3Z-4

OpenFlow を用いた未使用 IP アドレスへの通信をハニーポットに集約する方法の検討

田島　伸一[†]　太田　悟[†]　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. 研究の背景と目的

近年のインターネットの急速な普及に伴い，多くの脅威が顕在化し，その脅威のひとつにマルウェアがある．マルウェアとは，不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称である．これまで，マルウェアに対抗するためファイアウォールや IPS などの対策がとられているが，必ずしも全ての攻撃を防げるわけではない．そこで，対策をくぐり抜けた攻撃を早期に検出，解析することが重要になる．

現在，ネットワーク観測によりこのような攻撃を含むマルウェアなどの活動を調査する手法がある．その手法の中で本研究では，ハニーポットを用いた調査に注目する．その理由として，ハニーポットはマルウェアの細かい挙動の調査などのより詳細な情報の得られるからである．しかし，ハニーポットを用いた調査では，ハニーポットが監視できる範囲は自分自身への通信だけなので監視できる範囲が狭い問題がある．

したがって，本研究は，ハニーポットが監視できる範囲は自分自身への通信だけという欠点を克服することを目的とし，OpenFlow の経路制御を使い通信を集中させ，ハニーポットの監視範囲を拡大することを目指す．

2. 関連技術

2.1 ハニーポット

ハニーポットとは，クラッカーの侵入手法やマルウェアの振る舞いなどを調査・研究するためにインターネット上に設置された，わざと侵入しやすいよう設定されたサーバやネットワーク機器である．ハニーポットはサービスを提供しないため一般的なユーザから通信されず，不正な攻撃や，攻撃者からの調査のための通信のみされるという特徴がある．そのため，正常な通信を誤って不正アクセスと判断してしまうことを削減でき，未知の攻撃でもハニーポットに対するアクセスは不正であると判断することで，異常な通信を誤って正しいアクセスと判断してしまうことへの対策になるという長所がある．

しかし，ハニーポットは前述したように，自分自身への通信のみ監視し，他の通信に関与できないため監視範囲が狭いという欠点がある．もし，この欠点を解消するために複数のハニーポットを設置し，監視範囲を広げた場合，管理コストなどが増大し，ハニーポットが攻撃の踏み台にされてしまう可能性があるという新たな問題点が発生する．

2.2 OpenFlow

OpenFlow とは，現在注目されているネットワーク制御技術のことで，これまで 1 台のネットワーク機器の中に組み込まれていた，ネットワークの経路制御機能とデータ転送機能を分離し，データ転送機能を備える OpenFlow スイッチと経路制御を司る OpenFlow コントローラに分けられている[1]．それにより，柔軟かつ集中的な一元管理制御を行うことができる．従来のネットワーク制御方式は，主に IP アドレスのルーティングによって行われてきた．しかし，OpenFlow では MAC アドレスや IP アドレス，ポート番号などの L1 層から L4 層までの情報などの任意の組み合わせによって決定される一連の情報を「フロー」として定義し，そのフロー単位で処理方法を定義した「フローテーブル」で経路制御を実現する．

3. アプローチ

ハニーポットは大規模ネットワークの監視に不向きであることがわかっている[2]．そこで，本研究では，ハニーポットを学校や会社などの比較的小規模な組織で利用されることを想定する．ハニーポットの監視範囲を拡大するために，組織に割り振られている IP アドレスの特徴に注目する．その特徴とは，組織に割り振られているものの使われていない IP アドレスが存在するというものと，割り振られているものの時間帯によっては使用されていない IP アドレスが存在するというものである．本研究ではこれらの IP アドレスを未使用 IP アドレスと定義する．この特徴を利用し，未使用 IP アドレスへの通信をハニーポットに集約することで，監視範囲の拡大を行う．

4. 課題

未使用 IP アドレスへの通信の集約を行うに際し，IP アドレスの使用状況に則した経路制御を行うために対応すべきことが二つある．一つ目は，組織が利用しているネットワークの構成が変化することにより IP アドレスの使用状況が変化した場合の対応である．二つ目は，機器の動作状況の変化により IP アドレスの使用状況が変化した場合の対応である．これらに対応するために，動的な IP アドレスの使用状況を把握するシステムが必要となる．

5. 提案手法

本研究の前提として，システム管理者が，組織に割り振られている IP アドレスは把握しているものとする．組織に割り振られた各 IP アドレスの使用状況を記憶しておくリストを作成し，

A Study of how to aggregate to unused IP address communication to a honeypot using OpenFlow

Shinichi Tajima[†], Satoru Ota[†], Makoto Sato[††], Junichi Nagano[††], Norihiko Shinomiya[†] and Yoshimi Teshigawara[††]

