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

平成　３０　年　　６　月　１９　日現在

機関番号：　３２６７５
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００１３８

研究課題名（和文）マルチスケールSDNのための制御ソフトウェアの基礎研究

研究課題名（英文）Design and Implementation of System Management Software for Multi-scale SDN

研究代表者
廣津　登志夫（HIROTSU, Toshio）

法政大学・情報科学部・教授

研究者番号：１０３７８２６８

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：本研究では、現在、主に単一のサービス基盤の制御に使われているSDN技術を、複数の利用者ネットワークが重畳するマルチテナント環境や大規模なネットワーク等の多様なレベル（マルチスケール）のサービス基盤の管理・運用に適用可能とすることを目指している。
具体的には、各テナントがSDN技術で制御するデータセンタ・クラウドのネットワークをSDN基盤上に効率的に重畳させる技術や、大規模ネットワークの柔軟な制御機構としてSDN技術によるサイバー攻撃対処の機構を実現した。本研究の成果により、これまで管理レベルの技術であったSDNによる柔軟な制御の恩恵をユーザレベルネットワークもが受けることができるようになる。

研究成果の概要（英文）：SDN technologies are commonly used to manage a single specific service platform. In this research, we aim to apply the SDN technologies to multi-scale network, that means multiple level networks such as multi-tenant data center network, large-scale wide area network or small edge networks.
One of the result of our research enables multiple tenant (user) networks are co-located on the top of the SDN platform managed by a data center provider or a cloud service provider with controlling their tenant network using SDN technology. Another result helps to manage large-scale network efficiently using SDN technology. It works to defend the large-scale network against the cyber-attacks, and also enables to balance the load of the control network of SDN.
The contribution of our research will benefit each tenant of the SDN platform to control their own network in flexible using the SDN technology which were mainly used under the management level.

研究分野：　分散システム

キーワード：　SDN　OpenFlow　マルチテナント　セキュリティ　DDoS

１．研究開始当初の背景

TCP/IP に代表されるインターネット技術が急速に拡大した一つの要因は、その単純な制御の仕組みにある。通信経路の制御はネットワークアドレスの広報をベースとした緩い情報交換により実現され、データ配送においては各通信フローに対する詳細な制御を行わず、送信する情報を分割したパケットを単位として性能上限の範囲内(best-effort)で転送を行う。これにより、キャリアネットワークで行われていたような時分割通信スロットの予約に基づく非常に高精細な制御に比べて、格段に安価にネットワークサービスを実現することが可能となった。Web やメールといった当初の主たるアプリケーションのトラフィック特性を考えると、高機能化よりも単純な帯域拡大で十分なサービスレベルを提供することが可能であったという側面もあった。

このように、これまでのインターネットは疎に結合されたノード間での通信が主体でその到達性(Reachability)の確保に重点があった。しかし、現在ではその接続構成も利用形態も大きく変わってきており、通信の制御やサービス品質に対する要求が多様化している。例えば、VLAN や VPN のようにネットワーク上に仮想的に複数のネットワークを構築したり、データセンタのような非常に稠密かつ高負荷なネットワークで使用したり、また、動画像のストリーミングや周期的かつバースト性の高いセンシングストリームの集約に使われたりといったことが上げられる。つまり、今後のネットワークにおいてはネットワーク自体の制御可能性(Controllability)が重要になっていることを意味している。

ネットワークに対する制御可能性を高めるために、IP ネットワークでの RSVP や Diffserv といった資源管理の枠組みや、キャリアネットワークにおける ATM (Asynchronous Transfer Mode)のような技術が開発されてきた。しかし、これらの技術は互換性・ポリシ・コストなどの理由で、どれも広く使われるには至らなかった。これに対して、インターネット技術を一から作り直す Clean Slate と呼ばれるアプローチでは、ネットワークの制御プレーンを独立させ、ユーザ側の要求に応えうるネットワークを構築する SDN(Software Defined Network)という技術が登場した。OpenFlow はこの SDN の中核技術で、データセンタなどの集約型の大規模ネットワークで既に利用されており、組織の基盤ネットワークへの活用も始まっている。

