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　 ７ 日現在

機関番号：１４３０１
研究種目：基盤研究(B)（一般）
研究期間：2019～2023
課題番号：１９Ｈ０４０９４

研究課題名（和文）Intent-Based Networkingにおける管理者の意図の自動推定

研究課題名（英文）Automatic Estimation of Administrators' Intension in Intent-Based Networking

研究代表者
岡部　寿男（Okabe, Yasuo）

京都大学・学術情報メディアセンター・教授

研究者番号：２０２０４０１８

交付決定額（研究期間全体）：（直接経費）　　13,100,000円

研究成果の概要（和文）：大規模なネットワークの設定を行う際に、ネットワークに何を行わせようとしているかを高い抽象度の「意図」として記述し、コントローラがそれに従って各機器の設定を自動的に生成することで管理者の負担を軽減する、Intent-Based Networkingが期待されている。しかしながら管理者の意図はしばしば曖昧で矛盾を含み、かつ暗黙の前提もある。そこで、管理者がネットワークの設計や運用において行っている判断を人工知能に学習させ、システムに組み込めるようにすることで、大規模ネットワークの設計と運用、管理を自動化し、管理者の負担を軽減するための技術を研究開発した。

研究成果の学術的意義や社会的意義
本研究の特徴は現実に動作しているネットワークから人工知能により管理者の意図を推測しようとする点である。人工知能応用として、単に管理者が日常行っているネットワーク管理を人工知能に学習させ模倣させるだけのでは、学習データがブラックボックス化され、管理者の意図に反するものが含まれてしまってもそれが実際に使われるまでは顕在化しないという問題点がある。本研究では、管理者の動作そのものを学習させるのではなく、管理者が暗黙の前提や知識としているルールを学習し抽出して可読な形で出力させることでこの問題を回避しようとする点が独自であり、ネットワーク管理に限らず大規模な情報システムの運用に応用できる可能性がある。

研究成果の概要（英文）：There is a lot of anticipation for Intent-Based Networking, which reduces the burden on administrators by describing what you want the network to do as a high-level “intent” when setting up a large-scale network, and then having the controller automatically generate the settings for each device according to that intent. However, the administrator's intent is often vague, contradictory, and also contains implicit assumptions. Therefore, we have researched and developed a technology to reduce the burden on administrators by automating the design, operation, and management of large-scale networks by having artificial intelligence learn the decisions that administrators make in network design and operation, and then incorporating them into the system.

研究分野：情報ネットワーク

キーワード：Intent-Based Networking　機械学習　ACL　経路制御　パッシブ計測　Kubernetes

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

スマートフォンや IoT 機器の急速な普及や電子商取引の拡大などに伴い、インターネットを構成するネットワークの規模は年々大きくなり、通信量が増大し、ネットワーク機器も数が増えるとともに多様化が進んでいる。一人のネットワーク管理者が管理する対象のネットワークの複雑度が、機器の数や種類、構成等により拡大することでネットワークの全体構成を常に把握し、設定変更作業を行うには依存関係などに細心の注意を払う必要がある。このような状況を解決し、ネットワーク管理者の負担を軽減することを目的とした自動管理手法が長く研究されている。

古典的なネットワーク運用においては、サービス要件の追加・変更、トラフィックの増減、障害などの状況の変化やネットワークの構成変更に対して、管理者がその都度システムの設計を変更しそれに合った設定（コンフィグ, configuration）を作成してネットワーク機器に投入する。その際の管理者の設計の意図は設計書などの文書上に曖昧な記述でしか残されておらず、しかも障害や輻輳などの回避のための臨時の設定においてはしばしば文書への反映が漏れるため、設定を行った管理者の意図が機器に分散して格納されているコンフィグからしか推測できないことがあり、管理者の交代時の引継ぎが困難であるなどの問題があった。これに対し SDN (Software Defined Networking)では、ネットワークの設定が SDN コントローラ上ソフトウェアコードという形で一元管理でき可読性も向上する。しかしながらその設定を行った管理者の意図が必ずしもコードにわかりやすく書かれているとは限らず、コードの動作からそれが書かれた意図を推測せざるをえないという点では同じ問題が残る。

