擬陽性排除サーバを用いた HTTP フラッド攻撃緩和手法の提案

有川　佑樹 [a)]・久保田　真一郎 [b)]・山場　久昭 [c)]・岡崎　直宣 [d)]

A Proposal of a Mitigation Method of HTTP Flood Attacks Using a Server for Detailed Examination of Pseudo Positive Accesses

Yuki ARIKAWA, Shin-Ichiro KUBOTA, Hisaaki YAMABA, Naonobu OKAZAKI

Abstract

Typical mitigation for DDoS attack discarded legitimate user packets of at the same time as the attack packets so that the false positive problem of identifying the attacker despite the legitimate user cannot be eliminated. In this paper, we propose the system distributing accesses with OpenFlow to two types of server, a main server with allows only legitimate accesses and a sub server with allows certain attacks. The First threshold is set to eliminate any attacks, the second threshold is set to allow certain attacks. Packet determined to a attack in the second threshold is discarded. Our approach is to allow certain attacks in the second threshold despite of accesses discarded by the first threshold. This approach seems to result the number of false-positive cases decreases, and the legitimate users can succeed to use services.

Keywords: DDoS, OpenFlow, HTTP flood attack

1. はじめに

インターネットが社会基盤としての重要な役割を担う現代において，サービスを機能不全に陥らせる DDoS(Distributed Denial of Service) 攻撃は大きな脅威である．この攻撃に対してファイアウォールや IDS を用いてトラフィック量で判定を行う場合，正規ユーザのパケットも判定するトラフィックに含まれ，この攻撃は正規のトラフィックと見分けが付かない．そのため，攻撃を受けても継続してサービスを提供できる緩和策が必要であり，研究が行われている [1)2)]．

しかし，既存の緩和策では，攻撃パケットと同時に正当なユーザのパケットも破棄されるため，攻撃者でないにも関わらず攻撃者と識別する擬陽性の問題を排除することができない．これは既存の緩和策が，DDoS 攻撃と正当なトラフィックを判別することができないファイアウォールや IDS に依存しているためである．

そこで本論文では，DDoS 攻撃であると判定する閾値を 2 段階に設定し，判定された結果をもとに，正当なアクセスのみを許すメインサーバと，ある程度の攻撃を許容するサブサーバとに OpenFlow により振り分けるシステムを提案する．1 段階目の閾値は厳しい攻撃判定を行うよう設定し，2 段階目の閾値はある程度の攻撃を許す設定にする．2 段階目の閾値で攻撃と判定されたパケットは OpenFlow の制御により破棄される．1 段階目の判定により破棄されるアクセスであっても 2 段階目の判定によりアクセスを許すことで，システムとしては誤検知を少しでも減らし，正当なユーザがサービスを継続して受けることができると考えている．また本論文では数ある DDoS 攻撃の中でも HTTP フラッド攻撃に焦点を絞る．

この提案手法ではサブサーバに振り分けられた正当なユーザがパフォーマンスの劣化したサービスを受けることになるため，最終的にはサブサーバに振り分けられたパケットを解析し，再度メインサーバへの振り分け及び破棄を行う制御情報を OpenFlow コントローラにフィードバックする機能の実装を目指している．本論文では，その一部の機能である 2 段階の閾値を設定しメインサーバとサブサーバにパケットを振り分ける機能が誤検知率を下げるのに有効な手段であるか検討する．

表 1. 制御の例

パケットの条件	処理方法
宛先 TCP ポート = 80	物理ポート 1 から転送
送信元 IP アドレス = 192.168.1.10	パケットを破棄

2. OpenFlow

既存研究及び本提案システムで用いる OpenFlow[1)] について説明する．OpenFlow はソフトウェアによってネットワークを制御する技術であるため，柔軟で自由度の高い制御機能を備えたネットワークを構築することができる．OpenFlow によってスイッチで実行できる処理の例を表 1 に示す．

また，パケットの条件であるマッチングルールはレイヤ 1 からレイヤ 4 までの情報を用いることができる．表 2 に OpenFlow version 1.0 で扱うことのできる情報を示す．

