OpenFlow スイッチによる悪意のある通信の集約

山田 建史 †　　戸部 和洋 †　　森 達哉 †‡　　後藤 滋樹 †

† 早稲田大学 基幹理工学研究科 情報理工学専攻
169-8555 東京都新宿区大久保 3-4-1
{y.kenji, tobe, tatsuya, goto}@goto.info.waseda.ac.jp

‡NTT サービスインテグレーション基盤研究所
180-8585 東京都武蔵野市緑町 3-9-11
mori.tatsuya@lab.ntt.co.jp

あらまし 本研究は，OpenFlow スイッチを用いて悪意のある通信を判別する方法を提案する．この方法は，ポート番号によるポリシルーティングのような既存手法では制御しきれない，詳細なポリシを制御して通信を選別することができる．この方法を用いてポートスキャン，IP スプーフィングのような悪意のある通信を弁別する．仮想サーバ上で既存手法との性能比較を行うと，悪意のある通信の収集率に大きな改善がみられた．またパケット処理能力は既存手法に比べて遜色ない．この提案手法をハニーポットの前段のスイッチに用いると，悪意のある通信をハニーポットに集約することができる．

Collecting Malicious Traffic with OpenFlow Switches

Kenji Yamada†　　Kazuhiro Tobe†　　Tatsuya Mori†‡　　Shigeki Goto†

†Graduate School of Fundamental Science and Engineering, Waseda University
3-4-1 Okubo, Shinjuku-ku, Tokyo 169-8555 JAPAN
{y.kenji, tobe, tatsuya, goto}@goto.info.waseda.ac.jp

‡NTT Service Integration Laboratories, NTT Corporation
3-9-11 Midori-cho, Musashino-shi, Tokyo 180-8585 JAPAN
mori.tatsuya@lab.ntt.co.jp

Abstract This paper proposes a new method of discriminating malicious traffic with OpenFlow switches. The proposed method can distinguish malicious traffic by fine-grained policies beyond the capability of traditional policy routing. It collects malicious traffic including the port scan and the IP spoofing. We compare the performance of the new method with normal policy routing. The new method attains a better result in collecting malicious traffic. It is shown that the overhead of the new method is minor. One of the applications of the new method is collecting malicious traffic at a switch and feed it to honeypot efficiently.

1　はじめに

インターネットの発展に伴って悪意のある通信による脅威が顕在化し，グローバルなサイバー攻撃が頻発している [1]．また，ボットネットを中心に多様かつ複雑な攻撃が行われている．ボットネットとは，悪意のあるソフトウェアに感染したコンピュータで構成されるネットワークである．攻撃者は，インターネットを介して

ボットネットのコンピュータを遠隔操作できる．ボットネットは，国境を越えて様々な形態のものが複数存在している．そのため，ボットネットの規模や活動内容の全容を把握することは難しい．ボットネットの対策には，広域的な観測により多様な攻撃通信を収集することが必要である．このように広域に観測を行うために分散型ハニーポット [12] が用いられている．ボットネットの攻撃活動はインターネット全体に対して多様な攻撃手法で行われる．そのため，小規模なシステムを用いて検出しようとしても，多様化した攻撃の多くを検出できない．そこで，ハニーポットを広域的に分散配置して，広範に展開しているボットネットの実態や攻撃対象を観測することが重要である．ハニーポットは，攻撃者の侵入手法やコンピュータウイルスの振る舞いなどを観測・研究するために，わざと侵入しやすいように設定されたサーバーやネットワーク機器である．

IT システムの利便性を享受しながら，悪意のある通信を防ぐことが求められている．広域通信の選別による悪意のある通信の観測や防御には，通信経路中に侵入検知システムやファイアウォールなどの機器を用いる必要がある．しかし，観測を行う範囲を広げると，設備投資によるコストが増大し，機器の運用や設定にかかる人的なコストも問題となる．これを解決するため，通信を選別して悪意のある通信を収集することを考える．具体的にはセキュリティ機能を持たせた上で一元管理できるネットワーク管理システムが必要である．分散配置された機器が協調して攻撃を防ぐ方法 [8] も考えられるが，かなりの台数の機器を一元管理できることが分かっている [9]．このような背景のもとで，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 [10] スイッチング技術が注目されている．OpenFlow はスイッチの機能を再構成，細分化して機能をスイッチ部とコントローラ部に分けることにより，柔軟かつ集中的な一元管理制御を行うことができる．本研究では，OpenFlow 規格を用いたプログラマブルフロースイッチを用いて，広域に悪意のある通信を選別し，スループットのばらつきが少なく安定した通信をハニーポットへ集約するシステムを構築することを目的とする．

