7S-08

TCP SYN Authentication の OpenFlow による実現

永井 亮祐 †　　廣津 登志夫 †
† 法政大学情報科学部

1　はじめに

インターネットが重要な社会基盤になるに伴い, サイバー攻撃が問題となっている. その中でも標的となるサーバやネットワーク処理能力以上の大量のパケットを送ることによりサービスを機能停止状態にする DoS (Denial of Service) 攻撃や, 複数の端末から DoS 攻撃を仕掛ける DDoS (Distributed DoS) 攻撃は実際の EC サイトを停止させるような深刻な事態になっている. DDoS 攻撃対策は TCP SYN, UDP, HTTP GET 等の Flood 攻撃や DNS amp 攻撃などのそれぞれの攻撃の種類に応じたプロトコルレベルの対策が必要となり, これまでは専用機器で実現されていた. しかし, 専用機器は非常に高価であるだけでなく, 汎用性や攻撃の変化に対応する柔軟性に欠ける点がある.

本研究では, プロトコルレベルの DDoS 対策を OpenFlow [1] を用いて実現する. OpenFlow は Software Defined Network を実現する主要技術の一つであり, 従来のネットワーク機器で同一機器内に存在していた経路制御機能部分とデータ転送機能部分を OpenFlow スイッチ (OF スイッチ) と OpenFlow コントローラ (OF コントローラ) に分離した構造になっている. これにより, OF コントローラでソフトウェアによる高度な処理を実現し柔軟なネットワークの制御を可能にしている.

2　TCP SYN Authentication

TCP SYN Flood 攻撃の緩和手法のひとつに TCP SYN Authentication [2] がある. これはクライアントとサーバの間に専用の緩和装置を設置し, TCP 接続開始時の挙動から攻撃トラフィックを分離するものである. 3-way ハンドシェイク では, 通信相手から送られてきたパケットに返答する際の確認応答番号は受信したパケットのシーケンス番号に 1 を加えた値になる. もしも, この確認応答番号をそれ以外の値に設定して返信した場合, 通信相手は TCP 接続を中断するために RST パケットを送信してくる. 一方, 攻撃者はそのような処理を行わずに SYN パケットを送り続ける. TCP SYN Authentication では, この仕組みを利用して攻撃者の検出を行う (図 1).

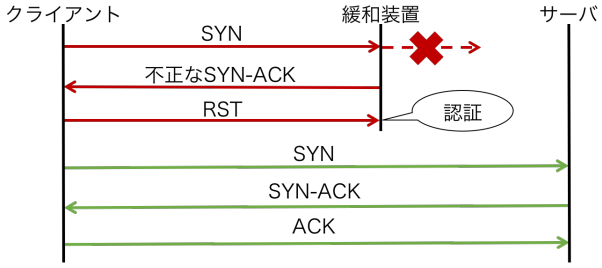

図 1: TCP SYN Authentication

具体的な処理手順は次の通りである.

1. クライアントからサーバに送られた SYN パケットを緩和装置が受信
2. 緩和装置が SYN パケットの送信元アドレスに対して, 不正な値の確認応答番号の SYN-ACK パケットを送信
3. 不正な SYN-ACK パケットを受信した正常なクライアントは接続を中断するために RST パケットを送信
4. 緩和装置が RST パケットを受信し, クライアントを認証してサーバへの通信を許可

3　OpenFlow による実現

TCP SYN Authentication を OpenFlow 上で実現するために, OF スイッチで認証済み・認証中・未認証の 3 つのフローテーブルを用意し, TCP 接続の認証状態の遷移を管理する. 図 2 に OpenFlow を用いて実装した場合の OpenFlow メッセージの流れ, 図 3 にシステム構成を示す.

1. クライアントからサーバ宛に送られた SYN パケットを OF スイッチが受信
2. OF スイッチが SYN パケットを OF コントローラに Packet In メッセージで転送
3. Packet In メッセージを受け取った OF コントローラが不正な SYN-ACK パケットを生成し, Packet Out メッセージで指示
   SYN パケットの MAC アドレス, IP アドレス, ポート番号をマッチ条件とするフローエントリの登録を Flow Mod メッセージで指示
4. Packet Out, Flow Mod メッセージを受け取った OF スイッチはクライアントに不正な SYN-ACK パケットを送信し, フローエントリを追加

Design and Implementation of TCP SYN Authentication using OpenFlow
†Ryosuke NAGAI　†Toshio HIROTSU
†Faculty of Computer and Information Sciences, Hosei University