また、ファイアウォールや IDS, NAT, VPN 等のネットワークに対する各種付加・制御機能(NF: Network Function)を汎用の仮想化基盤上で実現し、SDN により適切に経路を繋ぐこと(Chaining)で多様なネットワークの機能を柔軟に制御する NFV(Network Function Virtualization)の技術もひろまりつつある。

しかし、この OpenFlow は制御用のネットワークを用意しそこから制御することが必要になるために、これまでは主に単一組織や特定事業者内の運用レベルで使われているのが現状であった。

２．研究の目的

本研究では、SDN 技術の提供する高度な制御機能を、データセンタやクラウドといった複数組織で共用されている共有ネットワーク基盤や、大規模なネットワーク基盤に適用するための技術の研究開発を行う。ここでは、現在主に SDN 技術による制御が使われている特定エリアの単一組織ネットワークに対して、本研究の対象とするネットワークをマルチスケール SDN と呼ぶ。ここでいうマルチスケール性の意味するところは、家庭用ルータや組織内の L3 スイッチ単体のアーキテクチャの置き換えから、広域で大規模なネットワークの柔軟な制御、複数の利用者ネットワークが重畳するマルチテナント環境までのあらゆるレベルに SDN 技術を適用可能にすることを意図している。

３．研究の方法

マルチスケール性への対応を考えると、研究の方向性としては、複数の異なるレベルでの SDN 技術の併用という方向と、SDN 制御基盤の規模拡大性という方向の二つが考えられた。そこで、「SDN の上で複数の SDN を制御する階層構造」と「大規模ネットワークを想定した高機能制御」との二つの分野について、それぞれ問題を設定して研究を展開した。具体的には、

(1) SDN により制御されるネットワークを SDN 基盤上に実現する SDN マルチテナント技術
(2) モバイルクラウド環境のような大規模なネットワークを対象とした SDN ベースの DDoS 対策技術
(3) 大規模 SDN の制御基盤を想定した制御ネットワークの透過的スケーリング技術

の研究を行った。

４．研究成果

(1) SDN マルチテナント技術

近年のサーバ仮想化技術の発展により、既存の IT 基盤をデータセンタ上で仮想化して提供するクラウドサービスの普及が進んでいる。こうしたサービスを提供しているマルチテナント型データセンタやクラウドでは SDN の中核技術である OpenFlow 技術を用いて、その提供する仮想化や集中制御の機能を活用し多数のテナント向けネットワークを提供している。そこで，テナント毎に自由なネットワーク設計を可能とする OpenFlow ネットワークの仮想化技術の研究を行った。

そのような環境で、OpenFlow 技術による柔軟な制御をテナント側でも利用することを考えると、テナントレベルの OpenFlow による制御とデータセンタ・クラウド事業者レベルでの OpenFlow による制御が競合し、その利用に

一定の制約がかかる。これは、それぞれのテナントが個々のポリシに従ってネットワークのスイッチや NFV の間の通信を制御しようとするため、その制御エントリが干渉する可能性があるからである。また、データセンタ・クラウド事業者が各テナントのために用意しているネットワーク機器は多数かつ複雑な構成であり、それをそのまま各テナントが制御するのは難しい。

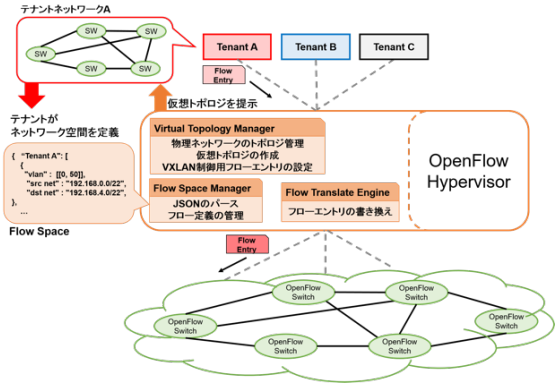

図 1　提案する OpenFlow 仮想化システム

以上の観点から、マルチテナント環境における OpenFlow ネットワークの仮想化基盤の実現に向けて、各テナントのアドレス空間の衝突管理と仮想トポロジの構築手法による SDN 仮想化基盤(図 1)を提案した。この基盤では、物理ネットワークのトポロジを適切に隠蔽した上でテナントが必要とする規模の仮想トポロジに抽象化して提示する。

