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　２５　日現在

機関番号：　２４４０２
研究種目：　基盤研究(B)（一般）
研究期間：　2015～2017
課題番号：　１５Ｈ０２６９４

研究課題名（和文）ビヘイビア指向ネットワーク制御を具現化するアジャイルポリシフレームワーク

研究課題名（英文）A Study on Agile Policy Framework for Behavior-driven Network Control

研究代表者

阿多　信吾（Ata, Shingo）

大阪市立大学・大学院工学研究科・教授

研究者番号：３０３２６２５１

交付決定額（研究期間全体）：（直接経費）　　12,600,000円

研究成果の概要（和文）：本研究では、ユーザ・端末・ネットワークの「挙動（ビヘイビア）」に着目し、新しいビヘイビア指向ネットワーク制御を提唱する。本制御では、さまざまな個別アプリケーションの組み合わせにより提供されている現在および将来のサービス・システムにおいて、個別アプリケーションではなくそれらを駆動させている挙動全体の観点から高い QoE（Quality of Experience）を提供するだけでなく、セキュリティと品質制御を統合的に扱うことが可能である。本研究ではその実現のため、アジャイルなポリシ管理運用を実現する、新しいポリシ管理フレームワークの構築と、その要素技術の研究開発を行う。

研究成果の概要（英文）：In this study, focus on behavior of users, terminals and networks, and propose an architecture of agile policy framework to achieve behavior-driven network control. This framework considers a "behavior", which is represented by a set of traffic flows, and provide a policy management scheme to satisfy overall Quality of Experience, and efficient protection agains various types of security. This framework aims agile policy management by establishing PDCA (Plan-Do-Check-Ack) cycle in network operations. A proof-of-concept model is also designed and developed.

研究分野：　情報ネットワーク

キーワード：　ネットワーク　運用管理　ビヘイビア　トラヒック分析　ポリシー

１．研究開始当初の背景

いまやネットワークは情報システムの社会基盤インフラとして必要不可欠な技術であり、そこではネットワークにより相互接続されたシステム・アプリケーションの複合によりシームレスなサービスが提供されていることは少なくない。例えば代表的 SNS である Facebook では、あらゆるサイトの情報が貼付可能であり、それらが複合された状態でユーザに示される。またクラウド型アプリケーション（Google Apps, Office 365 など）やマーケットストア（Google Play, iTunes）などにおいても、大量の TCP フローを生成させて即応性を確保するなどの工夫がなされている。さらにスマートフォン端末などでは、操作中のアプリケーションのみならずバックグラウンドでさまざまな情報同期のための通信が発生している。このように現在では、各端末が単一あるいは少数の通信フローを生成している事象は極めて少なく、むしろ常に大量の通信セッションが同時に活性化され、複合されたトラヒックが生成されていることが珍しくない。

一方トラヒック制御の観点から現状を鑑みると、依然として旧来のベストエフォート型、あるいはフローベース制御による QoS (≠ QoE) の向上に注力されている。近年研究開発が著しい SDN/OpenFlow においても、その制御主体はフローである。最終的にフローベース制御であることに異を唱えないが、大量のフローが常に生成されている現状においてユーザが体感する QoE を向上させるためには、個別フローの用途にもとづく画一的な品質制御では極めて不十分である。例えば Facebook においてユーザが注視していない動画に対し、単に動画という理由でトラヒック制御を行っても QoE の向上には何ら資さない。端末から生成される多量のトラヒックフローについて、ユーザの挙動由来であるフローを明確化し、挙動に応じた制御ポリシの設計、適用、検証する必要があるが、それらを主体的に捉えた研究は現時点ではほとんど存在しない。

２．研究の目的

本研究では以上の背景のもと、ネットワーク制御の単位について、個別フローではなくそれを生成する挙動（ビヘイビア）を主体的に捉え、ビヘイビアにもとづいた主フローの明確化、集約化とそれにもとづく制御を実現する、ビヘイビア指向ネットワーク制御を新たに提唱する。ユーザのビヘイビアは時々刻々と変化するだけでなく、ビヘイビアにより生成されるトラヒックは複数のアプリケーションから構成されることから、ビヘイビアに対するトラヒック制御の指針（ポリシ）も個別ポリシの複合により構成されることにな