[†]Faculty of Engineering, Soka University

[††]Graduate School of Engineering, Soka University

このリストを使い使用状況を判別していく．使用状況の変化条件は以下の通りである．

・未使用 IP アドレスから使用 IP アドレス

パケットの通信があった場合その送信元 IP アドレスを確認する．そして，その IP アドレスがリストにあるか確認し，未使用になっていた場合リストの使用状況を未使用から使用に変更する．

・使用 IP アドレスから未使用 IP アドレス

リストの使用状況が使用になっている IP アドレスから一定時間通信がない場合，その IP アドレスを使用から未使用に変更する．

この方式を利用することにより，4 章で述べた課題二つに対応できる．そして，本提案手法での経路制御方法は，パケットの通信があった場合その送信先 IP アドレスを確認し，リストとその IP アドレスを照らし合わせることにより，送信先の情報に従い送るかハニーポットに送るか判断するというものである．

このような機能を，Trema を用いて OpenFlow に組み込む．それによって出来たシステムを，Trema で仮想空間にホストとスイッチを作成し，システムを動作させて動作実験する．

6.実験

6.1 概要

本研究で提案した手法の通りにシステムが，使用状況の変化に対応してリストを変更し，リストに合わせてパケットの経路制御が正しく行われているかの動作実験を行った．本システムの実験環境の概要を図 1 に示す．その目的は，システムの正常性を計り，今後のシステムの向上のための検討に役立てていくことである．各確認方法だが，IP アドレスのリストは一定間隔でリストを表示するように作成し，それを確認し，経路制御は Wireshark を用いて観測した．また，今回の実験で使うシステムはプロトタイプとして簡単な L2 スイッチをベースに作成したものである．

6.2 実験方法

実験では，以下の送り先へネットワークと仮定したホストからパケットを送信し，通信がハニーポットと仮定したホストへ行くか送信先になっているところへ行くか，行き先を確認した．また，以下の状態を作るまでの各段階における使用状況のリストの状態を確認した．

(1)通信をしているホスト
(2)通信をしていたが通信をしなくなったホスト
(3)通信をしていたがしなくなってまた再開したホスト
(4)最初から通信をしていないホスト
(5)ホストのない IP アドレス

これにより，リストの IP アドレスが使用から未使用へ正しく変化するのかと，未使用から使用へ正しく変化するのかを確認できる．そして，その変化が正しく行われた場合，それが単一 IP

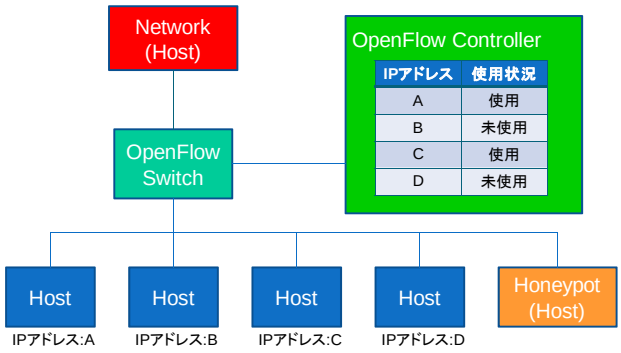

図 1　実験環境の概要

アドレスでのみ起こることではないことを確認することができる．さらに，上記に示した 5 つの状態それぞれに提案通りに送れるか確認できる．

6.3 実験結果

結果として，使用状況のリストは，実際の使用状況の通りに変化した．また，経路制御では，(1)と(3)への通信は，通常通りに送信され，(2)と(4)と(5)への通信はハニーポットと仮定したホストへ送信された．このように提案通りの正常な動作をした．

6.4 考察

今回作成したシステムにより，本提案手法によって，動的な使用状況の判別とハニーポットへの通信の集約ができることがわかった．また，理想的な動作の実現により，今後のベースとなるシステムの作成ができた．これにより，実ネットワークで利用可能なシステム作成の見通しを得た．

7. まとめと今後の課題

本研究は，ハニーポットの監視範囲の拡大のため，OpenFlow を用いた経路制御により未使用 IP アドレスへの通信を集める方法を検討している．本稿では，そのためのプロトタイプシステムを作成し動作実験を行った．

今後は，リストの IP アドレスが使用から未使用に変わる際の時間の検討をする．また，今回は簡単な L2 スイッチをベースとしたプロトタイプだったので，実際のネットワークに導入できるようなシステムを作成する．そして，実際にハニーポットを設置，運用をし，収集率などの評価を行っていく．

参考文献

[1] OpenFlow：OpenFlow. http://www.openflow.org/
[2] IPA：情報セキュリティ技術動向調査（2008 年下期）．
http://www.ipa.go.jp/security/fy20/reports/tech1-tg/documents/tech-1-2008b005.pdf