

# Software-Defined Network の形式検証に関する動向

八鍬 豊<sup>†</sup> 野田 夏子<sup>†</sup> 富沢 伸行<sup>†</sup> 登内 敏夫<sup>†</sup>

近年データセンターのネットワークの運用管理に関して SDN(Software-Defined Network)が注目されており、運用の自動化・効率化・省電力化といった期待を集めているが、自由度の高い制御に伴う不具合が混入する可能性も懸念されている。そこで我々は、SDN の「正しさ」を検証する技術に注目し、特に形式手法を利用するものについて動向を調査している。本稿ではそれらについて紹介し、ワークショップで議論したいテーマについて述べる。

## About Formal Verification Techniques of Software-Defined Network

Yutaka Yakuwa<sup>†</sup> Natsuko Noda<sup>†</sup> Nobuyuki Tomizawa<sup>†</sup> Toshio Tonouchi<sup>†</sup>

In recent years, SDN (Software-Defined Network) attracts attentions in respect to operation management, and it is expected to be useful for automation, streamlining and electricity saving of data centers. But there is an increasing concern that bugs will arise in networks that have high flexibility of control. Now We are interested in verification techniques of SDN, and we research on trend of them especially using formal methods. In this paper, we introduce them and describe a theme we want to discuss in the workshop.

### 1. はじめに

クラウドサービスの普及に伴い、データセンターの安定運用が今後の IT 化社会の大きな課題となっている。例えば、現在多くのサービスが Amazon Web Service と連携し稼働しているが、もしそのデータセンターが停止した場合、それらサービスの一部は機能しなくなる。人命にかかわる医療系サービス等の機能に支障が出るようなことも考えられ、それが社会に与える影響は計り知れない。そのため、データセンターの安定運用を目的とした数多くの取り組みがなされている。

データセンターの、特にネットワークの運用管理に関して、Software-Defined Network(以下 SDN)が注目されている。ネットワーク制御をプログラマブルな方法で一元管理することが可能になる新たなパラダイムであり、データセンターの運用の自動化・効率化・省電力化等、様々な期待を集めている[7]。

一方で、ネットワーク制御の柔軟性が増す分、それに伴う不具合の発生が懸念されている。例えば、パケット転送がループしてしまうような制御は、ネットワークの不具合として基本的なものだが、開発者がプログラムとして定義したネットワーク制御では、開発者の考慮漏れ

でそのような不具合が混入したり、その他のプログラムとの組み合わせにより予期せぬ形で不具合が顕在化したりすることが多くなる。また、SDN ではネットワークスイッチの設定が非同期分散で度々変更されるため、その最中に制御で不整合が生じる可能性もある。これらはほんの一例であり、新たなパラダイムである SDN の世界でどのような不具合が起こり得るか、その全容は明らかでない。しかし、将来データセンターのネットワークは SDN として構築されることが多くなると思われ、何らかの観点でそのネットワークの「正しさ」を担保する検証技術は極めて重要になる。SDN の概念を実現するプロトコルとして代表的な OpenFlow[4]の提唱者の 1 人である Prof. McKeown も、Open Networking Summit 2012 の基調講演[5]で SDN の検証の重要性を訴えている。

我々は SDN を検証する技術に注目し、特に形式手法を利用するものについて動向を調査している。従来から特定のプロトコルにおけるネットワーク制御が正しいかを形式検証する技術は提案されているが[2]、SDN では従来のプロトコルと比べネットワーク制御の自由度が高く、利用できる情報や定義できる動作の種類が増す。SDN においては、もはやネットワーク自体がソフトウェアの実行基盤の一部になると言える。そのため、新たな検証技術が必要になると考えられるためである。

本稿では、形式手法による SDN の検証技術の動向

<sup>†</sup>NEC 情報・ナレッジ研究所

Knowledge Discovery Research Labs., NEC Corporation

調査から 2 つの研究事例を紹介する。また、ワークショップで議論したいテーマについて述べる。

## 2. SDN とその形式検証

SDN は、ネットワーク制御をプログラマブルな方法で一元管理することを目指したパラダイムである。従来は個々のネットワーク機器を設定することでネットワーク全体を制御していたが、SDN はネットワーク全体を 1 つのプラットフォームに見立て、ソフトウェアで一元的に制御する。産業界でも SDN への注目が高まっている[7]。

