6D-04

ネットワーク管理ワークフローの自動実行機構の提案

明石修 † 水谷后宏 ‡ 小林諭 § 福田健介 ¶
国立情報学研究所 †§¶ 近畿大学 ‡

[概要]
複雑化するネットワークの管理運用において，管理ワークフローを自動的に実行することが望まれている．本提案では，従来は個別操作の寄せ集めであったサービス設定ワークフローを高い抽象度で表現可能として環境・実装依存の部分を隠蔽し，実行結果解釈においてはワークフロー全体としてネットワークオペレータが意図する通りであったことの妥当性を，ネットワーク状態観測を含めて自動的に検証することを目指す．ワークフロー記述は，基本操作をテンプレートとして抽出し，それらの合成として高い抽象度で表現する．妥当性検証は，全体意図とデータプレーン検証過程の学習を統合して自動化し，更に観測基盤経由のデータ参照に束ねて環境依存部分を抽象化して検証する．

1 はじめに

通信と情報処理機能の融合であるネットワーク環境が発展を続け，基本的な社会インフラとして不可欠な存在となる一方，その安定運用は必須の課題となっている．一方，さまざまな要求や機能を実現するための管理運用手順は複雑化し，その自動化や自律運用が望まれているが，1) 設定のためのワークフロー実行結果の妥当性の検証，2) 環境の変化や障害が発生した場合の影響範囲に応じた修正作業，等が必要であり，その時点でのネットワーク状況に応じた適応的な対処が重要となる．

自動操作を実現するためのアプローチとして，対象の操作を細かな基本操作に分解して定義し，単純にそれらの基本操作を組み合わせて，より抽象度の高い操作を実現したとしても，自動実行のフレームワークとして機能させるのは難しい．なぜならば，基本操作の実行結果は単純な真偽の値が戻ってくる関数ではなく，機器・機能依存の実行結果や状況を記述する様々な文字列を含むデータであり，どのような機器とどのようなトポロジで接続されているかなど，大域的なネットワーク情報を参照しながら判断する必要のあるケースも少なくない．すなわち，個別のメッセージを解釈することの困難さに加えて，適用先のネットワーク状態やワークフロー全体の意図に基づく統合的な解釈などが不可欠となる．機器がログシステムに出力する文字列を対象としても，状況の困難さは変わらない．

一方，基本操作をワークフロー実現のために組み合わせて実行することは，通常のプログラミングの概念に従えば，基本関数を合成してより抽象度の高い関数を作成・実行することに相当するが，個別の基本操作や参照するデータの抽象化・カプセル化が行われないと，手順全体の合成が見通しの効かないものとなってしまう．すなわち，細かな基本操作を単純にワークフローに沿って並べただけでは，局所可読性が損なわれ，ネットワーク環境の変化に応じた新たなワークフロー作成等の維持管理が不可能となる．これらの問題の直接的な解決策として，出力の差分を吸収するライブラリ等を作成する手段も想定されるが，様々な機器や環境からなるネットワークに対応可能なこれらのライブラリを作成・維持管理する困難さに加えて，ワークフロー全体の視点や環境の観測を通じてその実行結果の是非を判断しないとならない場合には対応ができない．

例えば，ネットワーク管理者は，特定の IP アドレスを持つパケットをブロック，あるいは，明示的に通過させるような制御を管理するが，アドレスブロック毎に各ルータに記述する必要があるため，ネットワーク全体での挙動が意図通りであるがどうか検証することは難しい．[1] では，ネットワーク管理者のアクセス制御に関する意図をネットワーク全体視点での高抽象度な言語体系で記述する．そのうえで，意図を具現化するルータ毎の設定が，意図通りであるか，変更する場合の矛盾がないかを検証し，更には操作意図を実現するための記述自体も生成する．実現方法としては，記述した意図とルータのコントロールプレーンでのアクセス制御記述を突合して検証を行うが，この枠組は一般的な制御への適用は困難である．それは，一般的な制御対象がコントロールプレーンの記述のみに閉じず，実際のネットワーク環境を測定しないと得られない情報を用いた制御動作を行う必要があるためである．更に，その参照する情報が他の操作や機器の状態に依存する部分が存在する場合もあるためである．