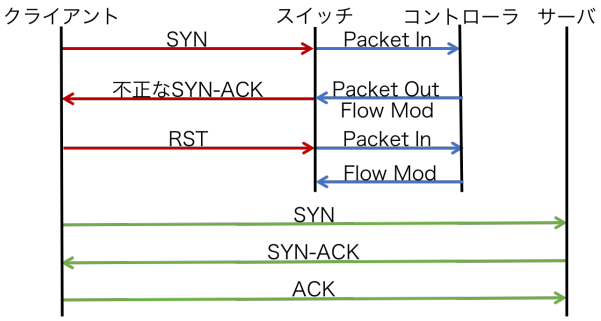

図 2: OpenFlow による TCP SYN Authentication

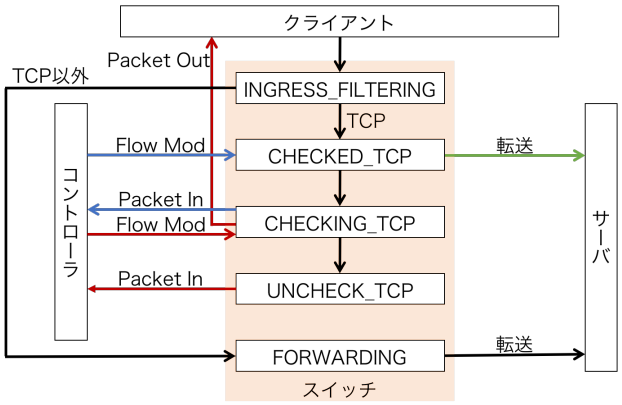

図 3: システム構成

5. 不正な SYN-ACK パケットを受け取ったクライアントは, RST パケットを送信
6. OF スイッチがクライアントからの RST パケットを受信し, それを Packet In メッセージで転送
7. Packet In メッセージを受け取った OF コントローラが RST パケットの MAC アドレス, IP アドレス, ポート番号をマッチ条件とするフローエントリの登録を Flow Mod メッセージで指示

以上の手順により, 認証中と未認証のフローテーブルはマッチする全てのパケットを Packet In メッセージにより OF コントローラへ転送する. 一方, 認証済みのフローテーブルに追加された非 DDoS 攻撃の通信は OF コントローラを介さずに OF スイッチのみで処理されるため, DDoS 攻撃による影響を受けない.

4 評価

本システムの TCP SYN Flood 攻撃に対するスループットを測定する. 評価環境は, 3.6GHz Intel i7-4790, メモリ 16GB を搭載した OF コントローラ (Floodlight) が同スペックの OF スイッチ (Open vSwitch) を管理する構成とした. 実験では, OF スイッチ配下の攻撃用ノードから被攻撃用ノードへ 100 秒間攻撃を行う. そのときの pps 値を 25000 pps から 45000 pps まで 1000 pps 刻みで変化させたときの結果を比較する.

表 1: スループット計測結果

SYN パケット (pps)	SYN-ACK / SYN (%)
37000	100
38000	99.988
39000	99.939
40000	99.937
41000	97.889
42000	91.207
43000	81.677
44000	49.690
45000	43.227

表 1 にスループット測定結果を示す. 37000 pps までは, すべての SYN パケットに対する SYN-ACK パケットが返信された. しかし, 38000 pps を超えるとパケットロスが発生した. さらに, pps 値が増加すると処理可能なパケット数が低下している. この結果より, パケットロスを発生させずに動作させる場合の本システムのスループットは 37000 pps であった. この性能上限については, スイッチの多段化や並列化などの実装の改良や OpenFlow1.5 準拠の機器による実装により, スループットの向上が見込まれる.

5 まとめ

TCP SYN Authentication の OpenFlow による実装を実現した. これにより, 特別な専用機器を用いずに通信基盤となる OpenFlow ネットワークだけで, 高度なネットワーク防御が可能になる. 将来的には, IP アドレスレベルのフィルタリングとプロトコルレベルの処理を別スイッチに分散させたり, 非 DDoS 攻撃と判定された通信に別経路や別優先度を与えたりとネットワーク基盤全体での柔軟な制御が期待できる.

謝辞

本研究は JSPS 科研費 JP15K00138 の助成を受けたものである.

参考文献

[1] M. Nick, A. Tom, B. Hari, P. Guru, P. Larry, R. Jennifer, S. Scott, and T. Jonathan, “Openflow: Enabling innovation in campus netwroks,” in *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, April 2008, pp. 70–74.

[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.