講演番号：41

SDNの特徴を利用したDDoS攻撃検知処理削減方式の提案

Reduction Method of DDoS Attack Detection Processing in SDN-based networks

B−14

山内　遼太郎†　　栗林　伸一†

Yamauchi Ryotaro and Kuribayashi Shin-ichi

†成蹊大学理工学部 Faculty of Science and Technology, Seikei University

1. まえがき

近年、DDoS攻撃が大規模化しており、従来よりも効率的にこの攻撃を防ぐ方法が求められている。その対策の1つとして、ネットワークを集中的かつ一元的に管理するSDN（Software Defined Network）の特徴を利用したDDoS攻撃検知・規制を行う方式が提案されている[1]。しかし、攻撃検知のため、SDNコントローラが通信フロー毎にトラヒックデータ(統計情報)を周期的にスイッチに問い合わせる必要があり、大きな処理負荷を伴う。

本論文では、OpenFlow[2]のメータ機能を拡張し、SDNコントローラにおけるDDoS攻撃検知のための周期的なトラヒックデータ問い合わせ処理を大幅に削減する方式とそれに伴うOpenFlow仕様の拡張を提案する。

2. SDNコントローラにおけるトラヒックデータ（統計情報）問い合わせ処理削減方式

2.1 方式概要

・攻撃検知アルゴリズムは複数あり、アプリ種別や状況に応じて適切なものを選択する。

・OpenFlowのメータ機能を拡張し、監視対象通信フロー毎に攻撃検知アルゴリズム番号とその判定条件を事前にスイッチ側に設定し、条件を満たした時点で‘異常’をSDNコントローラに通知する。検知アルゴリズム番号に対応する処理プログラムは事前にスイッチに設定されているものとする。

・通知を受けたSDNコントローラは他情報も踏まえ、最終的に攻撃の判定を行う。攻撃と判定した通信フローのパケットを廃棄または攻撃チェック分析装置へ転送するように、（送信側にもっとも近い）スイッチへ指示する。

・攻撃と判定した通信フローに関連する他通信フローに対しても同じ規制を行うことも考える。

・スイッチ側については、SDNコントローラと同様にやり取りするメッセージ数が従来よりも大幅に削減される反面、従来SDNコントーラで実施していた状態判定処理が追加される。このため、SDNコントローラに比べ処理負荷削減効果は小さい。

2.2 OpenFlow仕様の拡張

上記2.1節で提案した方式を実現するために以下の仕様拡張が必要となる。

①Meter Modificationメッセージへ新フィールド追加
- −攻撃検知アルゴリズム番号
- −攻撃検知アルゴリズムで使用する判定条件

＊判定条件を満足したらSDNコントローラに‘異常’を通知する。

②スイッチ側からSDNコントーラ側へ通知するため、以下のフィールドを含む「Reportメッセージ」を新設
- −レポート種別(異常の通知など)
- −メータID
- −メータ統計データ

2.3 提案方式のメッセージシーケンス

提案方式に基づくメッセージシーケンス例を図1に示す。破線は従来やり取りしていたが今回不要になるメッセージ、一点鎖線は新たにやり取りするメッセージをそれぞれ示す。

1)SDNコトローラからスイッチに対して、2.2節①で示したフィールドを含むMeter Modificationメッセージを送出する。

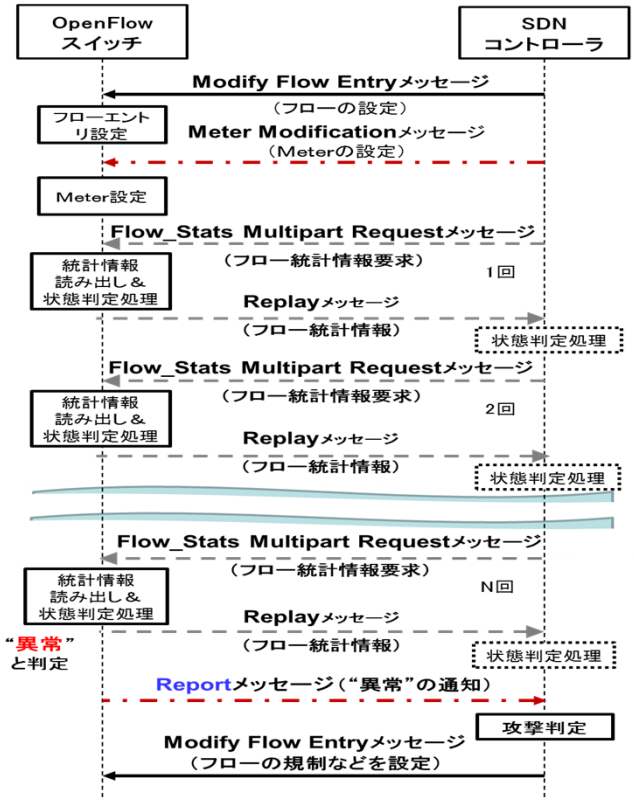

図1. 提案方式の攻撃検出、規制までのメッセージシーケンス例

2) 従来と異なり、フロー毎の統計情報の要求であるFlow_Stats multipart Request メッセージとその応答であるReplyメッセージの周期的なやり取りは不要となる。攻撃検出までに平均N周期要し、監視フロー数をFとすれば、SDNコントローラ全体でF*N個のメッセージ処理を無くすことが可能となる。

3) スイッチ側では、監視対象通信フローのトラヒックデータを周期的に収集し、指定された判定条件を満足すれば‘異常’と判定し、SDNコントローラにReplyメッセージを用いて通知する。そうでなければ次の周期で同じ判定処理を繰り返す。

4) スイッチから通知を受けたSDNコントローラは他情報と合わせ攻撃かどうか判定する。攻撃と判定したら、その通信フローに属するパケットを廃棄(drop)または攻撃分析装置へ転送するように、（送信側に最も近い）スイッチに対してModify Flow Entryメッセージを用いて指示する。

2.4 提案方式の検証

SDNコントローラとしてTrema1.0.1をベースに提案方式の評価システムを構築し、想定通り動作することを確認した。

3. 今後の課題

DDoS検出後の規制方式の詳細を明らかにする必要がある。

＜参考文献＞

[1] K,Bhushan and B.B,Gupta, “ Detecting DDoS Attack using Software Defined Network (SDN) in Cloud Computing Environment,” 5th International Conference on Signal Processing and Integrated Networks (SPIN), Feb. 2018.

[2]“OpenFlow Switch Specification v1.5.1”, ONF, Mar. 2015.

Copyright © 2020 IEICE