2 関連研究

悪意のある通信をハニーポットで収集する研究として，[6]，[7] がある．

文献 [6] は，ポート番号を元にネットワーク管理者が定義したポリシをルータに与え，パケットの転送とルーティングにより通信を収集する手法を提案している．ポリシルータは，iptables と iproute2 で構成されている．iptables では，パケットの判別及びマーキングを行い，ポリシにマッチするパケットに関連付ける値を設定する．そして，iproute2 で関連付けられたマーク値によってパケットの転送を行う．この研究ではポリシルーティングによって通信を制御できるが，ポート番号ベースのように短調な制御となる．またポリシルータに用いている Linux が保持できるルーティングテーブルは，エントリ数に上限がある．また，エントリ数が大きくなるとルータの負荷が大きくなってしまう．そのため，制御内容が通常のルータ機能と比べて多様になったとしても，その利点を活かすのは難しい．さらにポリシルータの制御内容は，適用したルータ自身にのみ適応される．そこで広範囲の通信を制御するために複数のポリシルータを用いることになる．複数のルータのそれぞれにポリシを適応させなければならない．ポリシを変更する際にはそれぞれを変更しなければならないから，スケールアウトしないという欠点がある．このように，広範囲の通信を制御し，悪意のある通信を収集するためには効率が悪くなる．しかも，ルータの台数を増やすにしたがいコストが増大する問題がある．このように，既存技術ではポリシルーティングの機能面に加えてコスト面や効率面で問題がある．一方，本研究では，OpenFlow を用いることでコントローラのソフトウェアによって複数のスイッチを一元管理できる．これにより柔軟かつ集中的な管理制御を実現し，スケールアウトにも有効である．また，スイッチ側には制御部が必要無いため，設備投資しても低コストで台数を増やすこ

とができる．ルーティングテーブルのエントリ数の制約も受けない．

文献 [7] は，組織に割り当てられているが使われていない IP アドレスブロック (ダークネット) に対する悪意のある通信を観測している．ダークネットは，攻撃や設定ミスによるパケットが届く．この研究では，40 個の IP アドレスから構成されるダークネットを観測している．そのうち 20 個の IP アドレスに届くパケットには全く応答をせず，残りの 20 個の IP アドレスに届くパケットには低対話型ハニーポット Honeyd が応答を返すように設定している．そして，これらの IP アドレスに届くパケットをキャプチャしている．悪意のある通信がグローバル化，および多様化するインターネットでは，広域に観測を行うことが求められる．しかし，ダークネットの観測は対象を広げることが容易でない．この研究でも，ダークネット観測用の IP アドレスブロックの確保に苦労したことが文献 [7] に記されている．一方，本研究は，通信経路上の OpenFlow が通信をハニーポットに集約することで，広域なネットワークを効率良く観測できる．そのため，多様な通信の傾向を容易に調査することが可能である．

3 通信の集約法

本章では，OpenFlow スイッチを用いて広域な攻撃通信を効率的に集約する手法を提案する．

本提案手法は，OpenFlow を用いて通信をフローととらえて，コントローラが定めるポリシーに従い，悪意のある通信と判断されたフローをハニーポットへ集約することを実現する．提案手法の動作は以下の 3 ステップからなる．

1. フロー単位による通信の判別
2. コントローラ部によるポリシーの定義
3. ハニーポットによる通信の収集

ここで挙げた 3 項目を以下の本文で説明する．

3.1 フロー単位による通信の判別

3.1.1 OpenFlow におけるフローの定義

OpenFlow は，通信の開始から終了までを 1 つのフローとみなして処理を行う．OpenFlow がフローを認識する基準は，スイッチの入力ポート及びパケットのヘッダに含まれるレイヤ 4 までのパラメータ[1]の任意の組み合わせである．例えば，同一 IP からの複数の通信でもそれぞれを一意に認識することができるため，柔軟な処理が可能である．

