DDoS 攻撃に対するプロトコルレベル防御の OpenFlow による実装

永井 亮祐[1]　　廣津 登志夫[1]

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，サーバに対する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 攻撃に対しては 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での対策が必要となり，これまでは高価な専用機器での実現されていた．

本研究では，この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通信の経路制御機構を 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，様々な処理を OF コントローラのソフトウェアとして実現を可能にしている．この OpenFlow を用いてネットワーク基盤全体での柔軟な DDoS 攻撃の防御を実現する．

2. TCP SYN Authentication

SYN Flood 攻撃は TCP 接続確立時の 3way handshake を悪用して行われる．攻撃者は SYN パケットを送り，サーバからの SYN-ACK パケットを無視することで，サーバに half-open な状態の TCP セッションを一定時間保持させる．これを大量に行うことで，サーバのメモリ領域や管理構造を枯渇させることになり，通信帯域に余裕があってもサービスの正常な提供が阻害される．

SYN Flood 攻撃の対策として，TCP 接続を中断する RST パケットを用いて，正常なクライアントか攻撃者かを判別する TCP SYN Authentication[2]と呼ばれる手法がある．これは異常パケットを正しく処理しているかを見ており，RST パケットを返してくるクライアントのみ通信を許可する．殆どの DDoS クライアントの通信は遮断される．以下に具体的な処理を示す．

1. クライアントからサーバ宛に送られた SYN パケットを緩和装置が受信
2. 緩和装置が SYN 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 を受け取っ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

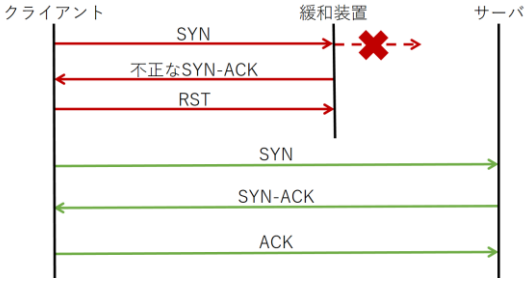

図 1 TCP SYN 認証

3. 提案手法

本論文では TCP SYN Authentication による SYN Flood 攻撃の緩和対策を OpenFlow 上で実現する．ここでは OF スイッチで複数のフローテーブルを使用し，TCP 接続の認証状態の遷移を管理する．未認証・認証中・認証済みの 3 つのフローテーブルを用意し，コントローラでフロー情報を適切なテーブルに登録・抹消する．これにより，認証の済んだ非 DDoS 攻撃の通信は OF スイッチのみで処理されるようになる．図 2 に一つの TCP セッションに対して TCP SYN Authentication の処理を行う際の OpenFlow メッセージの流れを示す．この 2 回の Packet In 前後に対して，UNCHECKED_TCP, CHECKING_TCP, CHECKED_TCP の 3 つのフロ

1 法政大学情報科学部

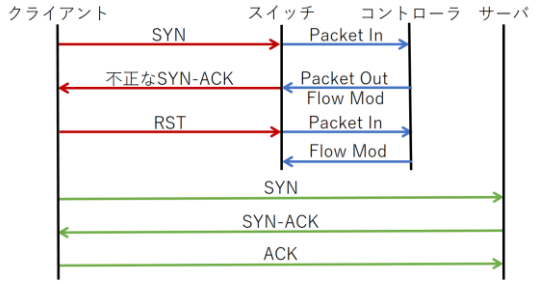

図 2 OpenFlow による TCP SYN 認証

ーテーブルを割り当てて，認証状態の管理を行う．システム構成を図 3 に示し，以下に処理手順を説明する．

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エントリの登録を Flow Mod メッセージで指示
4. 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，フローテーブルを追加
5. 不正な SYN-ACK 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 OF コントローラに 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エントリの登録を Flow Mod メッセージで指示

4. 実装

Ryu[3] を用いて前節に提案した TCP SYN Authentication の仕組みを L2 スイッチコントローラに組み込んだコントローラを実装した．ここでは OpenFlow1.3 の Lagopus switch[4]を用いて，動作の確認と初期的なスループットの測定を行った．TCP SYN Authentication を実装した OF スイッチに 2 台のマシンを接続し，一方から他方へ片方向で SYN パケットを送信した．SYN Flood 攻撃と同様に SYN パケットを送信するだけのものは遮断し，

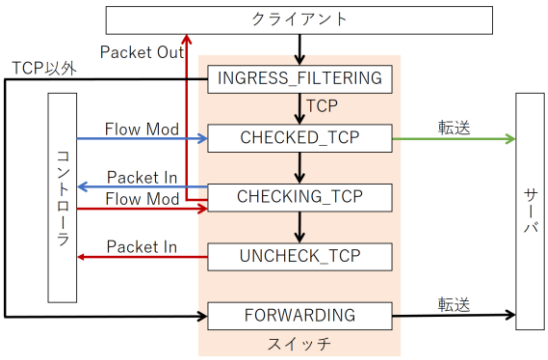

図 3 システム構成

通常の TCP の通信は確立するという期待通りの挙動を確認した．現段階の性能は，1000pps 程度でパケットのロスが発生しており，処理の余裕がなくなることが判明している．

5. まとめ

本研究では TCP SYN Authentication による DDoS 防御を OpenFlow で実現した．OpenFlow で実現することにより，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負荷分散させたり，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．性能面ではチューニングや実装の改良によるスループットの改善が必要な面はあるが，OpenFlow1.5 では SYN パケットや RST パケットの判定をスイッチ側でできるようになるため，将来的には性能の改善を見込むことができる．

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] N.McKeown, T.Anderson, H.Balakrishnan, G.Parulkar, L.Peterson, J.Rexford, S.Shenker, J.Turner, “OpenFlow: enabling innovation in campus networks”, ACM SIGCOMM Computer Communication Review, 38, 2, pp69-74, April 2008.

[2] Tony T.N. Miu, W.L. Lee, Alan K.L. Chung, Daniel X.P. Luo, Albert K.T. Hui, and Judy W.S. Wong, “Kill ‘em All – DdoS Protection Total Annihilation!”, DefCon 21 Hacking Conference, Las Vegas, USA, August 2013

[3] Ryu SDN Framework. https://osrg.github.io/ryu/

[4] Lagopus switch. http://www.lagopus.org/