3Z-5

OpenFlow を用いた DDoS 攻撃検知システムの検討

太田　悟† 田島　信一† 佐藤　信‡ 長野　純一‡ 篠宮　紀彦† 勅使河原　可海†
創価大学工学部† 創価大学大学院工学研究科‡

1　はじめに

近年，インターネットの急速な普及により，インターネットサービスは，ビジネスや政治での重要なインフラになった．それに伴い，大量のパケットを標的と定めたホストに送ることでインターネットサービスを妨害する Denial of Service（DoS）攻撃や，複数のホストから DoS 攻撃を仕掛ける Distributed DoS（DDoS）攻撃が問題となっている．DoS 攻撃・DDoS 攻撃を利用したサイバー恐喝やサイバーテロが今後ますます深刻化していくと予想される．

DoS 攻撃・DDoS 攻撃は攻撃対象となるサーバやサービスを使用不可能にすることを目的にしているが，発信元 IP アドレスなどをもとにした一般的なフィルタリングによる防御が困難である．その理由として，IP スプーフィング技術を用い，発信元 IP アドレスを偽装するため，攻撃者の特定が困難である．さらに，DoS 攻撃・DDoS 攻撃は正当な通信との区別が難しいことが挙げられる．

一方で，既存のスイッチ網を再構成するネットワークアーキテクチャとして OpenFlow スイッチング技術が注目されている[1]．OpenFlow は，通信の開始から終了までを 1 つのフローとして処理を行う．フローとはパケットのヘッダに含まれる L1 層から L4 層までの情報を任意に組み合わせたものである．また OpenFlow ではスイッチの機能がコントローラ部とスイッチ部に分かれており，OpenFlow コントローラ（OFC）が各 OpenFlow スイッチ（OFS）へ転送ルールに相当するフローエントリを送信し，OFS は受け取ったフローエントリに従ってパケットを転送する．このように，コントローラ部とスイッチ部を分けることにより，柔軟かつ集中的な管理制御を行うことができ，プログラマブルなスイッチを用いたネットワークを実現する手段となっている．

本研究では OpenFlow の機能を拡張することにより DoS 攻撃・DDoS 攻撃を自動的に検知しフィルタリングするためのシステムを開発することを目的としている．本稿では，DoS 攻撃・DDoS 攻撃検知システムを検討する．

2　検討課題と研究目的

現在，行われている被害者側での DoS 攻撃・DDoS 攻撃を対処するための手順を以下に述べる．

1. インターネット上のサービスを提供しているネットワーク管理者が，サービスを利用しているユーザから，サービスにアクセスできない，サーバにつながりにくいなどの連絡を受ける．
2. 連絡を受けたネットワーク管理者は，問題の原因を調査する．この時点ではサービスを利用できない原因が，ネットワーク機器の故障，ケーブルの断線，設定ミスなども考えられる．このため，原因が DoS 攻撃・DDoS 攻撃によるものであると直ちに断定することができない．
3. サーバのアクセスログや，ルータのモニタリングによる調査の結果，サービスを提供しているサーバの処理能力を超える大量のパケットが，ネットワーク上にあふれていることが確認される．これにより，問題の原因が DoS 攻撃・DDoS 攻撃であることが発覚する．
4. 問題の原因が発覚したのち，DoS 攻撃・DDoS 攻撃の対策チームを結成する．
5. 対策チームにより，サーバに送られてくるパケット情報を解析し，攻撃パケットの特徴を抽出する．抽出した特徴を利用して，攻撃パケットのフィルタリングするルールを作成する．
6. 対策チームは，フィルタリングルールをルータやファイアウォールに手作業で設定していく．

以上の手順により，対策が行われている．DoS 攻撃・DDoS 攻撃の攻撃元の特定や対処は，プロバイダが行うため，被害者側ではこれ以上の対策は出来ない．

攻撃の対処は，すべて手作業で行うため時間がかかる．また，フィルタリングルールの設定には専門的な技術が必要であり，ルータやファイアウォールの設定におけるミスも発生しやすい．そのため，被害が拡大し攻撃者の目的が達成されてしまう．被害の拡大を防ぐためには，短時間で攻撃に対処する必要がある．