3.1.2 フロー単位による通信の割り振り

フローテーブルの例を図 1 に示す．本手法では，OpenFlow を用いてフロー単位の通信の割り振りを行う．ある通信に対して，フローの最初のパケットが到達したときにコントローラ部のソフトウェア処理で割り振り先を決定し，ハードウェアによるスイッチ部にフローテーブルとして定義する．フローテーブルのエントリは，Rule, Action, Stats から構成される．パケット情報にルールを適用し，そのフローに関する処理方法を定義できる．その後は定義されたフローテーブルに従いルーティング処理を行う．これによりスイッチ部の処理を高速に行うことができる．このように，OpenFlow スイッチは転送部のスイッチと制御部のコントローラが分離するのでスケールアウトする．そのため，OpenFlow スイッチを用いる本提案手法もスケールアウトし，広域に展開できる．

3.2 コントローラ部によるポリシーの定義

3.2.1 OpenFlow コントローラの動作

OpenFlow コントローラは，OpenFlow スイッチから受け取ったパケットに応じてフローを定義し，スイッチに対して返答する．1 つのコントローラから，複数の OpenFlow スイッチを制御

[1]受信したスイッチポート，送信元 MAC アドレス，宛先 MAC アドレス，VLAN のタグ ID，送信元 IP アドレス，宛先 IP アドレス，Type of Service，送信元ポート番号，宛先ポート番号，ICMP の種類

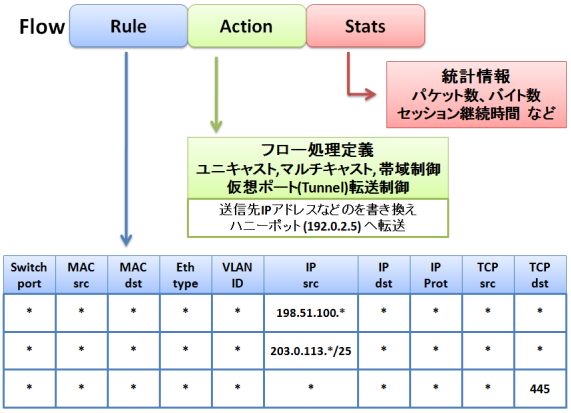

図 1: フローテーブルの例

することが可能である．そのため，OpenFlow スイッチを広域に展開しても，1 つのコントローラですべて制御できる．OpenFlow コントローラは，OpenFlow プロトコルに従ったプログラムで自由に実装することができる．ソフトウェアで制御することで，条件分岐などの複雑で柔軟な制御が可能となる．OpenFlow コントローラに自作のプログラムを組み込みための API として，NOX [11] が広く使われている．NOX は C++や Python の API を提供しており，一般に利用されているプログラミング言語で自作のプログラムを OpenFlow コントローラに組み込める．JGN2plus における広域通信の実証実験においても，NOX が使われている [3]．そこで，本研究においても NOX を使用して提案手法を OpenFlow コントローラに組み込んだ．

3.2.2 ポリシの定義

本手法では，送信元 IP アドレスとポート番号によるポリシを採用している．送信元 IP アドレスは，世界中からルータやファイアウォールのログを収集している Internet Storm Center (ISC) [13] が公開している統計結果による攻撃元 IP アドレスブラックリストを用いた．本研究では，上位 100 件を用いたが，ポリシをさらに増やすことも可能である．ポート番号は，低対話型ハニーポット Nepenthes が動作をエミュレートするポート番号 18 種類に加え，警視庁セキュリティポータルサイト@police [2] が発行するインターネット治安情勢 2010 年 7 月～9 月において報告された攻撃において，特に多く報告されたポート番号上位 20 件を用いた．これらの情報には重複があるため，合わせると 27 種類のポート番号がある．コントローラには攻撃元 IP アドレス 100 件と宛先ポート番号 27 種類を組み合わせたポリシーを持たせ，ポリシーにマッチした通信の経路をハニーポットへ振り向ける．

3.3 ハニーポットによる通信の収集

OpenFlow によって集約する通信はすべてハニーポットへ振り向ける．悪意のある通信をハニーポットへ集約することにより，ホストに必要のない通信が流れることを防ぐことができる．従来の侵入防御システムでも悪意のある通信がホストに流れることを防ぐことができる．ただし，本提案手法では悪意があると判定した通信を破棄せずにハニーポットに集約して観測することで，情報を有効に活用できる．そして，広域の通信をハニーポットに集約することで，多様な通信の傾向を容易に調査することが可能である．多様な不正通信における収集の有用性は，先行研究 [5] によって示されている．

