Optimistic ACKing を利用した LDoS 攻撃効果の検証

Evaluation of the Effects of LDoS Attacks Using Optimistic ACKing

萩原 啓道 Hiromichi Hagiwara
久末 瑠紅 Ryuku Hisasue
稲村 浩 Hiroshi Inamura
石田 繁巳 Shigemi Ishida

公立はこだて未来大学/ Future University Hakodate

1 はじめに

間欠的なバーストトラフィックを利用して通信の QoS (Quality of Service) を低下させる LDoS 攻撃 (Low-rate Denial of Service) がインターネット上の脅威として議論されている．この攻撃は，少ない攻撃通信量で攻撃を実現できることから，ステルス性が高く未知の要素が多い [1]．

LDoS 攻撃は一般に攻撃トラフィックに UDP を用いる [1]．しかしながら，TCP による LDoS 攻撃はあまり議論されていない．本稿では，TCP を用いた LDoS 攻撃の脅威を示し，攻撃に対する対策の必要性を示す．

2 関連研究

LDoS 攻撃は，TCP が有する再送制御タイマ RTO (Retransmission timeout) の間隔に合わせてバーストトラフィックを引き起こすことで，再送のタイミングに輻輳を発生させて通信を妨害する．ボトルネックリンク帯域幅の 10–20%程度の平均通信量で攻撃を実現することからステルス性が高い [1]．

LDoS 攻撃は，RTO が容易に推測可能な点を利用し攻撃する．RTO の初期値 $minRTO$ は 1 秒を推奨値としており，連続して再送が確認されない場合の RTO は，$RTO = RTO \times 2$ で再設定される．すなわち，$minRTO$ 周期で再送トラフィックが発生するため，LDoS 攻撃はこの再送に合わせて攻撃パルスを送信する．

LDoS 攻撃は多くの場合 UDP で構成されているが, TCP の Optimistic ACKing を利用する攻撃の実現可能性も確認されている [2]．Optimistic ACKing は，受信者が未着のセグメントに対して ACK を偽装して返すことで，輻輳制御をバイパスし，高速転送を実現する技術である [2]．

しかし，転送レートの増幅率を考慮せずに利用することで輻輳を招き，輻輳状態を判断できない．これを悪用することで，ACK ストリームを操作することでバーストトラフィックを形成できることが明らかになっているが，標的トラフィックに対する攻撃トラフィックの影響についてはまだ未知である．

そこで，Optimistic ACKing の LDoS 攻撃が標的トラフィックに与える影響の評価を行った．結果, 攻撃トラフィックによって，標的トラフィックに RTO を発生させ，完全に抑止できることを確認した．しかし，帯域幅を満たす攻撃トラフィック構成までに時間を要することが明らかとなり，攻撃効果の低下が明らかとなった．

TCP は徐々に通信量を増加させるスロースタートを採用しているため，Optimistic ACKing での LDoS 攻撃時においても，帯域幅を埋める攻撃トラフィックを構成するまでに時間がかかり攻撃効果が低下したと考えられる．しかし，ACK の送出量を調整することで，攻撃トラフィックの構成を高速化できる可能性がある．

さらに，TCP を拡張して複数経路通信を可能にする MPTCP (Multipath TCP) プロトコルでは，従来型 DoS 攻撃を単一ノードから複数リンクに分散させて実現できることが明らかになっている [3]．しかし，TCP において複数リンクに分散させた LDoS 攻撃の実現可能性については明らかになっていない．

本稿では，Optimistic ACKing の LDoS 攻撃時の ACK 送出量の調整，複数リンクを用いた攻撃に着目した，攻撃効果を向上させる手法の提案と評価を行い，その脅威を示す．

3 評価環境

ネットワークシミュレータ ns-3 を用いた仮想環境上にて，図 1 のトポロジで実験を行った．クライアント側である攻撃者（Host）が，悪意のないサーバ（Worker）から攻撃トラフィックを引き出し，標的トラフィックに対する攻撃を実施した．

Router 間のボトルネックリンクは帯域幅 10Mbps，遅延 10ms，各ノードと Router 間のリンクは帯域幅 100Mbps，遅延 10ms に設定した．シミュレーションによって得られたデータは，パケットモニタリングツール Wireshark を用いて分析・評価した．

4 Optimistic ACKing の ACK 送出量の最適化

Optimistic ACKing での LDoS 攻撃は, 帯域幅を満たす攻撃トラフィック構成に時間を要することを確認した．これは，TCP のスロースタートに起因して攻撃効果が低下したことが考えられる．