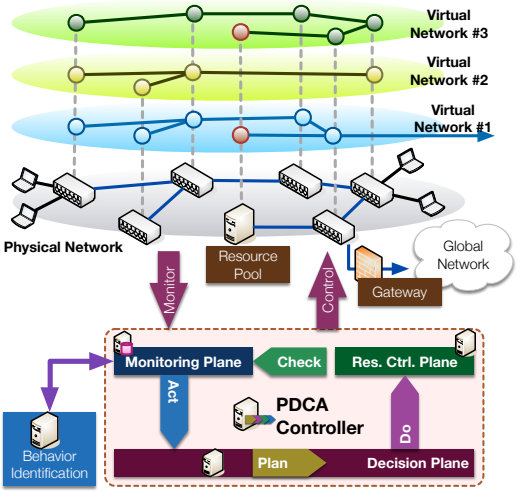

図１　アジャイルポリシフレームワーク概要

る。したがってビヘイビア制御を実現するためには、静的なポリシ制御では不十分であり、複数のポリシを動的に合成、適用、検証、制御するための統一的なフレームワークが必要となる。本研究では変化の著しいビヘイビアに適応的に対応するため、ポリシ制御にアジリティ（Agility）を導入する。そしてアジャイルポリシ制御を実現するために、ポリシ管理運用における PDCA（Plan-Do-Check-Act）サイクルを確立させる統一的なアジャイルポリシフレームワークの設計、実装および構築を行う。さらにビヘイビアに応じたポリシ合成方法、ポリシ決定に対するプログラマビリティの提供、複数ポリシが競合する場合のポリシ最適化手法について研究開発する。また、ビヘイビア指向ネットワーク制御の有効性を確認するため、テストベッド環境の構築と検証、実用化に向けた API の整備を行う。

３．研究の方法

図 1 に、本研究で提案するアジャイルポリシフレームワークの概要を示す。Physical Network が示すとおり、物理ネットワークとして SDN (Software Defined Network) スイッチ、ならびに Resource Pool が接続されている。Resource Pool は IDS、DPI、フィルタリング、暗号化などの仮想ネットワーク関数 (NfV: Network Function Virtualization) を提供する仮想 VM ノードである。また、物理ネットワークは Gateway を介してグローバルネットワー

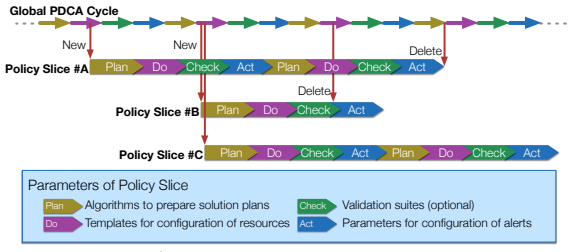

図２　ポリスライスとグローバル PDCA サイクル

クに接続されている。物理ネットワークはSDNにより複数の仮想ネットワークを動的に構築可能である。

ポリシのPDCAサイクルを確立するため、MP: Monitoring Plane、DP: Decision Plane、RCP: Resource Control Plane、PC: PDCA Controllerの4つで制御プレーンを構成する。MPはSDNスイッチ、Resource Poolおよび端末における各種情報（通信量、負荷、統計情報など）を各機器から取得し、データベースで管理する。取得した計測情報をもとにBehavior Identification機能において計測トラヒックの根拠となるビヘイビアを同定する。ただしビヘイビア同定は萌芽[A]において提案した手法を利用するため、具体的なアルゴリズムについては本研究の対象外である。DPはポリシ制御の対象となるトラヒックについて、どのような実制御を適用するかを決定する部分である。ここで実制御とは、仮想ネットワークおよびNfVの作成、削除、更新、経路変更、帯域等の資源割り当てなどを指す。DPではトラヒックおよび現在の資源の利用状況を与条件、適用したいポリシを目的関数とし、組み合わせ最適化問題を解くことで実制御のシーケンスを決定する。RCPはDPによって決定された実制御シーケンスについて、実際にSDNコントローラ、NfVコントローラに制御命令を送信することで、仮想ネットワークおよびNfVの構成を更新する。