OpenFlow は従来のスイッチの機能である経路制御とデータ

[a)] 工学専攻大学院生
[b)] 情報システム工学科准教授
[c)] 情報システム工学科助教
[d)] 情報システム工学科教授

表 2. マッチングルールで使用できる情報

レイヤ	扱える情報
物理層	スイッチの物理ポート番号
データリンク層	送信元 MAC アドレス
	宛先 MAC アドレス
	Ethernet タイプ
ネットワーク層	送信元 IP アドレス
	宛先 IP アドレス
	IP プロトコル
	IP の ToS 情報
トランスポート層	TCP/UDP の送信元ポート番号
	TCP/UDP の宛先ポート番号
	VLAN ID
	VLAN 優先度

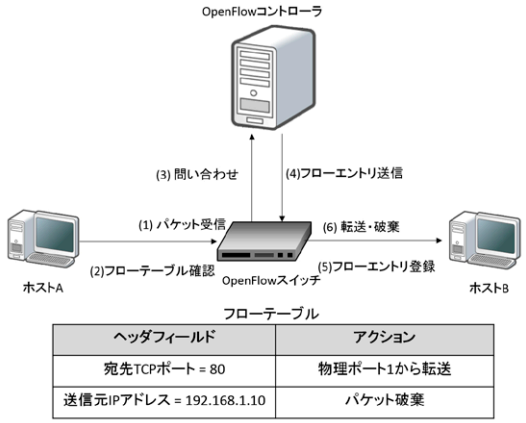

図 1. OpenFlow の構成図

転送の機能を別々の機器に分離している．そのため，経路制御を担う OpenFlow コントローラとデータ転送を担う OpenFlow スイッチの 2 つの機器から構成される．OpenFlow コントローラは，フローエントリと呼ばれる受信したパケットの処理方法を示す情報を OpenFlow スイッチに送信することで，パケットの転送や破棄を行う．フローエントリは OpenFlow スイッチ内のフローテーブルに登録される．

2.1 処理手順

ホスト A からホスト B へ通信する例である図 1 をもとに OpenFlow の処理手順を説明する．

(1) OpenFlow スイッチがポートから入るパケット信号を受信する．

(2) OpenFlow スイッチは処理方法を記憶しているかフローテーブルをチェックする．

(3) 処理方法を記憶してなければ OpenFlow コントローラに処理方法を問い合わせる．

(4) OpenFlow コントローラが OpenFlow スイッチにフローエントリを送信する．

(5) フローエントリをフローテーブルに登録する．

(6) フローエントリに従ってパケットを処理する．

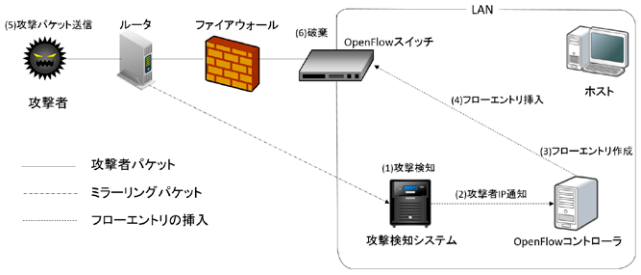

図 2. OpenFlow を用いた攻撃者遮断システムの構成図

3. DDoS 攻撃緩和システムの既存研究

3.1 OpenFlow を用いた攻撃者遮断システム

OpenFlow を用いた攻撃者遮断手法 [1] は IDS と OpenFlow コントローラを連携させ，動的なフローエントリを OpenFlow スイッチに登録することで攻撃者の通信を遮断する緩和策であり，実験によりサーバの応答率や応答時間の改善に有効であることが確認されている．この既存手法の処理手順を図 2 に示す．

(1) IDS が攻撃者を検知する．

(2) IDS が攻撃者 IP アドレスを OpenFlow コントローラに通知する．

(3) OpenFlow コントローラが，通知された攻撃者 IP アドレスのフローを破棄するフローエントリを作成する．

(4) OpenFlow コントローラが OpenFlow スイッチにフローエントリを挿入する．

(5) 攻撃者が攻撃パケットを送信する．

(6) OpenFlow スイッチが攻撃者からのフローを破棄する．

既存手法は DDoS 攻撃と判定された IP アドレスのパケットを破棄するフローエントリを作成して攻撃パケットを排除する方法である．しかし DDoS 攻撃を IDS によってトラフィック量で判定を行う場合，正規ユーザの IP アドレスもパケット破棄の対象となってしまい，正規ユーザがサービスを利用できなくなる恐れがある．判定技術の向上ももちろんあるが，IDS が攻撃者と正当なユーザを正確に判定できない場合でもサービスのパフォーマンスが劣化せず，誤検知率が下がるような検討が必要である．