2 提案アーキテクチャ

本提案では，サービス設定ワークフローを高い抽象度で表現することにより環境・実装依存の部分を隠蔽し，ワークフロー全体としてネットワークオペレータが意図する通りの実行結果であったことの妥当性を，全体意図整合性チェックとデータプレーン検証過程の学習により自動的に検証することを目指す．更に検証過程を適用先のネットワーク状態と共に学習する機構と連動させることにより，環境の変化や障害時に，サービスを維持するための代替ワークフローを推定し，ネットワーク運用の自動化・自律化を可能とすることも目指す．図 1 に提案手法によるワークフロー全体での検証アーキテクチャを示す．

最初の構成要素は，ワークフロー全体視点および環境情報を用いた解析・検証手法の体系化である．具体的には，ネットワーク管理を行うワークフローにおいて，ルータのコンフィグ/コントロールプレーンの制御記述のみから検証可能な部分と，環境依存で外部観測をしないと検証が不可能な部分に分ける．このような視点で解析と新たな体系化を行うことで，全体設計において必要な情報を明確化する．なお，外部環境依存部分は，データプレーンの観測で得られる情報，および機器等の内部情報から成り，後者は機器が出力するログ情報をも含む．解析対象のデータセットは，まずは，典型的なワークフローに対して行い，順次，SINET[2] 等の実際の ISP の作業ワークフローやログデータに拡張していく．

次の構成要素は，これらの解析結果に基づき，ワークフローの各操作を表す基本操作をテンプレート化し，ビルディングブロックとして使うことが可能なパーツとして取り出す手法である．汎用的なテンプレートとして表現した上で付加するパラメータ部分と分離することにより，同様の意味を持つ基本操作を同じ名前で扱うことを可能とし，合成，全体意図との整合性検証，類似度推定の学習を簡易化する．これらのテンプレートを合成して組み合わせ，目的のサービスを実現する

*Proposal of Automated Workflow Processing for Network Management
†Osamu Akashi, National Institute of Informatics
‡Kimihiro Mizutani, Kindai University
§Satoru Kobayashi, National Institute of Informatics
¶Kensuke Fukuda, National Institute of Informatics

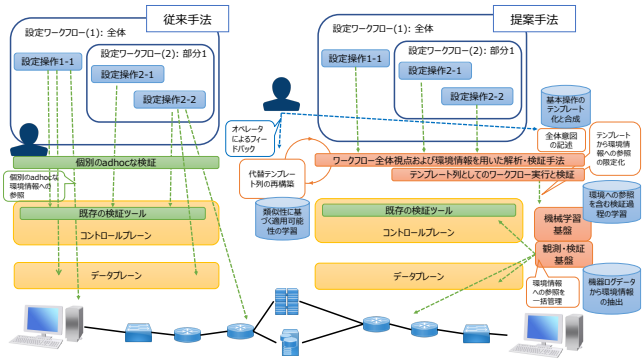

Figure 1: ワークフロー全体での検証アーキテクチャ

ためのワークフローを構築する．合成したワークフロー全体の実行に際し，個々のテンプレートの実行結果を環境を参照しながら判断し，最終的にはワークフロー全体で実行結果の成否を判断可能とする．そのため，適切なテンプレート化と，全体意図表現が重要となる．

また基本操作の意味解釈を，適用先のネットワーク環境，過去の事例，全体意図との整合性などと突合し，データプレーン検証過程の学習とも統合して自動化し，更にネットワーク状態の観測・解析過程を観測基盤経由に束ねて環境依存部分を抽象化した上で，統合的に妥当性を判断する枠組みを構築する．この手法においては，カプセル化された中身の局所的な検証のみでなく，ワークフロー全体を見た流れで判断することも求められるため，グローバル状態も参照する点から，完全なカプセル化ではない．しかしながらテンプレート合成を行うレイヤからは情報隠蔽がされた形で操作可能とし，参照ポイントを限定した環境情報観測・参照を実現する．

ワークフロー実行結果の解釈においては，外部ネットワーク情報への参照，解析過程，過去の事例等への参照を，機械学習フレームワークと連携しその処理を高度化・効率化する機構も実現する．学習基盤は，観測基盤と連携し，データプレーン観測結果や，関連機器の出すログ情報等から検証に必要な情報を効果的かつ効率的に抽出する．

また，適用先のネットワーク状態と関連させて学習することにより，テンプレート，全体意図，データプレーン状態が連携した形での学習となることで，従来のコントロールプレーンに閉じた検証とは異なる部分に適用可能となるが，環境の変化時にその影響範囲解析に基づき，設定したサービスを維持する代替ワークフローを推定して作成する機構を実現し，更なるネットワーク運用の自律化を可能とすることも目指す．