本研究では OpenFlow の機能を拡張することにより DoS 攻撃・DDoS 攻撃を自動的に検知しフィルタリングするためのシステムを開発することを目的としている．これにより，被害者側での対策における原因特定の時間を減らし，さらにフィルタリングルールを作成するためのパケットの解析をリアルタイムで行う．また，フィルタリングルールの設定も自動で行うことで，DoS 攻撃・DDoS 攻撃に迅速かつ動的に対応し，被害を最小限にとどめることができる．

現在では OpenFlow を用いた DoS 攻撃・DDoS 攻撃を自動で検知しフィルタリングするシステムは存在しないため，本研究では DoS 攻撃・DDoS 攻撃検知システムを作成する．検知システムを作成するために，今回はある既存手法を OpenFlow に適応させることで，実現可能性を検証する．

また，OpenFlow に防御システムを導入する際の問題として，OpenFlow のスイッチ部で観測されるすべてのパケットのヘッダ情報をコントローラ部に通知するため，トラフィックの処理に影響が出る場合がある．そのため本研究においては DoS 攻撃・DDoS 攻撃を検知することと，安定した通信の両立が重要な課題になる．現在，OpenFlow において，どのような手法が効果的であるのかという指標がない．そこで，いくつかの既存手法を OpenFlow に適応することで，既存手法との違いや，OpenFlow での利点や課題を明らかにしていく．

A Study on a Distributed DoS attack detection system using OpenFlow

Satoru Ota†, Sinichi Tajima†, Makoto Sato‡, Junichi Nagano‡, Norihiko Shinomiya† and Yoshimi Teshigawara†
†Faculty of Engineering, Soka University
‡Graduate School of Engineering, Soka University

3　攻撃検知手法の検討

防御システムに必要な機能としては，攻撃の検知と攻撃パケットのフィルタリングの 2 つが存在する．しかし，攻撃の検知の機能においては，今回は攻撃の検知に焦点を当てる．OpenFlow の主な特徴として，パケット情報の簡単な解析が可能であること．また，OFS で処理したパケットの統計情報を OFC に通知出来ることが挙げられる．そこで，今回はこの特徴を用いた攻撃検知システムを検討する．

そこで，観測トラフィックの統計的性質を利用した DDoS 攻撃の検知方法[2]を OpenFlow に適応することで，DDoS 攻撃を検知するシステムを作成する．

すべての観測された TCP トラフィックにおいて，SYN パケットの到着レートの平均および分散を算出し，式(1)によっての正規分布によるモデル化を行う．

$$F(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}\sigma} \exp\left[\frac{-(y-\mu)^2}{2\sigma^2}\right] dy \qquad (1)$$

y：単位時間毎の SYN パケット到着レート
σ^2：SYN パケット到着レートの分散
μ：SYN パケット到着レートの平均

ただし，式(1)は±∞における領域での正規分布であるが，SYN パケット到着レートは 0 以上の範囲で変動するため，式(1)の非負領域を用いる．すなわち，

$$G(x) = \frac{F(x) - F(0)}{1 - F(0)} \qquad (2)$$

により与えられる式(2)によってモデル化を行う．

さらに，正常でないトラフィックを検出するために，SYN パケット到着レートの分布を調べ，正規分布からの平均二乗誤差を導出する．はじめに，モデル化に用いる SYN パケットの到着レートのサンプル数を n，直近 n 個の SYN パケット到着レートを r1，r2, . . . , rn とする．ただし，ri($1 \le i \le n$)はあらかじめ昇順にソートされているものとする．このとき平均二乗誤差 D を以下の式で与える．

$$D = \frac{\sum_{i=1}^{n} \left(G(r_1) - {}^{i}/_{n}\right)^2}{n} \qquad (3)$$

観測されるトラフィックを単位時間毎に，式(3)を用いて D を算出し，D が急激に上昇した SYN パケットの到着レートの観測箇所においては，攻撃による影響であると判定して検出を行う．判定には閾値を用いて検出を行う．

