

OpenFlow1.5 による DDoS 緩和システムの設計と実装

栗原 航† 廣津 登志夫†
法政大学情報科学部コンピュータ科学科

1. まえがき

DDoS 攻撃は主要なサイバー攻撃のひとつである。代表的攻撃手法に TCP プロトコルの 3 ウェイハンドシェイクを狙った TCP SYN Flood 攻撃がある。従来は、このようなサイバー攻撃に対してファイアウォールや IDS のような専用のセキュリティ機器をネットワークの入口に配することで対処していた。しかし、専用機器は攻撃変化に対する柔軟性の観点で懸念があり、いつ発生するかわからない攻撃に対し導入コストも高いという問題もある。

そこで、OpenFlow[1]を用いて、通信を中継するネットワークの任意の場所で自在に攻撃を防御する手法が考えられる。OpenFlow はネットワーク全体をソフトウェアで管理することで柔軟な経路制御とネットワーク構成を実現する。これまでに、DDoS 攻撃の緩和手法である TCP SYN Authentication[2]が OpenFlow1.3 を用いて実現されている[3]。しかしこのシステムでは SYN パケットのホストへのスルーputが低いことが課題となっており、その原因は OpenFlow メッセージのひとつである Packet-In メッセージ処理のオーバーヘッドにあると考えられる。本研究では OpenFlow の機能拡張が行われたバージョン 1.5 と Nicira 拡張機能を用いて実現することで、従来システムよりも性能の向上を目指す。

2. TCP SYN Authentication

TCP SYN Authentication は「ボットは SYN パケットのみ送信する」という特徴を利用したクライアント認証である。手順を図 1 に示す。SYN パケットが送られてくると経路上でシステムが受信し、サーバに転送することなく、確認応答番号に不正な値を設定した不正 SYN/ACK パケットを返送する。TCP プロトコルでは SYN パケット内のシーケンス番号に 1 を加えた値が SYN/ACK パケットの確認応答番号にセットされていることが期待されるが、もしこれをその他の値にした場合、SYN パケットを送出したクライアントは RST パケットを送信し強制的に接続中断を行った後、SYN パケットを再送しなければならない。一方、DDoS の攻撃者は TCP のセッションを張らないため RST パケットを送るといった挙動を取らない。そのため、RST パケットを受信するかどうかでクライアントが正当か攻撃者かを判定することができる。

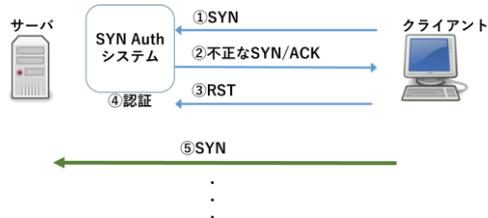


図 1 TCP SYN Authentication .

3. 既存研究

OpenFlow による TCP SYN Authentication の実現では、サーバの手前で OpenFlow コントローラと OpenFlow スイッチが連携し、認証を行う。図 2 にはデータの流れと処理手順を示す。まず OpenFlow スイッチが SYN パケットを受信すると Packet-In を行う。そして OpenFlow コントローラは不正 SYN/ACK パケットを生成し返送を行い、認証中テーブルに送信先、送信元の MAC アドレス、IP アドレス、Port 番号を Match 条件としたフローエントリ登録を行う。同クライアントからの RST パケットは登録したフローエントリにヒットし Packet-In を行った後、認証済テーブルに同様の Match 条件としたフローエントリ登録を行い認証完了する。

