4T-04

SDN 環境における NFV を用いたテーブルオーバーフローの緩和の一検討

ソユル ムスタファ [†1]　ギリエ ルイス [†2]　和泉 諭 [†3]　阿部 亨 [†1,†4]　菅沼 拓夫 [†1,†4]

[†1] 東北大学大学院情報科学研究科　[†2] 東北大学電気通信研究所　[†3] 仙台高等専門学校
[†4] 東北大学サイバーサイエンスセンター

1　はじめに

ネットワークをソフトウェアで制御・管理する Software Defined Network（SDN）[1] が注目されており，その実装として OpenFlow が一般に利用されている．OpenFlow では，コントローラがスイッチに対して指示を与え，スイッチはフローテーブルに格納されているフローエントリに基づいて，トラィックを処理することで，ネットワークの柔軟な管理や制御を実現している．

一方で，ネットワークに対するサイバー攻撃が増加しており，OpenFlow に対する攻撃の一つにテーブルオーバーフロー攻撃があげられる．この攻撃では，スイッチが格納できるフローテーブルの容量の限度を突くものであり，Distributed Denial of Service (DDoS) 攻撃など様々な手段により，スイッチにフローテーブルを過度に挿入してオーバーフローさせることでネットワークを制御不能とするものである．先行研究 [2] ではフローテーブルをネットワーク上に分散させるアプローチがあるが，ネットワークトポロジに依存する課題がある．

そこで，本研究ではネットワークの機能を仮想化する Network Function Virtualization (NFV) を利用して，攻撃者を動的にフィルタリングすることにより OpenFlow におけるテーブルオーバーフロー攻撃を緩和する手法を提案する．

2　関連研究

2.1　OpenFlow でのテーブルオーバーフロー

OpenFlow において，スイッチに新規のパケットが到達するとコントローラーにパケット情報を転送する．コントローラーはそのパケットに対する処理を決定し，スイッチにフローエントリを設定する．この処理は新規のパケットが到着する毎に実行される．この時，送信元アドレスやポート番号などが異なる様々なパケットが多数届くと，それぞれのパケットを処理するためのフローエントリをスイッチに設定する必要があり，テーブルオーバーフローが起こる原因となる．

A Study on Table Overflow Mitigation in SDN using NFV
Mustafa SOYLU[†1], Luis GUILLEN[†2], Satoru IZUMI[†3], Toru ABE[†1,†4], and Takuo SUGANUMA[†1,†4]
[†1]Graduate School of Information Sciences, Tohoku University
[†2]Research Institute of Electrical Communication ,Tohoku University
[†3]National Institute of Technology, Sendai College
[†4]Cyberscience Center, Tohoku University

2.2　テーブルオーバーフロー緩和の関連研究

テーブルオーバーフローを緩和する手法は，フローテーブルの圧縮，入れ替え，分離の大きく 3 つのアプローチに分類できる [3].

フローテーブルを圧縮する手法では，新規のパケットの共通部分をまとめて，1 つの条件としてフローエントリに設定する．これで，設定するフローエントリの数を削減する．しかし，様々な種類のパケットを送信してくるボットネットによる DDoS 攻撃などにおいては圧縮率が低く，テーブルオーバーフロー攻撃の抑制につながらない課題がある．

フローテーブルを入れ替える手法では，フローエントリ数が多くなると，設定してから長時間経過したフローエントリや重要性の低いフローエントリを消去し，新しいフローエントリを設定する．しかし，正当な処理を行うフローエントリまでも消去されてしまう恐れがある．

フローテーブルを分離する手法では，フローテーブルに空きがあるスイッチにパケットを誘導し，そのスイッチで特定のフローエントリを用いて，攻撃者のパケットを防ぐ [2]．この手法では，新規のパケット毎に全てのスイッチの状態を確認し，フローテーブルに余裕があるスイッチにパケットの処理を誘導する．この手法は処理の効率や負荷がネットワークトポロジに依存する課題がある．

3　提案

本研究では，上記で述べた課題を解決するためにフローを分離するアプローチを基にしたテーブルオーバーフロー緩和手法を提案する．具体的には，NFV を用いてセットアップしたバーチャルスイッチを利用し，そこにパケットを誘導することで，フローテーブルを分離して，テーブルオーバーフローを防ぐ．

テーブルオーバーフロー攻撃はドメインの外から受けると仮定し，攻撃対象はドメインのエッジスイッチとする．エッジスイッチのフローテーブルの分離のために，パケットを誘導させるフローエントリを設定する必要がある．本研究では，ソース IP を基にフローエントリを集約する．現在，普及している OpenFlow version 1.3 では，CIDR（Classless Inter-Domain Routing）マスクだけではなく，ビットマスクも使用できる．新規のパケットを処理するフローエントリと設定済のフローエントリのそれぞれの送信元 IP のハミング距離を計算する．ハ