3.2 DNS を用いた DDoS 攻撃回避システム

DNS を用いた DDoS 攻撃回避システム [2] は Web サーバの IP アドレスを変更する方法を用いて，正規ユーザに影響を与えず DDoS 攻撃による被害を緩和するシステムである．正規ユーザのアクセス成功率でシステムの有効性を評価した結果，DDoS 攻撃に対し有効であることが確認されている．この既存手法の処理手順を図 3 を用いて説明する．

(1) IDS サーバが攻撃を検知する

(2) DNS サーバ及び Web サーバに回避先 IP アドレスを報告し，回避要請をする

(3) 要請を受けたサーバは IP アドレスの変更を行い DDoS 攻撃を回避する．

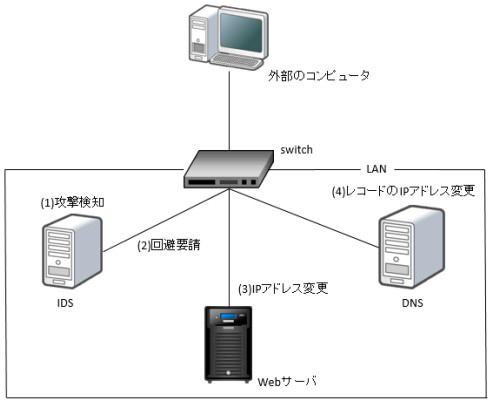

図 3. DNS を用いた DDoS 攻撃回避システムの構成図

(4) IDS サーバからの要請に従い DNS サーバは A レコードに書かれている Web サーバの IP アドレスの値を変更する．

攻撃ホストは攻撃を開始する前に攻撃先 Web サーバの IP アドレスを取得して DDoS 攻撃を開始する．しかし攻撃を IDS が検知し，Web サーバと DNS サーバに DDoS 攻撃回避を要請するため Web サーバの IP アドレスが変わり攻撃は失敗する．これに対し正規ユーザは毎回 DNS サーバに接続して IP アドレスを取得するため，Web サーバへのアクセスが成功する．以上のように DDoS 攻撃を緩和しつつ正規ユーザにサービスを提供できる．しかし，この手法では変更された IP アドレスを追跡し続ける DDoS 攻撃は緩和することはできない．また，IDS の検知ルールに当てはまる攻撃パケットが一度でも通過すると具体的被害が発生していない時点で IP アドレスが変更されるため，IP アドレスの切り替え時間が全体的に増加して正規ユーザがサーバにアクセスできなくなる時間が増加してしまう．よってサービスを行うサーバの IP アドレスを変更せずに DDoS 攻撃を緩和できる対策が必要となる．

4. 提案手法

4.1 概要

本提案手法は DDoS 攻撃であると判定する閾値を 2 段階に設定し，判定された結果をもとに，正当なアクセスのみを許すメインサーバと，ある程度の攻撃を許容するサブサーバとに OpenFlow により振り分ける．1 段階目の閾値は厳しい攻撃判定を行うよう設定し，2 段階目の閾値はある程度の攻撃を許す設定にする．つまり 1 段階目の判定により確実に正当なユーザだと判定されるとメインサーバに振り分けられ，1 段階目の判定により確実に正当なユーザだと断定することはできないが逆に 2 段階目の判定で確実に攻撃者であると断定することもできない場合サブサーバに振り分けられる．2 段階目の閾値で攻撃と判定されたパケットは破棄される．1 段階目の判定により破棄されるアクセスであっても 2 段階目の判定によりアクセスを許すことで，攻撃者でないユーザを攻撃者と識別してパケットを破棄する擬陽性の問題が緩和され，正規ユーザがサービスを継続して受けることができる．