そこで、管理者がネットワーク機器に設定をする際に、機器がどのように(How)動作するか記述するのではなく、ネットワークに何(What)を行わせおうとしているかの意図(Intent)を高い抽象度で記述する Intent-Based Networking あるいは Intent-Based Network Modeling (IB-nemo)が提唱され、IRTF Network Management Research Group (NMRG)や IETF IB-nemo BoF などで議論が進められている。OpenConfig や OpenDaylight で採用されている YANG データモデルに基づく機器ベンダに依存しない共通の記述と API を用いると、幅広く多くのネットワーク機器やソフトウェアを対象に制御を行えるようになる。これに Intent-Based Networking の考え方を取り入れ、管理者が、個々の機器の動作(How)ではなく提供したいネットワークに対するサービス要件(What)を Intent Description Language により高い抽象度で記述できるようにすることで、管理者の設計の意図を明確な形で記述しさえすれば、そこから個々のネットワーク機器のコンフィグを生成し機器に投入するところまでが自動化され、管理者の負担は大きく軽減されるとともに、意図が記録されることでネットワーク運用の継続性、一貫性も担保される。

しかしながら、現実には管理者の意図はしばしば曖昧でかつ矛盾する要求を含み、論理的には要求を満たすネットワーク構成の解はないということが生じうる。さらに管理者にとっては暗黙の前提となっているさまざまな制約条件があり、それを Intent Descrpition Language のような形式記述で網羅的に書き下す必要があるようでは却って管理者の負担を増大させてしまう。現実のネットワーク運用において知識と経験を備えた管理者が様々な事象に遭遇した際に行っている判断を代替し自動化するには、OpenConfig、OpenDaylight などのネットワーク設定自動化の仕組みに Intent-Based Networking の考え方を組み合わせるだけでは不十分である。

２．研究の目的

本研究では、ネットワーク管理者がネットワークの設計や運用において行っている判断を人工知能(AI)に学習させ、明示的に記述されていない諸要件のトレードオフや暗黙の制約条件を学習データとして抽出し、システムに組み込めるようにすることで、管理者の経験と勘が頼りと言われがちな大規模ネットワークの設計と運用、管理を真に自動化し、管理者の負担を軽減しあるいは非熟練者に代替わりさせられるようにすることを目指す。

本研究では、Intent-Based Networking に基づき、ネットワークが提供すべき運用上の目標やサービスについて、それがどのように実装されるかを指定せずに高い抽象度で宣言された「意図」(Intent)として扱い、曖昧でかつ相反する要件を含みうる「意図」がネットワーク全体を制御するものとする。その上で、管理者の意図が Intent Description Language により記述され、抽象化されたネットワーク上の汎用コンフィグを経由して実際のネットワーク機器のコンフィグに展開される「意図の記述⇒サービス仕様定義⇒ネットワーク設計⇒機器への実装」の通常の流れに対し、実際に動作しているネットワーク機器の抽象コンフィグと収集されたネットワークの状況に関する情報から管理者の意図を推定する逆方向を行おうとする点が、類をみない独自のものである。

３．研究の方法

本研究では、管理者がネットワーク運用において行っている判断を人工知能(AI)に学習させ、明示的に記述されていない諸要件のトレードオフや暗黙の制約条件をルールとして抽出する。