仮想トポロジは、物理トポロジから部分的な木を抽出しその組み合わせで構成する。手順としては、管理対象のネットワーク外へのゲートウェイと利用するエッジスイッチ(自テナントのノードが収容されるスイッチ)で最短経路法により部分トポロジを取り出す。この操作を繰り返し行い、エッジ間の最短経路と組み合わせて仮想トポロジのエッジを決定する。この候補パスに対して VXLAN や MPLS で仮想リンクを構成して、最適パスや冗長性などのトポロジの特徴はある程度維持しつつ、テナントに対して操作しやすい仮想トポロジを実現した。

この仮想トポロジのスイッチに対して各テナントのコントローラはそれぞれ独自のポリシで制御を行う。ここで、各テナントが自由にネットワークを設計・制御するとアドレス空間や設定するフローエントリに競合が発生する。そこで、コントローラとスイッチの間で稼働するスイッチハイパバイザが調停を行い、競合を解消する。具体的には、各テナントが使用するネットワークの仕様(フロースペース)を受けてその競合部分を検出し、競合するフローエントリについては適切な書き換えを行う。これにより各テナントは他のテナントのネットワーク構成を気にすることなく自組織のネットワークをデータセンタ・クラウド上に構築することができる。

本技術により、各テナントネットワークが自由に自組織の使用するネットワークを設計し、OpenFlow により使途や目的に応じた柔軟な制御を行う事ができるようになる。既存研究の FlowVisor を用いると、各テナントが使用するネットワークの空間に重なりがないことが前提であったため、テストベッドのようなトップダウンに利用環境を規定できる場合は良いが、テナントの自由な制御やミスによる思わぬフローエントリの設定に対しては対処できなかった。本技術は、OpenFlow の技術を複数の管理レベルで自由に使えるようにするものであり、SDN 技術のより広範な応用に役立つ。

(2) SDN ベース DDoS 対策技術

大規模なネットワークに対する高機能な制御技術のためには、スイッチ上で発生するイベントに対応したパケットインからの一連の処理をコントローラで高性能に処理する必要性がある。現在は、OpenFlow の利用局面がシステムの一括管理・運用であることから、パケットインのオーバヘッドを考慮してそのようなリアクティブな処理は回避される傾向にあるが、SDN 本来の柔軟な処理のためには実際の通信に反応するような処理は重要になってくる。そこで、従来の OpenFlow の拡張レベルでの処理の高性能化を行うと同時に、コントローラ側の高性能化に取り組んだ。

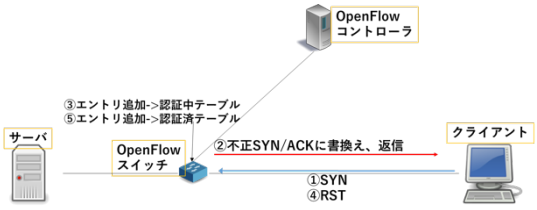

図 2　OpenFlow による DDoS 防御の実現

高性能化の実例としては、インターネットが重要な社会基盤になる中で問題となっているサイバー攻撃のうち、標的となるサーバ等に大量のパケットを送ることでサービスを機能停止状態にする DDoS(Distributed Denial of Service) 攻撃、特に TCP のセッション起動のメッセージである TCP SYN を多量に送ることでサーバのサービス不能を引き起こす TCP SYN Flood 攻撃への対処を対象とした。本研究では、TCP SYN Authentication という既存のプロトコルレベルの対処手順を OpenFlow により実現した(図 2)。TCP SYN Authentication はクライアントから到達する TCP SYN パケットに対して不正な ACK を返すことで、TCP セッション情報を維持せずに TCP SYN の再送を行わない DDoS 攻撃者を排除する手法であるが、これを OpenFlow で実現するとその状態遷移の度にパケットインが発生する。しかし、その状態遷移の一部を OpenFlow1.5 で導入された COPY 機能を用いてスイッチ上で処理することで、高速化が可能となった。具体的には、OpenFlow1.3 以前の機能で実現すると、27000pps の負荷に対して 1.5 秒くらい