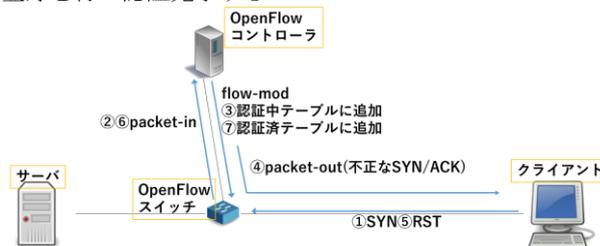


図 2 OpenFlow による TCP SYN Auth システム

4. OpenFlow 1.5 による実現

OpenFlow1.3 の場合スイッチは TCP コントロールフラグの認識や OpenFlow スイッチ上でのパケットの動的な書き換えを行うことはできない。そのため、Packet-In を行い OpenFlow コントローラによる書き換えが必要になる。また、OpenFlow スイッチがフローエントリのアクションとして新たなフローエントリを登録することもできない。そのため、Modify Flow Entry メッセージを利用する必要がある。従って TCP SYN Authentication の実現には、OpenFlow コントローラを介してクライアントへの不正 SYN/ACK パケットの返送と認証のためのフローエントリ登録をしなければならない。攻撃の負荷が高まると Packet-In メッセージのオーバーヘッドにより性能が低下していくことになる。

本システムで OpenFlow のバージョン 1.5 で加わったヘッダ情報をコピーできる OFPAT_COPY_FIELD と Nicira 拡張機能のフローエントリの生成登録する NXAST_RAW_LEARN, フローエントリの再検索を行う NXAST_RESUBMIT を利用する。SYN パケットを OpenFlow スイッチが受信すると、OFPAT_COPY_FIELD により送信元と送信先の Mac アドレス、IP アドレス、Port 番号の入れ替えを行い、TCP コントロールフラグを SYN/ACK にセットし返送する。そして Nicira 拡張機能の NXAST_RAW_LEARN によって認証中テーブルへ送信

† Faculty of CIS, Hosei University

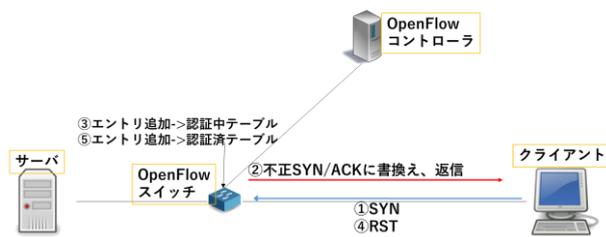


図3 OpenFlow1.5 ベース認証システム

元と送信先の Mac アドレス, IP アドレス, Port 番号を Match 条件としたフローエントリ登録する. RST パケットを同クライアントからの RST パケットを受信すると, 同様に認証済テーブルへ, 以後のパケットはサーバへ転送するフローエントリを登録する.

NXAST_RAW_LEARN の制限として登録するフローエントリの Instruction には OFPAT_OUTPUT, OFPAT_SET_FIELD のみとなっている. しかし, マルチテーブルと NXAST_RESUBMIT を用いることでその他の Instruction も実行可能である. 登録されるフローエントリには Packet-Register に条件判定用の値をセットする OFPAT_SET_FIELD を置く. さらに NXAST_RESUBMIT により再検索されたテーブル上で Packet-Register の値を Match 条件としたフローエントリをデフォルトで登録しておくことで上記の処理が可能になる.

以上の手順をソフトウェア OpenFlow スイッチである Open vSwitch により実現した. Open vSwitch のバージョン 2.8.90 は OpenFlow 1.5 に準拠しているものの, TCP コントロールフラグの書き換え機能は実現されていなかった. そこで, OFPAT_SET_FIELD の実装に TCP コントロールフラグについての追加実装を行った.

