1Y-03

Low-rate DoS攻撃の緩和のための代理再送機構の実現性の検討

児玉拓海† 久末瑠紅† 稲村浩† 石田繁巳†
†公立はこだて未来大学

1 はじめに

2003年からネットワークの脆弱性を悪用し，通信の品質を低下させるLow-rate DoS（LDoS）攻撃が議論されている．LDoS攻撃では，大量トラフィックを用いる従来のDistributed DoS（DDoS）攻撃とは異なりパルス形状の攻撃トラフィックを用いるため，平均通信量が低く，既存のDDoS攻撃に対する検知機構を回避するステルス性を持つ．

LDoS攻撃の1つにTCPの再送制御を悪用するShrew手法がある [1]．Shrew手法では，再送制御で用いられるRetransmission Time Out（RTO）の周期と攻撃タイミングを同期させ，攻撃を成立させている．この特性に着目し，LDoS攻撃のShrew手法を緩和する手法として，RTO周期と攻撃タイミングの同期を外すことが考えられる．

本稿では，RTO周期と攻撃タイミングの同期を外す手法として，Performance Enhancement Proxy（PEP）による代理再送を検討する．PEPは，通信プロトコルの通信性能を向上させるために設計されたプロキシである．PEPの1つにSnoopがある．Snoopは，TCP通信において送信者と受信者間の通信を監視して通信パケットをキャッシュし，パケットの送信に失敗した場合にキャッシュしたパケットをもとに送信者の代理で再送を行う [2]．本稿では，この代理再送機構を参考にしたLDoS攻撃を緩和する新たなPEPを検討する．

2 関連研究

細井らはLDoS攻撃に対して攻撃緩和効果のあるRTO計算アルゴリズムを提案した [3]．提案アルゴリズムでは，2回目以降のRTOの値を計算するアルゴリズムの係数をランダマイズすることで再送と攻撃タイミングの同期を外し，LDoS攻撃の緩和効果を示している．しかしながら，RTOの値をランダマイズする手法ではTCPの通信性能を考慮すると，ランダマイズの幅を大きく取れないため，緩和効果はわずかであることが報告されている [1]．

A Feasibility Study on LDoS Attacks Mitigation with Proxy's Retransmission
Takumi Kodama†, Ryuku Hisasue, Hiroshi Inamura†, Shigemi Ishida†
†Future University Hakodate, Japan
†{b1020239, g2122054, inamura, ish}@fun.ac.jp

3 提案手法

通信ノード間に配置するLDoS攻撃緩和プロキシが送信者の代理で再送を行うことで，再送タイミングを制御する．これによりShrew手法で成立していたTCPの周期的なRTO再送と攻撃タイミングの同期を外し，攻撃を緩和する．提案手法では，送信者と受信者間の通信を監視して通信パケットをキャッシュし，通信に失敗した場合にキャッシュしたパケットを基に送信者の代わりに再送するSnoop [2] の機構を参考に代理再送を行う．代理再送機構の導入によって，図1で示すような攻撃トラフィックの送信タイミングとは異なるタイミングであり，かつ送信者のRTO処理よりも早いタイミングで正常パケットの代理再送を行う．代理再送機構は，攻撃によって正常に通信できなかったパケットの代理再送を行う．代理再送を成功させることにより，送信者にACKが返送され，送信者による正常パケットの送信が再開されると予想される．次節では代理再送機構について詳述する，

3.1 実装

LDoS攻撃で用いられる攻撃トラフィックの多くはUDPパケットである [4] ことから，LDoS攻撃緩和プロキシは，UDPパケットの受信により攻撃パルスの開始を検知してからλ秒間に送信されるTCPパケットを全てキャッシュする．ここで，λはLDoS攻撃緩和プロキシが攻撃パルスの開始を検知後，代理再送を行うまでの待機時間とする．キャッシュされるTCPパケットは，攻撃トラフィックがルータのバッファを埋めるまでに送信中のパケットである．

λ秒後，LDoS攻撃緩和プロキシは，キャッシュした全てのTCPパケットの代理再送を行う．今回の実装では，ACKの返送の有無に関わらず，キャッシュした全てのTCPパケットを代理再送している．