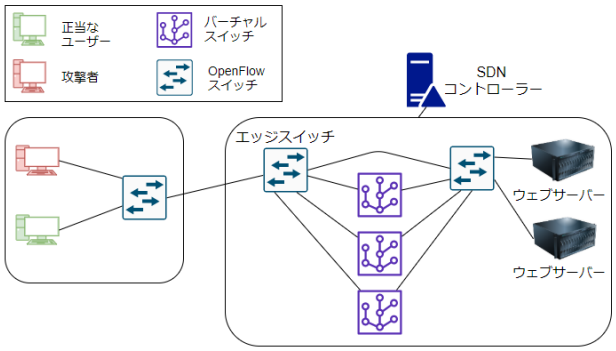

図 1: 実験のトポロジー

ミング距離は 2 つの 2 進数で，ビット数が異なる数の合計値を表す．ソース IP のマスクも計算し，ハミング距離を求める．ハミング距離は IP とマスクを 2 進数で表現したとき，例えば，0*0010*と 10*0110 のハミング距離は 2 となる．ハミング距離が閾値 ($d_{threshold}$) を超えない新規のフローエントリと既存のフローエントリをそのソース IP で融合し，エッジスイッチに設定する．上記の例の場合，融合した結果は***01**となり，３２個の７ビットのアドレスを表す．ここで，フローエントリの設定数が大きくなりすぎないように制限する．融合されたフローエントリは該当するパケットをバーチャルスイッチに誘導する．ロードバランスのため，$t_{interval}$ 毎にバーチャルスイッチの情報を求め，スイッチにあるフローエントリ数を記録し，利用率の低いスイッチを選ぶ．正当なパケットを破棄しないようにするためのフローエントリもバーチャルスイッチに設定する必要がある．なお，本研究では攻撃パケットは何らかの方法で検知され，その情報がブラックリストに保持されることを想定する．

攻撃パケットが検知されると，バーチャルスイッチにおいて，ブラックリストにあるパケットが破棄され，そうでないパケットは OpenFlow スイッチに転送され，適切な処理が行われる．

4 実験

提案手法によりテーブルオーバーフローを緩和し，フローエントリ数を削減できることを確認するためにシミュレーション実験を行った．この実験では，コントローラーとして Ryu を使用し，仮想のネットワーク環境を Mininet で構築した．実験のトポロジーを図 1 に示す．図の右側はテーブルオーバーフロー緩和の対応を行うためにバーチャルスイッチを導入したネットワークを示す．エッジスイッチには三つのバーチャルスイッチが付属している．攻撃者はネットワーク中にある 2 台のサーバを通じて，テーブルオーバーフロー攻撃を行う．提案手法を確認するために，スイッチの利用率を計測した．

図 2 に，バーチャルスイッチがある場合（提案手法）とバーチャルスイッチがない場合（単純手法）のスイッチの利用率として、フローテーブル利用率

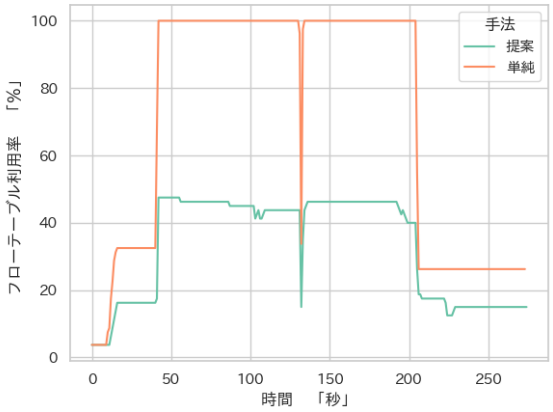

図 2: エッジスイッチの利用率

を示す．図から提案手法の方が利用率が低くなった．特に 10 から 40 秒の間は提案手法が単純手法の半分程度の利用率となったが，保持するフローエントリ数も半分程度となっていた．攻撃者が 40 秒から攻撃を開始したが，単純手法では利用率が 100% に達して，テーブルオーバーフローが発生した．一方で，提案手法は利用率を 50% 程に抑制するこができた．以上から，提案手法は単純手法が対応できないテーブルオーバーフローを緩和することが確認できた．加えて，通常時のトラフィックを制御するフローエントリ数も 50% 程度少なくなったことが確認できた．

5 おわりに

本稿では，NFV を用いてフローテーブルを分離するテーブルオーバーフロー緩和手法を検討した．実験により，スイッチのフローエントリ数を削減し，テーブルオーバーフローを緩和することができることを確認した．今後は，ネットワークや攻撃の規模を大きくした場合の対策を検討するとともに実験によりその効果を検証する．

参考文献

[1] ONF: Software-Defined Networking (SDN) Definition, , available from ⟨`https://www.opennetworking.org/sdn-definition`⟩ (accessed 2020-12-25).

[2] Bhushan, K. and Gupta, B.: Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment, *Journal of Ambient Intelligence and Humanized Computing*, Vol. 10, pp. 1985–1997 (2019).

[3] Nguyen, X., Saucez, D., Barakat, C. and Turletti, T.: Rules Placement Problem in OpenFlow Networks: A Survey, *IEEE Communications Surveys Tutorials*, Vol. 18, No. 2, pp. 1273–1286 (2016).