その際、管理者の意図が確実にルール化されるよう、行うべき作業が多目的最適化となる場合にはパレート最適解となる複数の作業フローの候補を提示し、管理者に選択させる。また、管理者は可視化されたネットワークの状況を把握し、必要に応じて自動生成された設定を修正する形で干渉する。システムは、それらを管理者の意図として学習することで精度を高める。さらに各応用サービスが要求するサービス要件についても、時期や時刻などと紐づけてその傾向を学習する。これにより、従前は管理者／運用者の知識と経験に頼らざるを得なかったネットワーク運用上の高度な判断を、AI が代替できるようにする。このような考えをネットワーク管理の具体的な問題に適用した。

４．研究成果

ネットワーク管理の具体的な課題として、まずルータやファイアウォールで実装されている Access Control List(ACL) の最適化に取り組んだ。ACL ではネットワーク管理者が予め指定したルールリストに基づいて，パケットの通過・拒否の判断を行う．通過・拒否の判断は，ルールに記載されたヘッダ情報の組と，届いたパケットの情報とが合致したかどうかのマッチングを行い，マッチしたルールに記載されている処理によって決定される．ルールリストはネットワーク管理者によって人手で作成されることが多く，ACL の質はネットワーク管理者のスキルに依存する．規模の大きいネットワークの場合，ACL のルールリストは数千行にも及び，その膨大なルールリストを理解し，アップデートされるセキュリティ方針に則って，ルールリストを適宜更新するのは非常に困難な作業となる．その結果，ネットワーク内の他の ACL で拒否され届くことのないパケットや出現率の低いパケットを対象とした非効率なルールや，他のルールと統合できる冗長なルールが存在する可能性がある．ACL が処理するパケットは膨大な量になるため，このようなルールに対するマッチング処理が ACL 全体のパフォーマンスに与える影響は大きい.本研究では，既存ルールのポリシーを厳密に反映するの手法ではなく，非効率なルールや冗長なルールを大きく削減することを目的とし，ACL によって通過・拒否されたトラフィックのデータから，トラフィック傾向に基づいたルールリストを再構築する手法を提案した．具体的には，ある ACL ルールリストと ACL 適用前のトラフィックデータから，各パケットに通過・拒否のラベルを付与したデータセットを作成し，これを入力データとして決定木を構築後，決定木をルールリストに変換する手法を提案した．データセットの作成は，ACL のエミュレータを用いて，トラフィックデータに含まれる全パケットに正確にラベルを付与する．決定木の構築には，複数の決定木構築アルゴリズムを用い，最もルール数が少なく，精度が高い木を選択する．同時に，決定木が深くなることによるルールの増加と複雑化を避けるため，木の深さを調整する．出力された決定木に対して，根から葉まで到達する全ての経路を算出し，経路に含まれる各条件式の直積を求めることで，葉に到達する条件を一意に定める．各経路で定まった条件式は ACL の文法に則ったルールの形に変換可能なので，全ての経路に対して条件式の変換を行い，ルールリストを作成する．最後にルールリストのルール間の包含関係を算出し，部分集合に当たるルールを上位にするソートを行うことで，新たな ACL ルールリストを構築する．あるネットワークとそのネットワーク内のトラフィックを仮定したうえで，入力データセットに，手動で生成したトラフィックデータとルールリストを用い，上記手法について実験を行なった．その結果，提案手法を用いることで，一定の精度を保ったまま，既存ルールリストから大幅にルール数を減らしたルールリストの構築が可能であると示された．