制御プレーンにおけるPDCAサイクルの確立は、PCが行う。PCではサイクルに応じた4つのフェーズが定義、管理されている。(A) Planフェーズは MPからの制御対象トラヒックおよびビヘイビアの検出アラートにより移行され、DPにおける実制御決定処理が実行され、実制御シーケンスが生成される。(B) Doフェーズでは DPの実制御シーケンスを RCPに送信し、仮想ネットワークおよびNfVの再構成を行う。(C) Checkフェーズでは (B) において設定した制御が正しく動作しているかを一定期間モニタリングすることで検証する。ここで特筆すべき点は、(B) における再構成は即座に実トラヒックに適用されず、まず一時的に作成された仮構成によりポリシ制御後のネットワーク状態を検証し、問題が生じないと判断された場合のみ実際に移行されることである。検証に失敗した場合、Doフェーズの実制御は破棄される。(D) Act フェーズでは、引き続きポリシ制御を適正に適用するためのビヘイビア検出のためのパラメータ更新、資源の利用効率を高めるためのアルゴリズム最適化を行う。そしてPDCAサイクルの継続のため、次のPlanフェーズへの移行のためのアラートが設定される。

本研究では、制御ポリシ全体を独立した個別ポリシの合成として捉え、個別ポリシごと

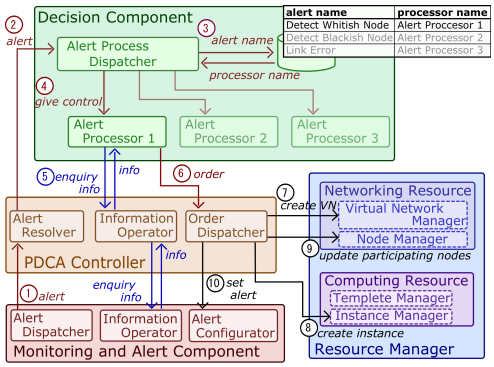

図3　動作シーケンス

にPDCAサイクルを確立させる。この個別ポリシをポリシスライスと定義する。ポリシスライスは独立したPDCAサイクルを確立可能な最小のポリシ構成を表す。ポリシスライスは、Planのための解決アルゴリズム、Doのための実制御シーケンステンプレート、Checkのための検証ツール、Actのためのアラートパラメータを入力として作成される。図2に示すとおり、新しいポリシ制御対象トラヒックが発生すると、それに対するポリシスライスが作成され、PDCAサイクルが動作する。ただし個々のポリシスライスが独立動作するとお互いが干渉するため、ポリシスライスとは別にGlobal PDCA Cycleを定義する。Global PDCA Cycleは、PCにおいてポリシスライスを制御、管理するためのPDCAサイクルである。Planフェーズにおいて新しいポリシスライスを検討し、Doフェーズでポリシスライスの作成、削除、更新を行う。さらにCheckフェーズで検証後正式運用される。またActフェーズでポリシスライスの相互干渉防止と最適化について検討し、ポリシスライスの再構成を決定する。

図3に各コンポーネント間の動作シーケンスを示す。図の通りPCは本研究におけるGlobal PDCAサイクルの管理、および各ポリシスライスのPDCAサイクルの管理を行うほか、各プレーンを駆動させるためのシグナリングを統括する。各プレーンで処理されるすべてのイベントはPCにより集中制御することで、ポリシ制御のトレーサビリティを確保する。また、シグナリングはREST (Representational State Transfer) を採用し、各コンポーネントのAPIはREST APIとして定義する。また、パラメータはJSON (JavaScript Object Notation) フォーマットにより記述する。REST APIをオープンにすることで、他コンポーネントとの連携を容易にする。

DPはPCとならび本研究における重要な機能コンポーネントであり、ポリシスライスに応じた解決アルゴリズムの実行を行う。PCからDPに対しPlanフェーズのためのAPIが駆動されると、DPはAPIに指定されたポリシス

