様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １６ 日現在

機関番号：６２６１５
研究種目：若手研究
研究期間：2019～2023
課題番号：１９Ｋ２０２５２

研究課題名（和文）ネットワーク・ホスト間の連携による省リソース型E2E経路検証機構の開発

研究課題名（英文）Development of resource-saving E2E route verification mechanism by network-host coordination

研究代表者

北川　直哉（Kitagawa, Naoya）

国立情報学研究所・学術ネットワーク研究開発センター・特任准教授

研究者番号：５０７４９９００

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：Software Defined Network（SDN）において、各スイッチやホスト、アプリケーション等から取得可能な通信量や稼働状況等の多様な情報をSDNコントローラで活用することで、End-to-Endでの経路検証機構を開発した。
また、転送状態の整合性を検証する異常検出方式では従来方式では閾値を管理者が主導で設定する必要があることに加え、ネットワーク全体で同一の閾値を使用していた。本研究ではこれを改善し、閾値の自動調整や部分的な細かい閾値設定が可能な方式を開発した。

研究成果の学術的意義や社会的意義
SDNのデータプレーン保護のために提案されている従来のバイト整合性検証手法は、検証精度がコントローラの統計情報処理能力に依存することやフロー集約に非対応である問題があった。この問題に対し本研究では、集約されたフローを分解することでより粒度の高い転送量情報を扱える方式を開発した。
また、SDNネットワークを構成する末端のSDNスイッチに接続されたホスト内にSDNスイッチと同様の転送量情報レポーティング機能を持たせることで、異常検知可能な機器の範囲を拡大させた。
さらに、異常検知に用いる閾値の自動調整や部分的な細かい閾値設定が可能な方式の開発により、検出率向上や誤検知率低下を実現した。

研究成果の概要（英文）：In this research, an end-to-end route verification mechanism was developed for Software Defined Network (SDN) by utilizing various information available from each switch, host, application, etc., such as communication volume and operating status, in the SDN controller. In addition, the conventional anomaly detection method for verifying the integrity of the forwarding state requires the administrator to manually set the threshold value, and the same threshold value is used for the entire network. In this study, we improved on this situation and developed a method that allows automatic adjustment of threshold values and detailed partial threshold settings.

研究分野：情報ネットワーク

キーワード：Software Defined Network　SDN　OpenFlow　ネットワークセキュリティ　異常検知　障害検知　データセンタセキュリティ　経路検証

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

インターネットは情報化社会において重要な役割を担っているが，情報の漏洩や改ざん等のセキュリティインシデントが後を絶たない状況が続いており，セキュリティ対策や情報そのものの信頼性の確保が急務である．現在のセキュリティ対策は，TLS（Transport Layer Security）等を用いた伝送データの暗号化による通信データの改ざんや盗聴の防止や，ファイアウォールや侵入検知システムを用いたホストへの攻撃を検出する技術を中心として展開されている．しかし，全ての通信が暗号化されているわけではなく，例えばドメイン名の名前解決に用いられるDNS(Domain Name System) では容易にデータ改ざんが可能な通信プロトコルであるUDP(User Datagram Protocol) が用いられる．DNS 通信では，DNS over HTTPS 等の暗号化に対応したプロトコルも提案されているが，普及には程遠い状況にある．さらに，インターネット通信で最も通信量の多いウェブ通信においても，Google 社の調査によると国内で暗号化されているトラフィックは全体の約 70%程度であり，完全に安全な状態であるとは言い難い．また，現在広く利用されているファイアウォールや侵入検知システム等のホストベースのセキュリティ対策では，通信が暗号化されていることによって検査不可能な悪性トラフィックや，プロトコルスタックを無視する巧妙なマルウェアの出現等により，検出不可能な攻撃が多く発生しており重要な問題となっている．

また，SDN(Software Defined Network) 等，ネットワークそのものを高機能にする技術が普及し，高機能な端末と高機能なネットワークの組み合わせという従来網の設計コンセプトをより高度化した運用ができるようになっている．学術界では，SDN を活用したファイアウォールである FlowGuard や，ホストを OpenFlow に対応させることでセキュリティポリシの適用を可能とする PBS(Programmable BYOD Security)等の多数の手法が提案されている．しかし，ルーティングテーブルの省リソース化のために SDN で広く利用されている Flow Aggregation（フロー集約とも呼ばれる）によるスイッチの省リソース化と，これらの先行研究の悪性トラフィック検出精度はトレードオフの関係にある．このような背景から，実運用化に向けて必須であるルーティングテーブルの省リソース化やパケット処理性能と，不審な通信挙動の検出精度を如何にして両立するかが問われている．

２．研究の目的

巧妙化するサイバー攻撃に対応するためにセキュリティ対策の研究がさかんに行われているが，新たな手口の攻撃を検出できない事例が多数発生しており，重大な問題となっている．従来のセキュリティ対策は，ネットワークに接続されるホストに対する対策と，ネットワーク内部での対策が分離して実施されている．また，攻撃の検出に使用するためのデータ解析や学習に活用可能な情報もそれぞれ独立しているため，通信経路全体を対象とした検証は実現されておらず，検出不可能な攻撃が増加しつつある．