第二に、SDN を用いた中央集中型の経路制御では，刻一刻と変化するネットワークの状況に応じて動的に柔軟な経路制御を行うことができることを前提に、このような環境の変化によって，リアルタイムに Quality of Service(QoS)を最適化する経路を求める手法の研究に取り組んだ．任意の QoS 指標に対して最適な経路を求める問題は，中規模以上のネットワークにおいて現実的な時間で解くことが困難であることが知られている．そのため Genetic Algorithm(GA) のようなメタヒューリスティックスを使用する手法が提案されているが，リアルタイムに最適化を行うという要求を満たすのはなお困難である．これを機械学習によって解決しようという試みがあり、機械学習モデルを事前に学習しておけば，運用時にはわずかな時間で準最適解を出力することができる．このアプローチの課題は，機械学習モデルがネットワークのトポロジー変化に対応できないということである．そこで本研究では画像認識の分野で成果を上げている，Convolutional Neural Network(CNN)をグラフ構造に適用した Graph Network を用いることで，トポロジーの変化に頑強なモデルを作成することを目指した。提案手法の性能を確認するため，まずは最も簡単な最適経路制御として広く用いられている分散型経路制御である OSPF を学習対象とした．様々なトポロジーを用いて学習を行なったのち，全く新しいトポロジーに対して 84%の精度で OSPF の経路を予測することに成功した．より現実的な QoS 指標として最大帯域使用率を採用し，最大帯域使用率最小経路を学習させたところ 53%程度の精度にとどまり，より一層のモデルの検討が必要であるという課題が明らかになった．

第三に、ネットワークの状態推定の課題に取り組んだ。SNMP（Simple Network Management Protocol）は、ネットワークに接続された通信機器に対し、ネットワーク経由で監視、制御するためのアプリケーション層プロトコルである。管理者は SNMP 等を用いて管理している通信機器の状態を調べることができるが、他の管理者によって運用されているネットワークの情報を入手することは一般にはできない。そこで通信機器の状態を観測するのではなく、End-to-End の通信の状態を観測することでネットワークの状態を推定することに取り組んだ。TCP は

Endto-End の通信を保証するプロトコルであり、UDP (User Datagram Protocol) と異なり、ネットワークの状態に応じて、送信するデータ量を調整するため、その振る舞いを観察することでネットワークの様々な状態を解析することができる。そこで中間ノードにおいてパッシブ計測を行うことでネットワークの状態を推定する研究を進めた。上流ネットワークとの接続点でありトラフィック集約点となる通信機器において複数の TCP フローを監視することで上流ネットワークの状態を推定する手法を提案した。複数の TCP フローをパッシブ計測し、ヘッダに格納されている情報をフローごとに解析する。それらの情報を総合的に判断することでフローが共通に経由する上流ネットワークの経路上で起きている性能低下の原因事象の特定を試みる。TCP の輻輳制御の周期性に着目し、ヘッダから得られる情報の時系列データを Lomb-Scargle 法を用いてスペクトル分析し、周波数空間に落とし込む。そこから得た強い周波数成分を特徴量とし機械学習を用いることで、ネットワークの状態を推論する。この手法を用いるためには訓練データを準備する必要があるが、実ネットワークで性能低下の原因事象が特定できる状況は稀であり、教師ありデータを用意するのは容易ではない。そこでテストベッドとしてネットワークにおける様々な事象を NS-3 によりシミュレーションすることで、機械学習に必要となるデータセットを作成した。評価実験としてクラスタリングの性能といくつかのシナリオに基づく手法の評価を行い、その結果シミュレータを用いた簡単なシナリオにおいて手法が有効であることを確認した。また実ネットワークにおける激しい輻輳の検知とその発生箇所の範囲を推定できる可能性が示された。