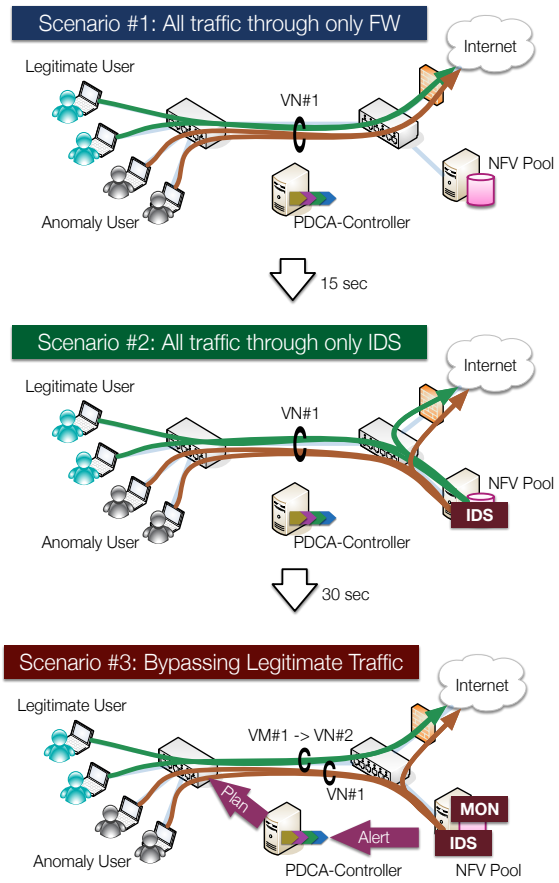

図4　実証実験のためのユースケース

ライスから、対応する解決アルゴリズムを選択して実行する。解決アルゴリズム内では、必要に応じて MP へのリソース利用状況およびトラヒック情報の取得要求を行い、最終的な実制御シーケンスを決定し、DP へ返送する。ただし実制御シーケンスはコントローラの違いによる互換性を維持するため、事前定義された抽象化リソースを用いて記述する。

次に、ユーザビヘイビア同定技術に関するリアルタイム性の向上について述べる。中継ノードにおけるインターネットトラヒックのユーザビヘイビア識別はネットワーク管理者にとって重要な技術である。しかし、従来提案されている識別手法はフローに含まれる全パケットを用いて識別を行うオフライン識別であり、ポリシーやアプリケーションにもとづいたトラヒック制御を即時に適用するためには、アプリケーション識別のリアルタイム化が必要不可欠である。

本研究では、フローに含まれる一部のパケットの情報を利用してアプリケーション識別を行うアプリケーション識別のリアルタイム化手法を提案している。まずリアルタイム識識別に悪影響を及ぼす特徴量を特定し、その特徴量を除去した時の識別精度を評価する。さらにリアルタイム性を向上させるため、複数の識別器を用いてアプリケーション識別を行う階層型アプリケーション識別手法についても提案する。

図 6 に提案する多段階階層型ビヘイビア識別の概要について示す。ここでは、識別したいビヘイビアの種類全体を複数のサブグループに分割し、サブグループごとに有効な特徴量の選定、および特徴量導出に必要となるパケット数について求める。そしてそれらを逐次的・段階的に適用しグループ分割を行うことで、最終的なビヘイビア同定を行う。

Software-Defined Network (SDN) はネットワークをデータプレーンと制御プレーンに分割し、制御プレーンを集中管理・運用することで柔軟なネットワーク管理を実現するアーキテクチャであるが、ネットワーク規模に対する制御プレーンのスケーラビリティが重要な課題となる。この課題に対応するために種々の SDN の設計手法が提案されているが、それぞれは独立した視点からの解法を提示しているため、個別課題に対する部分最適解の範疇となる。全体最適解となる設計を求めるためには、全ての設計手法を統一的に評価する枠組みが必要となる。

本研究では、上述の統一的な比較評価を目的とした、SDN アーキテクチャのモデル化手法を提案する。SDN によるネットワーク管理において、全ての設計手法に共通する基本的な機能や処理を抽象化し、機能モデルおよび処理モデルを定義する。モデル内の各要素について、処理単位の多重化や処理の同期性など、設計上のバリエーション項目を考え、提案モデルにおける構造のパラメータとして定義する。図 5 に提案する SDN の抽象化モデルを示す。

