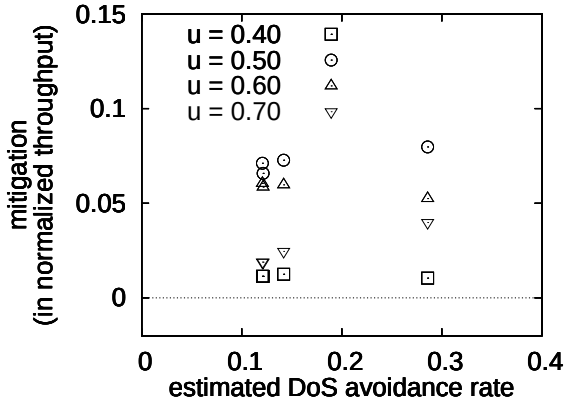

図 6: 攻撃後正規化平均回線容量の差と攻撃回避率の推定値の測定結果.

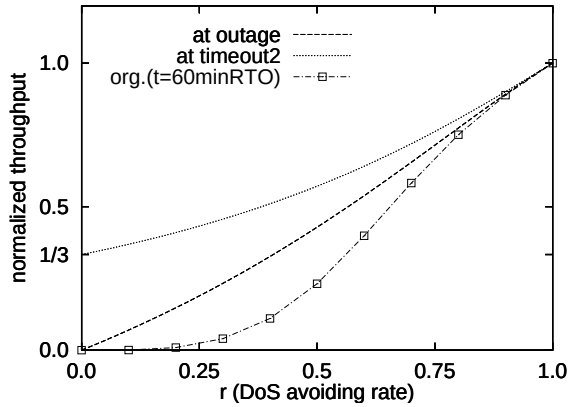

図 7: 提案方式での正規化平均回線容量の収束値（文献 [6]）.

の場合に最大の正規化平均回線容量を示し，それより u が大きくなっても小さくなっても正規化平均回線容量が減る結果となった．またその値は全ての場合で (10) 式を下回っている．この食い違いの理由は不明である.

図 6 は，攻撃被害の緩和効果の指標として，縦軸に攻撃後正規化平均回線容量の TCP 再送タイマ管理方式間の差を取り，横軸には元の TCP 再送タイマ管理方式での攻撃後正規化平均回線容量から推定した攻撃回避率 r の値を当てたグラフである．文献 [6] での解析的評価では，回避率 r が 0.3 になるあたりで，提案方式の再送タイマ管理の被害緩和効果が高く（正規化平均回線容量の差が大きく）なっている（図 7）. しかし図 6 では被害緩和効果の値（縦軸）に一定の傾向は見えず，この性質は確認できなかった．これは今回のシミュレーション実験の設定で攻撃回避率 r の推定値が 0.3 を超える実験例が得られなかったことが原因である可能性がある．この点は今後の実験で確認する必要がある.

6 まとめ

本稿では，文献 [1] で提案された低量 DoS 攻撃の被害を緩和するような再送タイマの管理方法の変更 [5] について，その被害緩和効果を実験的に評価した．実験はネットワークシミュレータ ns-3 [7] を用いて行い，元の TCP 再送タイマ管理方式と提案方式の場合の攻撃後正規化平均回線容量を測定した．この測定結果を指標として攻撃緩和効果を評価すると，提案方式には明瞭な攻撃被害緩和効果が認められた．ただし，解析的評価が示していた，攻撃回避率との相関は確認できなかった.

残念ながら，今回の実験評価は各種のパラメータについて徹底的に調べてはいない，また低量 DoS 攻撃も攻撃通信を加えるのではなく，模擬的に実装したものになっている．今後はこれらの不足点を補うことと，提案方式が他のネットワーク機構に与える影響（副作用）について調査する予定である.

参考文献

[1] A. Kuzmanovic and E.W. Knightly, “Low-rate TCP-targeted Denial of Service Attacks: the Shrew versus the Mice and Elephants”, In Proceedings of ACM SIGCOMM’03, pp.75-86 (August 2003)

[2] M. Allman and V. Paxson, “On Estimating End-to-end Network Path Properties”, In Proceedings of ACM SIGCOMM’99, pp.263-274 (September 1999).

[3] J. Postel (Ed.), “Transmission Control Protocol”, Internet RFC 793, IETF (September 1981).

[4] V. Paxson, M. Allman, J. Chu, M. Sargent, “Computing TCP’s Retransmission Timer”, Internet RFC 6298, IETF (June 2011).

[5] 細井 琢朗, 松浦 幹太, “低量 DoS 攻撃を緩和する TCP 再送信タイマ管理の一検討”, 情報処理学会コンピュータセキュリティ研究会（研究報告コンピュータセキュリティ（CSEC））, vol.62, no.51, pp.1–5 (July 2013)

[6] 細井 琢朗, 松浦 幹太, “TCP 再送信タイマ管理の変更による低量 DoS 攻撃被害の緩和効果”, コンピュータセキュリティシンポジウム 2013（CSS2013）論文集,（CD-ROM）（2013 年 10 月）

[7] ns-3, http://www.nsnam.org/