既存の構成管理プラットフォームとしては Ansible[3] が知られており，アプリケーションデプロイ，ソフトウェアデリバリー迅速化などを自動化する．また，コントロールプレーン分析，特にルータのコンフィグ分析においては Batfish[4] が，アクセス制御情報を含めて，セキュリティ，信頼性，コンプライアンスの妥当性，変更分析などを行う．これらは自動化に向けては有用なツール類であり，広く使われている．しかしながら本提案が対象とするような，データプレーン状況や観測結果に依存するようなケースへの対処は対象外となる．

[1] では，ネットワーク管理者のアクセス制御に関する意図をネットワーク全体視点での高抽象度な言語体系で記述し，その意図を具現化するルータ毎の設定が意図通りであるか検証する．また意図を実現するための記述自体も生成する．実装としては，高抽象度で記述した意図と，ルータのコントロールプレーンでのアクセス制御記述を突合して検証を行うが，実際のネットワーク制御への直接の適用は困難である．それは，制御対象が，コントロールプレーン外のデータプレーンや，機器やネットワーク状況を観測したいと得られない情報を用いた制御動作を行う必要があるためである．

実際の運用例として，データプレーン参照への必要性に加えて，管理ポリシなどの上位レイヤの要求を考慮すべきケースも発生している．これはコントロールプレーンの範囲で妥当性を検証したワークフローの記述と不整合を起こす場合もあり，これらの整合性チェックも不可欠となる．例えば，隣接する複数のドメイン群とセキュアな通信路を作成し，自ドメインのクラウドと接続設定をする場合を想定する．サービス実現のためには，通例，収束安定性に優れる L2-VPN を隣接ドメインと自ドメインのクラウドと結ぶ個別ワークフローを設定し，それを複数回繰り返す全体ワークフローを設定する．しかし，あるドメインが L2-VPN を管理上の理由で許容しない場合，これは全体として妥当なワークフロー実行とはならない．このような場合その不整合を検出し，セキュアな通信路を構築するという，より抽象度の高い本来の要求意図に従って，特定の接続に関しては L3-VPN で実現する代替ワークフローを提示する必要がある．このようなケースは既存の手法では対応できないため，より抽象度の高い操作意図で表現されたワークフローに基づき，個別の代替操作を提示して全体として意図通りとなるように実行する新たなフレームワークを必要とする．

3 おわりに

ネットワーク管理ワークフローの自動実行機構を実現するため，まずはルータの設定記述に注目し，ワークフロー解析と検証手法の体系化，データプレーン情報を含むネットワーク環境情報依存部分の分析を行い，ワークフロー全体視点で検証する手法を体系化する．対象とする設定記述は，典型例に関して予備解析を行い，次に公開されているネットワーク設定ファイルや，実際の学術情報ネットワークである SINET 等の実運用データ等に拡大して解析を行う．自動化の視点からは，ワークフローを構成する個別操作，設定コマンド群をテンプレートとしての自動抽出する手法をドメイン知識を入れながら確立し，意味的な集合として操作可能なような階層的クラスタリング手法，ビルディングブロックとしての利用可能性やその合成手法を含めて解析を行い，その適用可能性を検討する．また全体意図に基づいてテンプレート列を合成して表現することが可能なように，その記述手法や，自然言語処理の手法等の適用も考慮した自動化手法を検討する．

1. B. Tian, X. Zhang, E. Zhai, H. Liu, Q. Ye, C. Wang, X. Wu, Z. Ji, Y. Sang, M. Zhang, D. Yu, C. Tian, H. Zheng, and B. Zhao. “Safely and Automatically Updating In-network ACL Configurations with Intent Language”. *Proc. of SIGCOMM19*, pages 214–226, 2019. ACM.
2. SINET. https://www.nii.ac.jp/research/centers/network/
3. Ansible. https://www.ansible.com
4. A. Fogel, S. Fung, L. Pedrosa, M. Walraed-Sullivan, R. Govindan, R. Mahajan, and T. Millstein, A General Approach to Network Configuration Analysis, *Proc. of the 12th USENIX Conference on Networked Systems Design and Implementation (NSDI)*, pp. 469–483, 2015. https://www.batfish.org

謝辞

本研究は JSPS 科研費 20H04185 の助成を受けたものです．