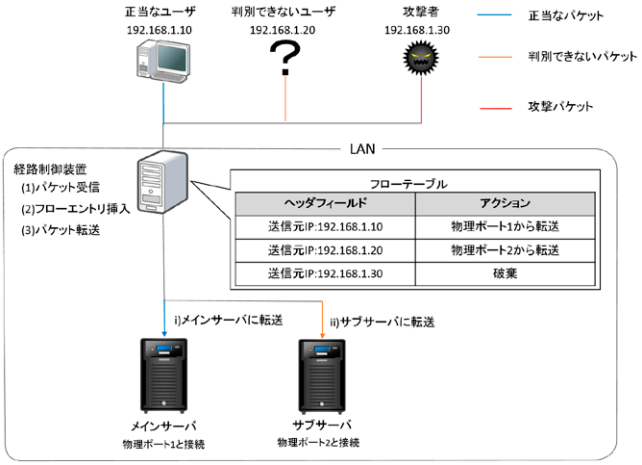

図 4. 提案手法の構成図

4.2 提案手法の構成

提案手法の構成図を図 4 に示す．経路制御装置は経路制御とパケット転送を行う装置であり，OpenFlow コントローラ，OpenFlow スイッチ，侵入検知システムである snort から構成される．メインサーバは確実に攻撃者ではないと判断されたホストのみと通信を行う．正当な利用者へ正常なパフォーマンスのサービスを提供することを目的としている．サブサーバはメインサーバと同じサービスをユーザに提供しており，攻撃者もしくは正当な利用者か判断が難しいホストとの通信を行う．このサブサーバを用いることで，正当な利用者が攻撃者であると誤検知される偽陽性の問題を排除することを目指す．

4.3 処理手順

図 4 により処理手順を説明する．

(1) パケット受信

OpenFlow スイッチがパケットを受信すると，snort から OpenFlow コントローラへアラートが送信される．OpenFlow コントローラは送信元 IP アドレス毎にアラートの数をカウントする．

(2) フローエントリ挿入

OpenFlow スイッチにフローエントリを挿入する．挿入するフローエントリはアラート数によって異なる．仮の閾値を設定し，挿入するフローエントリの例を示す．

仮の閾値設定

1. 1 秒間のアラート数が 10 回以下の場合は正当なユーザと判断する．
2. 1 秒間のアラート数が 11 回以上 100 以下の場合は正当なユーザか攻撃者か判別できないユーザと判断する．
3. 1 秒間のアラート数が 101 回以上の場合は攻撃者と判断する．

フローエントリ挿入の例

1. アラート数 $<$ 11
   メインサーバへ転送するフローエントリを挿入
2. 10 $<$ アラート数 $<$ 101
   サブサーバへ転送するフローエントリを挿入

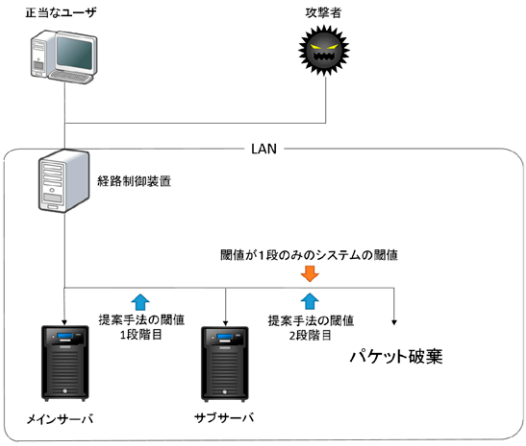

図 5. 実験環境の構成図

3. 100 < アラート数
   パケットを破棄するフローエントリを挿入

(3) パケット転送
フローエントリに従って，パケットの転送及び破棄を行う．

5. 実験計画

本章では提案手法の有効性を検証する実験の計画について説明する．

5.1 概要

提案手法の特徴は，閾値を 2 段階に設定することで 1 段階目の判定により破棄されるアクセスであっても 2 段階目の判定によりアクセスを許可できることであり，これにより正当なユーザを攻撃者だと誤って判定する誤検知を減らし，正当なユーザがサービスを継続して受けることができると考えている．よって実験では提案手法を閾値が 1 段のみであるシステムと比較することで，提案手法が誤検知率を下げるのに有効であるか，また正当なユーザに対するサーバのパフォーマンスが向上するか検証する．

