[Work in Progress] 研究報告

OpenFlow を用いた不正通信制御システムの評価

下川 大貴[1]　小刀稱 知哉[1]　池部 実[2]　吉田 和幸[3]

Evaluation of the attacker blocking system using the OpenFlow

1. はじめに

我々は，TCP コネクションに着目した不正通信検知システム (以下，IDS) を開発・運用してきた。IDS が検知した攻撃者の通信を OpenFlow を用いて制御する手法を提案してきた．本発表では，提案システムの運用に向けて，実環境を模倣した実験から得られた性能評価の結果を報告する．

2. 提案手法

IDS と OpenFlow コントローラが連携して，フローエントリを動的に設定し，攻撃者を遮断する．提案システムの構成および攻撃者の遮断手順を図 1 に示す。(1)IDS が攻撃者を検知，(2)OpenFlow コントローラへ攻撃者の IP アドレスを通知，(3)OpenFlow コントローラは攻撃者を Drop するフローエントリを作成，(4)OpenFlow スイッチへフローエントリを転送，(5) 攻撃者はパケットを送信，(6)OpenFlow スイッチで攻撃者が送信したパケットを破棄する．

3. 性能評価

我々はこれまでに OpenFlow 環境を構築し，擬似的に DoS や DDoS 攻撃を発生させ，本システムが攻撃者を遮断する際の他の通信への影響を検証してきた．

本稿では，図 1 に示した環境で，IDS で収集しているパケットを tcpreplay により実環境を再現した．本実験では，学外ホストから学内ホストへの ping 応答時間，iperf による UDP パケット喪失率を計測し，提案システムが攻撃者を遮断する際に，通常のトラフィックへの影響を調査した．本実験で用いたデータには，IDS で検知した約 4000 件の攻撃者を含む．これらの攻撃者を分析した結果，送信元を偽装した scan 攻撃と考えられる．図 2 より，攻撃者が 5 分間隔で約 1000 件増加し続けていた時点での ping 応答時間，UDP パケット喪失率は，図 2 の 0 時付近の平常時との差異は確認できなかった．したがって，攻撃者遮断処理が他の通信に与える影響は小さいと考えられる．

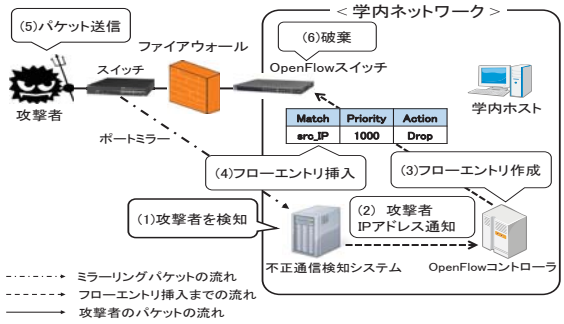

図 1　提案手法の構成図

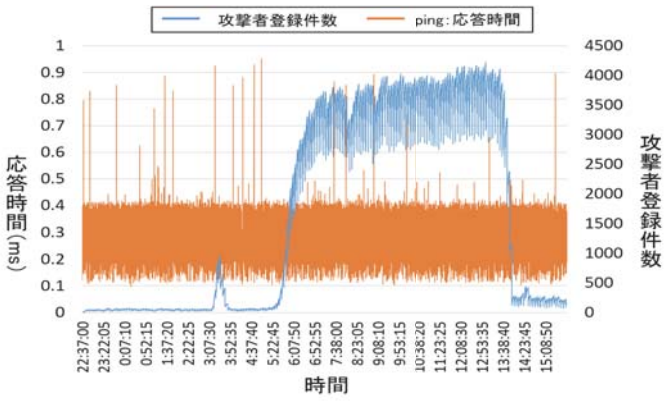

図 2　実験結果：攻撃者登録件数と ping の応答時間

4. おわりに

提案手法の実運用に向けて実環境で取得したパケットデータを用いて性能を評価した．攻撃者登録件数が急増した場合においても攻撃者登録処理が他の通信に与える影響が小さいことを確認した．今後の課題として，OpenFlow コントローラが単一障害点になっており，OpenFlow コントローラを複数台設置し，スケーラビリティに関する検証を進める．

1　大分大学大学院工学研究科知能情報システム工学専攻
2　大分大学工学部知能情報システム工学科
3　大分大学学術情報拠点情報基盤センター