本研究では，ホストやアプリケーションで取得可能な通信量や稼働状況等の多様な情報 を SDN コントローラで活用可能にすることで，従来手法では実現できなかった End-to-End での経路検証機構を開発する．また，SDN スイッチの省リソース化を目的として一般的に行われている Flow Aggregation を，ホストから得られる情報の活用によって分解し，フローレベルでの解析 を可能にすることで，実運用環境にも適用可能な，高精度かつ低負荷な経路検証基盤を実現する．

３．研究の方法

本研究は，従来のネットワークセキュリティでそれぞれ独立していた，ネットワークに接続された ホストの保護と，ネットワーク自体の保護を，ホストからの情報と SDN コントローラとの連携に よって包括的に実現するために，(A)ホスト情報の活用による End-to-End の経路検証機構の実現，(B)ホスト情報の活用による Flow Aggregation の分解とフローレベル解析の実現の 2 点を達成した．

(A) では，ホストにおけるトラフィック量のほか，動作中のアプリケーションから収集できる多様な情報の収集によって，ネットワークレベルでの保護を可能とする経路検証機構を実現した．

(B)では，従来のネットワーク検証手法で対応されていなかった Flow Aggregation 化された状態において，多様なホスト情報の活用によってそれを分解することで，フローレベルでの解析を実現した．

本研究では，(A)および(B)の実現に向けて，(1)ホスト情報とネットワークレベル情報の組合

せ方式の開発，(2)Flow Aggregation 分解方式の開発およびフローレベルでの解析方式の開発，(3)通信先ホスト特定方式の開発およびホスト間での検証の実現と評価，の 3 つのフェーズに分け， 方式の開発から実運用に向けた実装・評価までを包括的に実施した．

本研究により，図 1 に示すように通信経路上のスイッチ間のみで検証可能だった従来手法の制限を脱却し，エンドホストを含めたネットワーク全体での検証を実現することで，これまでは不可能だった End-to-End のネットワーク経路の検証を可能とし，ネットワーク全体を対象とした検証基盤を開発した．統計値の取得等の操作はフローテーブルのサイズに比例して取得に必要な時間が増大するが，本研究で開発する Flow Aggregation の分解によるフロー別処理の実現により情報取得に要する時間を抑制できるほか，フローエントリの増大によるスイッチの消費リソースを大幅に削減し，従来の研究で成し得なかった実運用環境でも適用可能な方式の開発を実現した．

４．研究成果

Software Defined Network（SDN）において、各スイッチやホスト，アプリケーション等から取得可能な通信量や稼働状況等の多様な情報を SDN コントローラで活用することで，End-to-End での経路検証機構を開発した．

また，転送状態の整合性を検証する異常検出方式では従来方式では閾値を管理者が主導で設定する必要があることに加え、ネットワーク全体で同一の閾値を使用していた．本研究ではこれを改善し，閾値の自動調整や部分的な細かい閾値設定が可能な方式を開発した．

これらの成果をまとめ，下記の論文誌，国際会議，国内研究会にて成果発表を行なった．

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Shimizu Takahiro、Kitagawa Naoya、Ohshima Kohta、Yamai Nariyoshi	４．巻 7
２．論文標題 WhiteRabbit: Scalable Software-Defined Network Data-Plane Verification Method Through Time Scheduling	５．発行年 2019年
３．雑誌名 IEEE Access	６．最初と最後の頁 97296～97306
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2929958	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計5件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 佐藤純平，森山直樹，清水貴弘，大島浩太，北川直哉
２．発表標題 SDNにおける任意ノード間の動的閾値調整機能を備えたバイト整合性検証方式の提案
３．学会等名 電子情報通信学会ネットワークシステム研究会
４．発表年 2023年

１．発表者名 森山直樹，天野友樹，清水貴弘，大島浩太，北川直哉
２．発表標題 SDN上の各ホストにおけるプロセス毎の通信量監視によるデータプレーン異常検知
３．学会等名 電子情報通信学会 インターネットアーキテクチャ研究会
４．発表年 2022年

１．発表者名 天野友貴，清水貴弘，北川直哉，大島浩太
２．発表標題 End-to-Endの転送量情報を用いたSDNデータプレーン検証手法の提案
３．学会等名 電子情報通信学会 ネットワークシステム研究会
４．発表年 2021年

１．発表者名 清水 貴弘，北川 直哉，山井 成良
２．発表標題 SDNデータプレーン検証のためのフロー分解による転送量情報の推定手法
３．学会等名 電子情報通信学会 情報ネットワーク研究会
４．発表年 2020年

１．発表者名 Naoya Kitagawa, Naoki Moriyama, Kohta Ohshima
２．発表標題 Anomaly Detection by Monitoring Communication Volume at the Process Level of Each Host in SDN
３．学会等名 Twentieth International Conference on Networking and Services (ICNS 2024)（国際学会）
４．発表年 2024年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関