5.2 実験環境

実験環境を図 5 に示す．ホスト 2 台，サーバ 2 台，経路制御装置 1 台を VirtualBox で作成し，仮想ネットワーク上で実験を行う．OpenFlow 環境は ryu version 3.2.6[3] と Open vSwitch version 2.4.0 で作成し，IDS には snort を使用する．また，閾値が 1 段階のみのシステムはメインサーバとサブサーバによる分散処理を行う．

5.3 実験方法

閾値が 2 段の提案手法及び閾値が 1 段のみの 2 つのシステムに対し，HTTP フラッド攻撃が行われている状態にしたうえで正当なユーザから http リクエストを送信する．そのときの誤検知率と正当なユーザに対するサーバからの応答時間の平均をそれぞれ求め，2 つのシステムを比較する．

6. 考察

DDoS 攻撃はファイアウォールや IDS を用いてトラフィック量で判定を行う場合，正規ユーザのパケットも判定するトラフィックに含まれ，正規のトラフィックと見分けが付かない．よって一般的な緩和策では，DDoS 攻撃を受けた際に攻撃パケットと同時に正当なユーザのパケットまで破棄されてしまうため，誤検知率が高くなってしまう．しかし提案手法は，一般の緩和策では破棄されるパケットをある程度の攻撃を許容するサブサーバによって受け取ることができるため誤検知を減らすことができると考えている．

サーバが DDoS 攻撃を受けると処理能力が落ち，応答速度が遅くなるなどサービスのパフォーマンスが劣化する．分散処理といった緩和策を講じても，正当なユーザは攻撃を受けているサーバと通信を行うため，サービスパフォーマンスの劣化を回避することはできない．これに対し，提案手法では確実に正当だと判断できるユーザのみメインサーバと通信させることで，パフォーマンスの劣化がないサービスを正当なユーザに提供できると考えている．

提案手法の閾値はメインサーバとサブサーバの境界となる 1 段階目の閾値，サブサーバとパケット破棄の境界となる 2 段階目の閾値の 2 つがある．誤検知率を低くするためには破棄するパケットを少なくする必要があるため，2 段階目の閾値はサブサーバのパフォーマンスが許容できるレベルである限り攻撃を許容する設定にするのが適切だと考えられる．また，正当なユーザに対するサービスのパフォーマンス劣化を防ぐためにはメインサーバに送信される攻撃パケットを少なくする必要があるため 1 段階目の閾値を出来るだけ厳しく攻撃判定を行う設定にするのが適切だと考えている．

提案手法では DDoS 攻撃か正規のトラフィックか判別できないパケットはサブサーバに振り分けられるが，この方法ではサブサーバに振り分けられた正当なユーザはパフォーマンスの劣化したサービスを受けることになり，攻撃パケットはサブサーバに負荷をかけ続けることになる．これを解決するためにサブサーバに振り分けられているパケットを分析し，改めてメインサーバとパケット破棄に振り分ける機能を実装する必要がある．

7. まとめ

本論文では DDoS 攻撃に対して 2 段階の閾値を設定しメインサーバとサブサーバにパケットを振り分けることで擬陽性の問題を緩和し，正当なユーザができるだけサービスを利用できる手法を提案した．また，提案手法は一般の緩和策より誤検知率が低く，正当なユーザに対するサービスの応答速度が向上すると考えている．今後はサブサーバに振り分けられているパケットを分析し，正当なユーザはメインサーバへ，攻撃者はパケット破棄へ再び振り分ける方法について検討していきたい．

参考文献

1) 下川大貴，小刀祢知哉，池部実，吉田和幸：OpenFlow を用いた攻撃者遮断システムの提案と評価，マルチメディア，分散協調とモバイルシンポジウム 2014 論文集，pp.197-204,(2014).

2) 安部幸太郎，森口一郎：DNS を用いた DDoS 攻撃回避システム，東京情報大学研究論集 17(2)，pp.63-72，(2014).

3) SDN Framework，https://osrg.github.io/ryu-book/ja/Ryubook.pdf,(2015.10.30).