5. 評価

既存システムと本システムに TCP SYN Flood 攻撃を行った場合の防御性能の計測を行った. 評価環境は, 3.6GHz Intel i7-4790, メモリ 32GB 上で稼働する Floodlight により実装した OpenFlow コントローラと, 3.6GHz Intel i7-4790, メモリ 16GB 上で稼働する Open vSwitch を用いて, 図 3 の接続構成で行った. 攻撃ホストから被攻撃ホストに一定レートで 100 秒間 SYN パケットを送信する. レートは 22000pps から 40000pps までの 1000pps 刻みである. またここでは不正 SYN/ACK パケットを受信するまでの時間(応答時間)が 1.5 秒を超えたものはパケットロスとみなし通信に対する処理の影響を調べた. これはフローエントリのタイムアウトに設定した 3 秒に依存する. この実験では OpenFlow スイッチ上での OFPAT_COPY_FIELD によって不正 SYN/ACK パケットを生成した場合と Packet-In を行い, OpenFlow コントローラ上で生成した場合の性能が比較された. 図 4 にはそれぞれのシステムにおける平均応答時間とパケットロス率の推移を示す. 既存システムは 23000pps からパケットロスが発生し 27000pps で応答時間 1.5 秒をこえたことによるパケットロスが急増した. 本システムは Packet-In メッセージのオーバーヘッドがなくなり応答時間に向上がみ

られた. 応答時間が 1.5 秒を超えたことによるパケットロスは 40000pps でも確認されず, パケットロス率も大幅に減少した. またパケットロス率 0%は 32000pps までである.

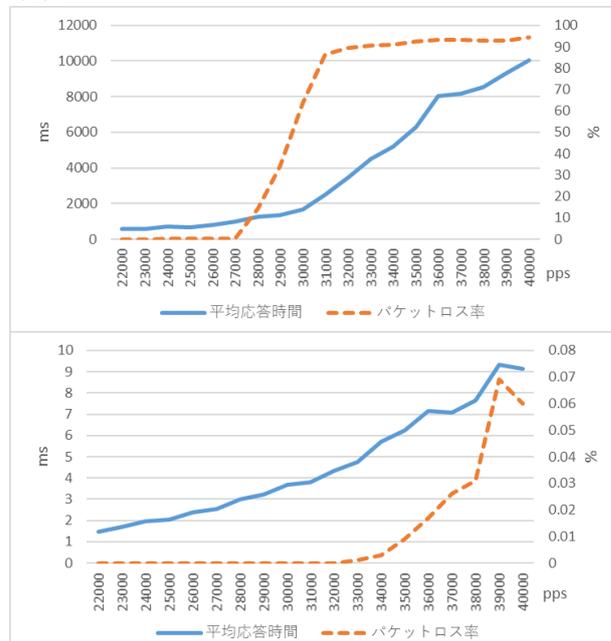


図4 平均応答時間とパケットロス率
上: 既存システム下: 本システム

6. まとめ

本研究では TCP SYN Authentication 備えた OpenFlow システムにおいて, OpenFlow1.5 をベースにし, Nicira 拡張機能を用いることで OpenFlow1.3 ベースの従来に比べより手順が簡素なシステムの実装を行った. 既存システムは不正 SYN/ACK パケットの生成とフローエントリの登録は OpenFlow コントローラを介さなければならなかった. 従って Packet-In におけるオーバーヘッドで転送効率の悪さが課題であった. 本システムは OFPAT_COPY_FIELD と NXAST_RAW_LEARN, NXAST_RESUBMIT を用いることで OpenFlow スイッチの挙動のみで認証を行える. また評価では不正 SYN/ACK パケットの生成に Packet-In を用いない本システムは従来に比べ大幅な性能向上がみられた.

謝辞

本研究は JSPS 科研費 JP 15K00138 の助成を受けたものである.

文献

- [1] OPEN NETWORKING FOUNDATION “Software-Defined Networking: The New Norm for Networks White Paper” April 13, 2012.
- [2] T. M. Tony, W. Lee., K. C. Alan, X. L. Daniel, K. H. Albert, and W. W. Judy, “Kill ’em all – ddos protection total annihilation!” DefCon 21 Hacking Conference, 2013.
- [3] 永井 亮祐, 廣津 登志夫 ” TCP SYN Authentication の OpenFlow による実現” 第 79 回全国大会講演論文集, Vol. 2017, No. 1, pp.169-170, March 2017.