本稿では，RTO再送タイマの初期値$minRTO$の推奨値が1.0秒であること [5]，LDoS攻撃で用いられるパルス幅が0.1–0.3秒であること [4] から，代理再送を行うまでの待機時間λは

$$\lambda = \frac{1}{3} minRTO \tag{1}$$

とする．

4 実験と評価

提案手法の代理再送機構によるLDoS攻撃緩和の初期的評価として実験を行う．

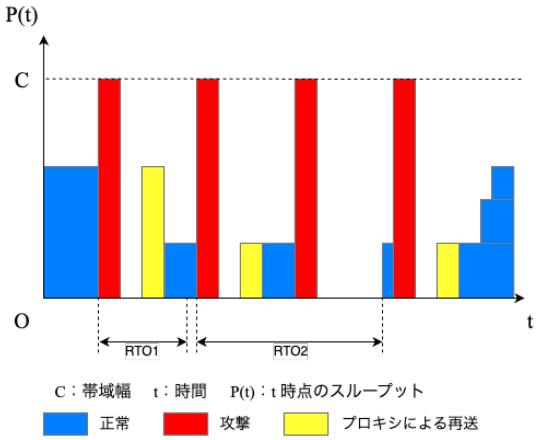

図 1: LDoS 攻撃緩和プロキシによる代理再送

4.1 実験環境

実験は図 2 に示すトポロジで行った．Sender と 3 台の Attacker を Router に接続し，Router からボトルネックリンクで Receiver に接続している．Router は，Sender のデータを Receiver に向けて転送する．Attacker は Router に対して，パルス形状になるよう攻撃トラフィックを送信する．今回の実験では，Sender の送信データサイズを 30MB に設定して行った．Attacker の攻撃パルス幅は 0.3 秒とし，攻撃は Sender の送信が終わるまで続ける．攻撃パルスの周期は，RFC6298 [5] で *minRTO* の推奨値が 1 秒であると定義されているため，1.0 秒に設定した．

Sender の送信開始から送信終了を 1 試行とし，PEP を導入するときとしないときのそれぞれで 100 試行の実験を行い，Observer で実験の pcap データを取得する．

4.2 評価方法

実験で得た pcap データからスループットを算出し，攻撃効果を求めた．攻撃なしの正常トラフィックのスループットを T_N，攻撃時 PEP なしの正常トラフィックのスループットを T_A，攻撃時 PEP ありの正常トラフィックのスループットを T_P とし，攻撃効果 E_A，E_P を式 (2)，攻撃の緩和率 R を式 (3) で計算した．

$$E_A = 1 - \frac{T_N}{T_A}, \quad E_P = 1 - \frac{T_N}{T_P} \tag{2}$$

$$R = \frac{E_A - E_P}{E_A} \tag{3}$$

4.3 評価結果

表 1 に，スループット，攻撃効果，改善率を示す．PEP を導入したときの式 (3) で計算した攻撃の緩和率は，約 23.1%となり，PEP の導入によって攻撃の緩和が確認できた．しかし，代理再送したパケットに対して Receiver から Dup ACK の返送が多く見られた．LDoS 攻撃緩和プロキシがキャッシュして代理再送を行った TCP パケットの中に Sender が次に送信すべきパケットが含まれていない場合があることと，代理再送機構の実装上，

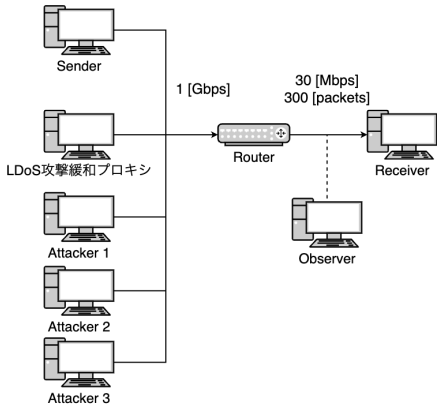

図 2: 実験環境

表 1: 平均スループットと攻撃効果

攻撃	PEP	スループット (Mbps)	E(%)	R(%)
なし	なし	9.56	0.0	0.0
あり	なし	1.36	85.8	0.0
あり	あり	3.25	66.0	23.1

キャッシュした全ての TCP パケットを代理再送していることが原因だと考えられる．

5 おわりに

本稿では，TCP 自体に変更を加えず，代理再送機構を導入することで，LDoS 攻撃によるスループットの低下を抑え，攻撃を緩和であることを明らかにした．しかし，TCP の周期的な再送と攻撃タイミングの同期を外し，攻撃を緩和するためには，実装に改善が必要であると考えられる．具体的な改善点として，キャッシュした TCP パケットの中から ACK が未返送のパケットのみを代理再送することを挙げる．今後は，攻撃の緩和効果を向上させるために，代理再送する最適な TCP パケットについて調査し，代理再送機構の実装を見直していく．

参考文献

[1] A. Kuzmanovic and E. W. Knightly. Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants. *ACM SIGCOMM*, pp. 75–86, 2003.
[2] M. García et al. An experimental study of Snoop TCP performance over the IEEE 802.11b WLAN. *IEEE WPMC*, Vol. 3, pp. 1068–1072, 2002.
[3] 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論文集, Vol. 2013, No. 4, pp. 957–964, 2013.
[4] W. Zhijun et al. Low-rate DoS attacks, detection, defense, and challenges: A survey. *IEEE Access*, Vol. 8, pp. 43920–43943, 2020.
[5] V. Paxson et al. RFC 6298: Computing TCP's retransmission timer, 2011.