ここでは形式手法による SDN の検証技術の動向調査から 2 つの研究事例を紹介する。

### 2.1. NICE

NICE[1]は OpenFlow コントローラーNOX[3]向けのテストツールである。テストの網羅度を上げるため形式検証技術を利用している。基本的な機能は、入力としてコントローラー用プログラム・ネットワーク構成モデル・プロパティ(パケット転送がループしない等)を与えると、プロパティの成否と、プロパティが満たされない場合には反例を出力する。コントローラー用プログラムの変更なしに検証でき、ユーザーにとっての利便性は高い。

検証のアプローチとしては、モデル検査をベースにしているが、記号実行も組み合わせで用いる。ネットワークに流れるパケットを具体的な値で抜おうとすると状態爆発してしまうので、記号実行によりコントローラーにとって等価なパケットのクラスを導出し、その代表値のみを用いたモデル検査を行うことで、状態数を削減する。また、OpenFlow の検証に特化した探索戦略を採用している。これにより、実験では Spin や JPF と比較しても良好な検証効率を示す結果が得られている。

また、ネットワーク構成モデルやプロパティに関しては、利用頻度の高い一般的なものはツール側であらかじめ用意し、ユーザーはそれらを選択するだけで利用可能な形で提供している。一方で、ユーザーがカスタマイズしたものを入力も可能なため特殊なモデルやプロパティについても検証でき、検証する内容に応じて柔軟な使い方が可能なツールであると言える。

### 2.2. ネットワーク設定更新メカニズムの整合性保証

Reitblatt らは、OpenFlow のネットワーク設定(パケットの内容に応じた処理の定義)の更新に関する整合性を定義し、その整合性を保つネットワーク設定の更新メカニズムを提案している[6]。

定義している整合性は per-packet 整合性と per-flow 整合性の 2 種類である。前者は「任意のパケットは同一のネットワーク設定によってのみ処理される」というもの、

後者は「任意のフロー上の全てのパケットは同一のネットワーク設定によってのみ処理される」というものである。ネットワーク設定の更新の際に、これらの整合性のいずれかを満たしていれば、ネットワーク設定の更新前と更新後の両方で成り立つ任意の性質は、ネットワーク設定の更新中でも成り立つということを定理証明支援ツール Coq により証明している。

文献では、ネットワークに関する基本的な性質を、更新前と更新後の設定において NuSMV で検証することで、全体を通して整合性を保ったネットワーク設定の更新が可能なることを保証する例を示している。また、NuSMV に限らず、ネットワーク設定が静的に適用される環境での性質を検証する技術であれば、上記の整合性と組み合わせることで、ネットワーク設定が動的に更新される環境での性質の成否が検証可能となる。これにより、検証の難しさを緩和することができる。

## 3. おわりに

本稿では、ネットワークの分野において SDN という新たなパラダイムが注目されていること、その検証技術が今後重要になるだろうことを述べた。また、特に形式手法を用いた検証技術に注目した動向調査から 2 つの研究事例を紹介した。

ワークショップでは、SDN の正しさを担保する検証技術という重要なテーマに向けて、形式手法という分野からどのようなことができるか議論したい。

## 参考文献

- [1] Canini, M. et al.: “A NICE Way to Test OpenFlow Applications”, Proc. of NSDI, 2012.
- [2] Feamster, N. et al.: “Detecting BGP configuration faults with static analysis”, Proc. of NSDI, 2005.
- [3] Gude, N. et al.: “NOX: Towards an Operating System for Networks”, ACM SIGCOMM Computer Communication Review, Vol. 38(2), pp. 105-110, 2008.
- [4] McKeown, N. et al.: “OpenFlow: Enabling Innovation in Campus Networks”, ACM SIGCOMM Computer Communication Review, Vol. 38(2), pp. 69-74, 2008.
- [5] McKeown, N.: “Making SDNs Work”, Open Networking Summit, 2012.
- [6] Reitblatt, M. et al.: “Abstractions for network update”, to appear at ACM SIGCOMM, 2012.
- [7] 河井保博ほか: “[特集] Software Defined Network”, 日経コミュニケーション, No. 574, pp. 8-25, 2011.