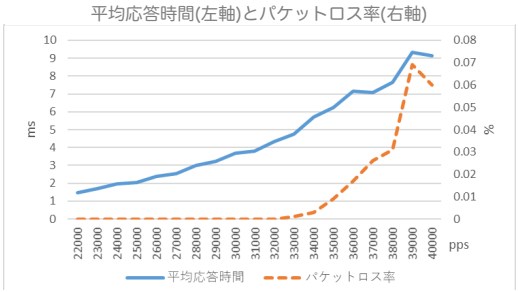

図 3　OpenFlow1.5 による処理性能

の遅延が見られ、パケットロスも発生し始めるが、スイッチ上に処理を移すと同じ負荷に対して 2.5 ミリ秒程度の遅延でパケットロスも全く発生しない(図 3)。この結果は DDoS 攻撃を スイッチレベルで対処できる可能性を示すもので、今後はモバイルクラウド環境のように多数の端末が クラウドと連携するような環境で、中継ネットワーク内で薄く広く防御することが考えられる。

OpenFlow スイッチの処理の高機能化については P4 や Flare ではスイッチ自体での言語処理を可能にしている。本研究の結果から、比較的記述しやすいスイッチの状態遷移レベルでも、ある程度高機能な処理は実現可能であると考えられる。また、従来の OpenFlow による制御機能による状態遷移処理をスイッチ上に移すことにより、十分な性能が得られる可能性が高いことも明らかになった。

(3) 制御ネットワークの透過的スケーリング技術

大規模なネットワークの制御についてのもう一つのアプローチとして、制御ネットワーク自体の高性能化の研究にも取り組んだ。前述のように、OpenFlow の制御ネットワーク(C プレーン)の処理性能の低下はデータネットワーク(D プレーン)の遅延を引き起こす。そこで、OpenFlow のコントローラの数を変更してスケーリングする技術や、それらの切り替え等の処理をスクリプト化して記述する記述言語を開発した。

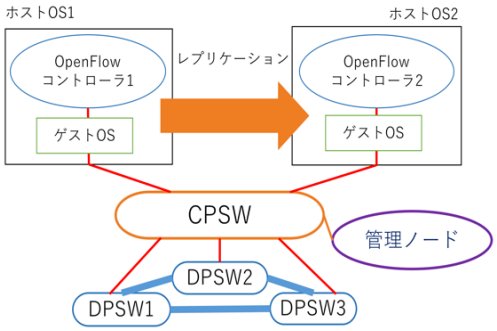

図 4　制御ネットワークの透過的スケーリング機構

OpenFlow の制御ネットワークは、スイッチが起動時にコントローラに対して TCP 接続(OpenFlow チャネル)を確立することで構成される。そのため、制御ネットワークのスケーリングのためには、TCP の状態を維持したまで

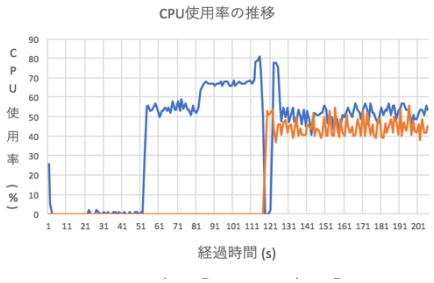

図 5　動的スケーリングの効果

スイッチ側から見て透過的に負荷を分散する必要がある。そこで、コントローラは KVM の仮想化を用いて仮想マシン内に稼働させ、スケーリングの際には KVM の複製によりコントローラ数を増やす。その際、TCP のセッションは維持する必要があるので、制御ネットワーク自体を OpenFlow で制御し、TCP のセッション単位で負荷分散させる仕組みを実現した(図 4)。ここで制御ネットワークを構成する OpenFlow スイッチの制御プログラムや KVM による仮想化基盤は REST API で操作可能として管理ノードから一括操作できるようにした。

実際に、複数のデータネットワークのスイッチ上で多量のパケットインを発生させ負荷の分散を行う実験をしたところ、制御ネットワークに異常を起こすことなくスケーリングにより負荷が分散することが確認された(図 5)。さらに、システムの管理・運用を記述する構成管理記述言語である Chef を拡張して、状態の推移や障害回復性の機能を実現した。これらの技術は、今後、制御ネットワーク自体の負荷平準化やサービス起動・停止について自動化を行う際の基盤技術となる。