4．研究成果

本研究で提案するフレームワークの有効性を検証するため、図 4 で示す実験環境を構築す

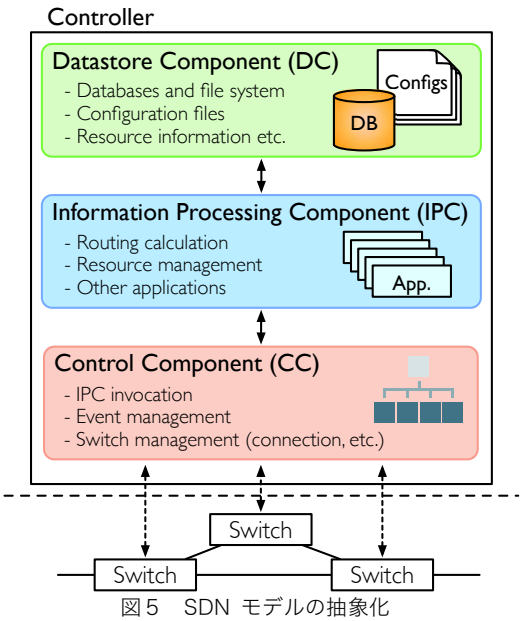

図 5　SDN モデルの抽象化

る。実験では、正常トラヒックと攻撃トラヒックを生成するユーザが混在している環境を想定 (Scenario #1) し、異常トラヒックが検出された段階で、すべてのトラヒックを IDS (Intruder Detection System) 経由で処理するようポリシスライスを生成する (Scenario #2)。しかしながら IDS は処理負荷が大きくネットワーク性能のボトルネックとなるため、明らかに正常と見なせるトラヒックを検出できればそれらについて IDS をバイパスさせることで、安全性と性能の両立を実現する (Scenario #3) ポリシスライスを生成する。以上の制御がポリシスライスの PDCA サイクルにより自律的に動作可能であることを実機により検証する。

図６に実験シナリオごとのスループットの変化（上段)、および各シナリオにおけるファイルアップロード時間の比較結果を示す。Scenario #2 において異常トラヒックが発生すると、スループットが大幅に低下した結果ファイルアップロード時間の急激な増大が観測されたが、Scenario #3 において正常トラヒックをバイパスさせた結果、全体のスループットは Scenario #1 とほぼ同等となり、また正常トラヒックに対するアップロード時間は Scenario #1 と比較して 10% 以内のオーバーヘッドで同等の性能が得られていることが分かった。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１３件）

① 佐藤 寧洋, 河合 勇輝, 阿多 信吾, 岡育生,“データベースを利用した SDN アーキテクチャの動的構成手法,” 電子情報通信学会論文誌, J100-B (12), 2017 （査読有）

② Naoki Yoshida, Shingo Ata, Hiroki Nakayama, Tsunemasa Hayashi, “Automation of Network Operations by Cooperation between Anomaly Detections and Operation Logs, ” Proc. IEEE GLOBECOM 2017, December 2017. （査読有）

③ Hiroki Kawai, Shingo Ata, Nobuyuki Nakamura, Ikuo Oka, “Identification of Communication Devices from Analysis of Traffic Patterns,” Proc. CNSM 2017, November, 2017. （査読有）

④ Shingo Ata, Yusuke Iemura, Nobuyuki Nakamura, Ikuo Oka, “Identification of User Behavior from Flow Statistics,” Proc. APNOMS 2017, September 2016. （査読有）

⑤ Shingo Ata, Toshio Tonouchi, “ Management of Information, Communications, and Networking: from the Past to the Future,” IEICE Transactions on Communications, E100-B (9), pp. 1614-1622, 2017.（招待論文、査読有）

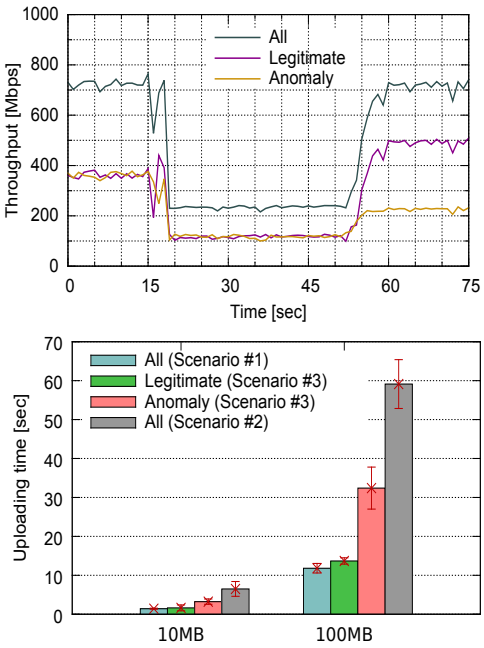

図６　検証結果

〔学会発表〕（計５件）

① 阿多 信吾「運用管理の自動化によるパーソナライズネットワークの実現に向けて」、*電子情報通信学会情報通信マネジメントワークショップ（招待講演およびパネリスト）* 2018 年 3 月

② 阿多 信吾「キャンパスネットワークの SDN 化の実例と課題」*大学 ICT 推進協議会年次大会*、2017 年 12 月（招待講演）

〔その他〕
ホームページ等
http://www.c.info.eng.osaka-cu.ac.jp/ に研究成果の概要を公表

６．研究組織
(1)研究代表者

阿多　信吾（ATA SHINGO）
大阪市立大学・大学院工学研究科・教授
研究者番号： 30326251