従来の ACK 送出量では，初期バーストトラフィック構成時の ACK 送出量をスロースタートに基づいて設定されていたが，帯域幅の大きさとパケットサイズに基づいて，帯域幅を埋めるために必要な ACK 送出量を算出し，初期バーストトラフィック構成時に送出することで帯域幅を迅速に満たす手法を提案する．これにより，帯域幅を満たすまでの時間を短縮し，攻撃効果を低下することなく，攻撃を実現できる可能性が考えられる．

評価結果

実験結果を図 2 に示す．上図が従来の ACK 送出量の実験結果となっており，帯域幅を満たす攻撃トラフィックを構成するまでに時間を要していたが，下図の提案手法では，スロースタートの影響を受けず，初期バーストトラフィック時から帯域幅を満たすことができた．すなわち，従来の ACK 送出量と比較して，効率的に攻撃を行えることが示唆された．

5 複数ネットワークインタフェースを用いた LDoS 攻撃

複数リンクを用いて攻撃を行うことで，利用可能な帯域幅が増加し，攻撃レートの向上が期待される．従来，複数リンクからの攻撃は，複数ノードから構成することが考えられている．そこで，単一ノードから複数ネットワークインタフェースを用いる LDoS 攻撃を提案する．この提案手法では，単一ノードから複数のネットワークインタフェースを使用して，複数の TCP コネクションを受け付けるサーバに対して複数コネクションを張ることで LDoS 攻撃を行う．各インタフェースから，別々の TCP コネクションを確立し，それぞれのリンクから LDoS 攻撃トラフィックを送信する．これにより，異なる IP アドレスから攻撃トラフィックが送出されるため，複数ノードから攻撃しているかのような状況を作り出す．複数ネットワークインタフェースを用いて攻撃に使用するリンクに分散させ攻撃を行うことにより，使用できる帯域幅を増加させ，より高い攻撃レートで攻撃の実現を目指す．

評価結果

実験結果を図 3 に示す．青色の標的トラフィックが流れるボトルネックリンクに，単一ノードから，それぞれデータレートが異なる，赤，橙黄色の 2 つの攻撃トラフィックが流入し始めるシナリオで行った．5 秒から帯域に流入し始めた，攻撃トラフィックによって，8 秒時点で，標的トラフィックを完全に抑止された．従って，単一ノードから複数リンクを用いてバーストトラフィックを送出して標的トラフィックを効果的に抑止できることが確認された．

6 おわりに

本稿では，TCP による LDoS 攻撃の効果を確認し，その効果を向上させる LDoS 攻撃手法の提案と評価を行った．これらの結果は，TCP での LDoS 攻撃の脅威を再認識させるものであり，検知と防御に向けた研究と実装の必要性を示すものであった．今後，実環境での評価を進め，TCP での LDoS 攻撃に対する脅威をより明確にしていく．

参考文献

[1] W. Zhijun, et al., “Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey,” IEEE Access, vol.8, pp.43920–43943, 2020.

[2] V.A. Kumar, et al., “On remote exploitation of TCP sender for low-rate flooding denial-of-service attack,” IEEE Communications Letters, vol.13, no.1, pp.46–48, 2009.

[3] V.A. Kumar, et al., “Data sequence signal manipulation in multipath TCP (MPTCP): The vulnerability, attack and its detection,” Computers & Security, vol.103, p.102180, 2021.

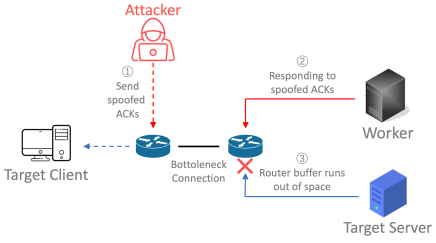

図 1 TCP での LDoS 攻撃図

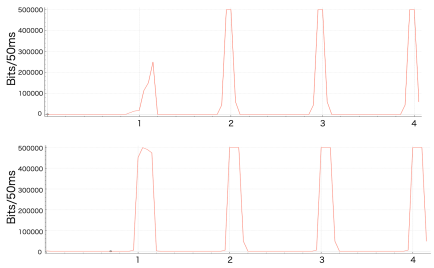

図 2 ACK 送出量の最適化
上図：従来の送出量 下図：ACK 送出量の最適化

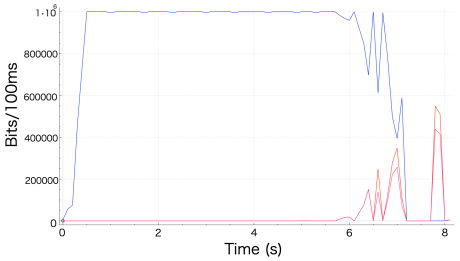

図 3 複数ネットワークインタフェースを用いた LDoS 攻撃