5．主な発表論文等

〔雑誌論文〕(計 1 件)

① S. Higuchi, T. Hirotsu, Design and Implementation of Verification Based OpenFlow Hypervisor for Multi-Tenant Virtualized Network, International Journal on Advances in Networks and Services (Netserv), 査読有, Vol. 10, 2017, pp. 152-159, http://www.iariajournals.org/networks_and_services/tocv10n34.html

〔学会発表〕(計 19 件)

① R. Nagai, W. Kurihara, S. Higuchi, T. Hirotsu, Design and Implementation of an OpenFlow-based TCP SYN Flood Mitigation, The 6th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (IEEE Mobile Cloud 2018), 2018

② 樋口 俊、廣津 登志夫、マルチテナント型 SDN 仮想化基盤のためのネットワーク抽象化手法、情報処理学会システムソフトウェアとオペレーティング・システム研究会

(OS)、2018
③ 漆田 瑞樹、廣津 登志夫、NUMA 上の Docker コンテナスケジューリングにおけるメモリマイグレーションの改善、情報処理学会システムソフトウェアとオペレーティング・システム研究会(OS)、2018
④ 栗原 航、廣津 登志夫、樋口 俊、OpenFlow1.5 による DDoS 緩和システムの設計と実装、情報処理学会第 80 回全国大会(学生奨励賞受賞)、2018
⑤ 丸古 凌介、尾花 賢、藤田 悟、独立したグループで割り当てを行うマッチングメカニズムの提案、情報処理学会第 80 回全国大会(学生奨励賞受賞)、2018
⑥ S. Higuchi, T. Hirotsu, Design and Implementation of Virtual Topology Management for Multi-tenant OpenFlow Hypervisor, The 2017 International Symposium on Cloud Computing and Data Centers (CSCI-ISCC), 2017
⑦ 樋口 俊、廣津 登志夫、フロースペース管理による SDN 仮想化基盤の提案、情報処理学会システムソフトウェアとオペレーティング・システム研究会(OS)、2017
⑧ S. Higuchi, T. Hirotsu, A Verification Based Flow Space Management Scheme for Multi-Tenant Virtualized Network, The 11th International Conference on Digital Society and eGovernments(ICDS 2017), 2017
⑨ 永井 亮祐、廣津 登志夫、TCP SYN Authentication の OpenFlow による実現、情報処理学会第 79 回全国大会、2017
⑩ 大野 智裕、廣津 登志夫、レプリケーションによる OpenFlow コントローラの透過的切り替え手法、情報処理学会第 79 回全国大会(学生奨励賞受賞)、2017
⑪ 樋口 俊、廣津 登志夫、マルチテナント向け OpenFlow ハイパーバイザのためのフローエントリ検証手法の検討、情報処理学会コンピュータシステムシンポジウム(ComSys2016)、2016
⑫ S. Fujita, Y. Kase, Service Market Simulation based on Service-Dominant Logic, IEEE International Conference on Agents(IEEE ICA 2016), 2016
⑬ 岡部 誠人、廣津 登志夫、シミュレーションによる NETCONF 検証環境の設計と実装、情報処理学会第78回全国大会(学生奨励賞受賞)、2016
⑭ 青山 真也、廣津 登志夫、ChefScript: ログベースの障害回復性を備えた運用ワークフロー記述言語、情報処理学会システムソフトウェアとオペレーティング・システム研究会(OS)、2015

〔その他〕
ホームページ等
https://hirotsu.cis.k.hosei.ac.jp/

６．研究組織

(1)研究代表者
廣津　登志夫（HIROTSU, Toshio）
法政大学・情報科学部・教授
研究者番号：10378268

(2)研究分担者
藤田　悟（FUJITA, Satoru）
法政大学・情報科学部・教授
研究者番号：40513776

(3)連携研究者
菅原　俊治（SUGAWARA, Toshiharu）
早稲田大学・理工学術院・教授
研究者番号：70396133

福田　健介（FUKUDA, Kensuke）
国立情報学研究所・アーキテクチャ科学研究系・准教授
研究者番号：90435503