さらに、コンテナオーケストレーションツールである Kubernetes によるコンテナ運用管理の課題にも取り組んだ。Kubernetes は宣言的な設定管理手法を採用しており、クラスタ管理者が宣言した望ましい状態を自動的に維持する仕組みを持つ。これは制御プレーンと呼ばれる管理層において複数のコントローラがそれぞれ自律的に自分の担当するリソースを変更し調整することで実現されており、このような設計のため、ある一つのリソースに対する変更が他のリソースに連鎖的に伝播していく。変更伝播が遅延するとアプリケーションのデプロイが遅れてユーザからのリクエストを処理できないなど、この連鎖的変更に要する時間はクラスタ上で動くアプリケーションの可用性に直結する。しかしこの連鎖的な変更を効率よく観測する手法が存在せず、変更がどのリソースまで伝播するのかや変更伝播のどの部分に時間がかかっているのかを特定することは容易ではない。そこで、マイクロサービスアーキテクチャで構築されたアプリケーションを監視する仕組みである分散トレーシングの手法を応用して、制御プレーン内のオブジェクトの変更を自動で追跡するシステムを提案した。本手法は、現在の状態や望ましい状態を保持しているオブジェクトのメタデータに対して変更伝播 ID(CPID) という識別子を 1 つだけ付加し、そのオブジェクトの変更を観測したコントローラが次のオブジェクトに CPID を伝播させる。また、複数の変更情報を 1 つのオブジェクトに載せる必要があるときは新たに CPID を生成し、元の CPID との関係を記した情報を追跡サーバに送信する。追跡サーバではその情報をもとに CPID の派生を表すグラフを構築し、計測者からのリクエストに応じてある CPID から派生した CPID を列挙し、それらの CPID とともに出力されたログを取得する。提案手法の一部を実装したシステムを用いてテスト環境で動作検証を行い、変更伝播の可視化や変更伝播に要する時間の計測が可能であることを確認した。

以上のように、要素となるネットワーク管理の課題について研究の目的に沿った具体的な成果が得られた。一方で、当初目指した、「意図の記述⇒サービス仕様定義⇒ネットワーク設計⇒機器への実装」の通常の流れに加えて、実際に動作しているネットワーク機器の抽象コンフィグと収集されたネットワークの状況に関する情報から管理者の意図を推定する逆方向によりサイクルを完成させるところにまでは至らなかった。

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Kei Wakabayashi, Daisuke Kotani, Yasuo Okabe	４．巻 34
２．論文標題 Traffic-aware Access Control List Reconstruction	５．発行年 2020年
３．雑誌名 International Conference on Information Networking (ICOIN)	６．最初と最後の頁 616-621
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ICOIN48656.2020.9016512	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kaku Sawada, Daisuke Kotani, Yasuo Okabe	４．巻 34
２．論文標題 Network Routing Optimization Based on Machine Learning Using Graph Networks Robust against Topology Change	５．発行年 2020年
３．雑誌名 International Conference on Information Networking (ICOIN)	６．最初と最後の頁 608-615
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ICOIN48656.2020.9016573	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kenta Murayama, Yasuo Okabe	４．巻 38
２．論文標題 Network State Estimation by Spectral Analysis of Passively Measured TCP Flows	５．発行年 2024年
３．雑誌名 International Conference on Information Networking (ICOIN)	６．最初と最後の頁 373-378
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 江平智之，小谷大祐，岡部寿男，	４．巻 123-277
２．論文標題 分散トレーシング手法を用いたKubernetes制御プレーンにおけるオブジェクトの連鎖的変更の観測手法の検討	５．発行年 2023年
３．雑誌名 電子情報通信学会技術報告	６．最初と最後の頁 18-24
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計4件（うち招待講演　0件／うち国際学会　4件）

1．発表者名 Dongyang Li, Daisuke Kotani, Yasuo Okabe
2．発表標題 Improving Attack Detection Performance in NIDS Using GAN
3．学会等名 2020 IEEE 44th Annual Computers, Software and Applications Conference (COMPSAC2020)（国際学会）
4．発表年 2020年

1．発表者名 Tsuyoshi Arai, Yasuo Okabe, Yoshinori Matsumoto
2．発表標題 Precursory Analysis of Attack-Log Time Series by Machine Learning for Detecting Bots in CAPTCHA
3．学会等名 35th International Conference on Information Networking (ICOIN2021)（国際学会）
4．発表年 2021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
研究分担者	中村　素典 (Nakamura Motonori) (30268156)	京都大学・学術情報メディアセンター・教授 (14301)	

	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
研究協力者	小谷　大祐 (Kotani Daisuke) (70783059)	京都大学・学術情報メディアセンター・助教 (14301)	

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