4　実験・評価

実験構成を図 1 に示す．実験は次のように行う．

1. 3 つの異なるホストを送信元，送信先，攻撃元として OFS に接続し，送信元，送信先間でトラフィックを発生させる．
2. 一定時間後，攻撃元ホストから SYN Flood 攻撃を発生させる．
3. OFC により平均二乗誤差を算出し，その上昇率を計算する．
4. ステップ 2 と 3 を繰り返し行う．

本稿では，モデル化に用いる SYN パケット到着レートは直近 20 個，通常トラフィック量は平均 20 packets/sec を用いる．攻撃については，攻撃元ホストから 500packets/sec の SYN パケットを約 1 分間，間隔をあけて 10 回発生させる．結果を図 2 に示す．

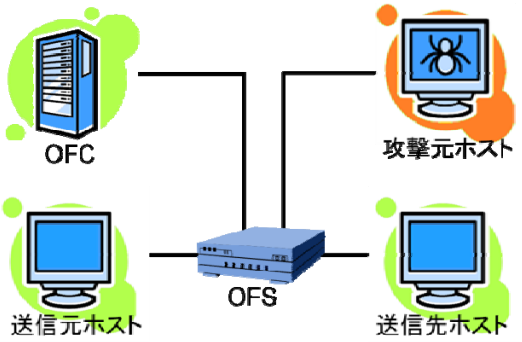

図 1　実験構成

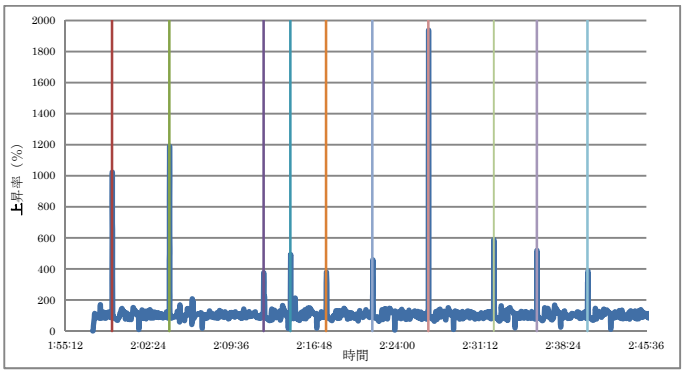

図 2　実験における平均二乗誤差の上昇率

実験により，提案手法の検出性能を評価する．評価方法として，SYN パケット到着レートの平均二乗誤差の上昇率により，SYN Flood 攻撃を検出できる閾値を考える．また，評価指標として攻撃未検出率および誤検出率を定義する．これらは以下の式で与える．

$$\text{攻撃未検出率} = \frac{\text{攻撃検出ができなかった箇所}}{\text{定義されている攻撃箇所の総数}}$$

$$\text{誤検出率} = \frac{\text{実際には攻撃ではないが検出された箇所}}{\text{攻撃と検出された総数}}$$

閾値が約 250 以下であればすべての攻撃を検出することが可能である．閾値を小さくすると攻撃発生時にトラフィックが段階的に増加する場合，同一の攻撃を何度も検出してしまう箇所（2 箇所）があるため．誤検出率は 0 であると考えることができる．

5　まとめと今後の課題

本研究では，OpenFlow を用いた DDoS 攻撃の防御システムの開発を目的としており，本稿では，トラフィックの到着レートの統計的な性質を利用した DDoS 攻撃検知システムを OpenFlow の機能を拡張することで適応した．実験から，開発したシステムは，想定した攻撃をすべて検出できた．このため，2 章で述べた課題を解決する見通しが得られた．今後の課題としては，実環境におけるシステムの動作の確認，またシステムの最適化があげられる．さらに，本稿では検知について取り上げたが，攻撃パケットをフィルタリングするためのシステムの開発を行っていく．

参考文献

[1]　OpenFlow：OpenFlow．http://www.openflow.org
[2]　三島 大季，安達 直世，滝沢 泰久："統計情報を利用した DDoS 攻撃フィルタリング手法"電子情報通信学会施術研究報告，Vol. 109, No.137, IA2009 22, pp.7-11, 2009.07