3.4 提案手法の動作

提案手法の構成を図 2 に示す．OpenFlow スイッチに新しいフローが到着したとき，そのフローの最初のパケット情報[2]が OpenFlow コントローラに転送される．OpenFlow のコントローラ部には送信元 IP アドレスとポート番号によるポリシーを定義しており，OpenFlow コントローラはパケット情報を受け取った段階でのポリシーを参照し，宛先を決定する．宛先は以下の 2 つに分岐される．

1. ポリシーに適合した場合，宛先をハニーポットへ変更
2. 適合しなかった場合，パケット情報に従ってフローを定義

[2]パケット情報とはレイヤ 4 までのヘッダの情報及び入力スイッチポートの情報である

次に，ポリシーによる分岐から決定された宛先に基づいて OpenFlow スイッチにフローテーブルの設定を命令する．スイッチはコントローラから受け取った命令に従ってフローテーブルを設定し，パケットの転送を開始する．フローテーブルに登録された情報に合致するパケットは，以後 OpenFlow コントローラに問い合わせを行わずに同じ動作を行うため，安定したパケット処理が行われる．一方で，フローテーブルに登録された情報に合致しない新しいフローのパケットが到着したならば，新規の通信として OpenFlow コントローラに転送される．

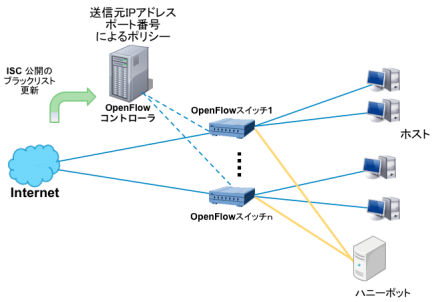

図 2: 提案手法の構成

4 性能評価

4.1 悪意のある通信の集約における優位性評価

実ネットワークに近い環境で悪意のある通信を収集するために，本実験では，hping3 と iperf を用いて，悪意のある通信と正常な通信が混在する通信を再現した．hping3 は，icmp プロトコルで動作する ping ライクなコマンドである．パラメータを設定することで多種様々なパケットの生成が可能である．本実験では，ポートスキャンと IP スプーフィングによる送信元 IP アドレスの変更を行ったパケットを生成し，悪意のある通信をエミュレートする．iperf はトラフィックを発生してネットワークのスループットを測定するツールである．本実験では，iperf によるトラフィックを正常な通信とみなした．既存手法 [6] と提案手法の通信において，集約できた通信を確認して集約率を比較する．ここで，集約率は悪意のある全トラフィックから，集約した通信の割合である．この割合は tcpdump によって観測されたパケットのうち hping3 と iperf によるパケットを元にして算出する．既存手法と提案手法による通信の収集率を表 1 に示す．表 1 を見ると，既存手法に比べ提案手法は集約率が 22.1 ポイント向上したことがわかる．また，既存手法ではポートスキャンのみ集約できたのに対して提案手法では IP スプーフィングによる通信も集約できることが確認された．

表 1: 悪意のある通信の収集率

手法	収集率 (%)
既存手法	10.4
提案手法	32.5

4.2 スループットの性能比較

OpenFlow スイッチは制御部をコントローラとして分離したことで，フローの最初のパケット処理や以後のパケット情報の書き換えによる遅延が生じる [4]．一方で，一度フローテーブルに登録した通信については，ハードウェア処理によってスループットが安定した通信を行うことができる．そこで、提案手法が既存手法 [6] に対して遜色ないスループットが出て，スループットのばらつきが少なく動作することを示す．本実験では，iperf によってトラフィックの負荷を変化させてスループットの測定を行う．ルータ内で処理を行うポリシルータに対して，OpenFlow コントローラに問い合わせを行う OpenFlow スイッチのスループットを比較する．iperf を動作させた直後では通信が不安定なため，通信が安定してから測定している．また，測定中にトラフィック量を変化させ通信が集中する状態を再現した．既存手法と提案手法における平均スループットの測定結果を図 3 に示す．また，既存手法と提案手法それぞれの，測定時間全体におけるスループットの平均と分散を表 2 に示す．図 3 を見ると，提案手法は既存手法のスループッ

トと遜色ないことが分かる．これは OpenFlow がフローの最初のパケットについてのみ処理し，以後のパケットは書き換え処理が行われているためである [4]．さらに，表 2 を見ると，提案手法は既存手法に比べ，スループットの分散が少ない安定的な通信が行われている．これにより，提案手法は悪意のある通信が集中しネットワークに負荷がかかってもスループットの低下が防ぐことができた．これは通信が OpenFlow スイッチのフローテーブルに登録されれば，それ以降はコントローラに問い合わせを行わずに，ハードウェアで処理されるためである．

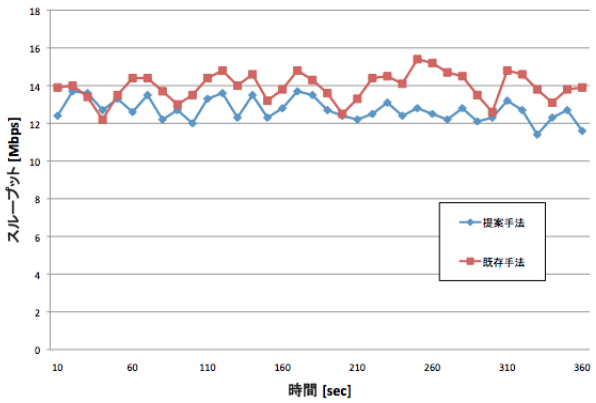

図 3: 既存手法と提案手法の平均スループット

表 2: 平均スループットと分散

手法	平均スループット (Mbps)	分散
既存手法	13.95	0.56
提案手法	12.71	0.35

5 おわりに

本研究では，OpenFlow を用いて広域な悪意のある通信を効率的に集約する手法を提案した．提案手法は広域の通信を対象として，既存手法では制御しきれないポリシを制御し，きめ細かく通信を選別することでより多くの通信を集約することを目指した．本提案手法の実用性を示すため，仮想サーバ上で実験を行った結果，集約率に大きな改善がみられた．また，スループットは既存手法と遜色なく，悪意のある通信が集中してネットワークに負荷がかかっても既存手法は安定した処理が行えることが確認できた．したがって，OpenFlow を用いた本提案手法はポリシルータによる既存手法と比べて広域通信での通信集約を能率良く行うことができること，さらに攻撃によってネットワークが高負荷なときでも安定した通信ができるという点において優れている．

謝辞 本研究において貴重なご助言を頂いた早稲田大学後藤研究室の下田晃弘氏，石井翔氏に感謝致します．

参考文献

[1] 情報処理推進機構, 情報セキュリティ白書 2010 広まる脅威・多様化する攻撃：求められる新たな情報セキュリティ対策, 初版第 1 刷, pp.6–44, 情報処理推進機構, 2010.

[2] @police, インターネット観測結果等 平成 22 年度第 2 ／四半期（7 月～9 月）, http://www.npa.go.jp/cyberpolice/detect/pdf/20101202.pdf, 2010.

[3] 金海好彦, 高島正徳, 鈴木順, ビラウォンミナイサイ, 田中仁, 太田善之, 下西英之, 岩田淳, JGN2plus 上での OpenFlow 実証実験, 2009 年電子情報通信学会総合大会, S-135, 2009.

[4] M. P. Mateo, OpenFlow Switching Performance, Masters Thesis, the Univercity Politecnico di Torino, 2009.

[5] 曽根直人, 森井昌克, ポートスキャン対策を目的としたハニーポットの提案とその応用, 電子情報通信学会技術研究報告, pp.19–24, 2006.

[6] 白畑真, 南政樹, 村井純, ポリシルーティングを用いたネットワークハニーポットの構築, 情報処理学会研究報告, 2005-DSM-38, Vol.2005, No.83, pp.55–58, 2005.

[7] 溝口誠一郎, 福島祥郎, 笠原義晃, 堀良彰, 櫻井幸一, ハニーポットとダークネットセンサーを用いた攻撃用センサーの配置, 2010 年暗号と情報セキュリティシンポジウム, 2010.

[8] Y. Ohsita, et al., Deployable Overlay Network for Defense against Distributed SYN Flood Attacks, IEICE transactions on communications, Vol.91, No.8, 2008.

[9] M. Casado, et al., Ethane: taking control of the enterprise, ACM SIGCOMM Computer Communication Review, Vol.37, No.4, pp.1–12, 2007.

[10] The OpenFlow Switch Consortium, http://www.openflowswitch.org/

[11] NOX: An OpenFlow Controller, http://noxrepo.org/

[12] leurrecom project, http://www.leurrecom.org/

[13] Internet Storm Center, http://www.dshield.org/