ニューラルネットワークを用いたトラフィック解析による ネットワーク状態推定手法の設計と実装

吉田 蓮 [1,a)]　松下 葵 [1,b)]　和泉 諭 [1,c)]　髙橋 晶子 [1,d)]

概要：ネットワークに接続されている機器の増加に伴い，ネットワークに接続されている機器の構成管理や状態管理が重要になってきている．従来では危機の状態推定のためのネットワーク解析としてポートベースやペイロードベースの手法が行われてきた．しかし近年では，動的ポートの技術の発展や暗号化通信の増加などによってこれらの手法による解析は困難になっている．そこで，本研究では，トラフィックデータの統計的特徴からニューラルネットワークを用いてネットワーク状態を推定する手法を提案する．さらに，実際に収集したトラフィックデータを用いて実験を行い，提案手法の有効性を評価する．

1. はじめに

サイバー攻撃などのネットワーク犯罪の増加に伴い，ネットワークを提供する管理者はネットワークに接続されている機器の構成管理や状態監視が重要となっている．さらに，近年ではパソコンやスマートフォンなどの従来のインターネットに接続するためのデバイスに加え，家電や自動車，ビル，工場など世界中の様々なものがネットワークに接続する IoT 技術が発展している．実際に，IoT 技術の発達や通信の高速化などによりネットワークに接続される機器の数は増加しており，総務省による調査[1]によると 2016 年から 2020 年にかけてネットワークに接続されている機器の数は約 1.5 倍の 253 億台になっている．このため現状からネットワーク管理者によるインターネット接続機器の管理が煩雑になってきている．

このような大多数の機器を対象としたネットワーク管理のアプローチの例として，ネットワークに接続されている全ての機器にプロキシサーバなどによる一定の制限を加える手法がある．この手法では容易にネットワークの管理を行うことが可能であるが，個々の端末や利用者に合わせた管理や制御ができないことから可用性の低下が課題として挙げられる．

また，ネットワーク利用者の通信のプライバシへの関心が高くなっており，暗号化された通信が急激に増加している．Web の情報を保持するリポジトリである http archive[2]によると 2016 年ではおよそ 25%程度であった HTTPS を利用している web サイトが 2022 年時点では 95%にまで増加している．このことから従来の通信の内容に含まれる情報に対するトラフィック解析は困難になっている．

そこで本研究ではネットワークに接続されている機器やその状態の把握を自動化することでネットワーク管理者の負担を軽減することを目的とする．その実現のために，機械学習を用いてトラフィックデータを解析して，ネットワーク状態を推定する手法を提案する．本研究におけるネットワーク状態とは，ネットワークに接続している端末，その端末を利用している利用者，利用しているサービスを想定する．本手法はトラフィックデータから統計的な情報などを特徴量として抽出して，それを用いて利用している端末やサービスを推定する．これにより暗号化通信に対しても適用することができる．

本稿では，トラフィックデータから抽出する特徴量の設計を行った．また，実際にネットワークに接続している端末のトラフィックを収集し，それに対して特徴量を抽出し，設計した特徴量とサービスの相関関係を調査した．さらに，機械学習を用いて，それら特徴量からサービスを推定できるかを実験により検証した．

2. 関連研究と提案

2.1 ネットワーク状態の推定に関する関連研究

ネットワーク管理は主にネットワークに接続されている機器や利用者の把握，異常状態の検知，対応のステップに従って行われる[3]．本研究ではネットワーク管理における機器や利用者の把握のステップに注目し，ネットワーク状態の把握や推定を行う．

ネットワークに接続している端末や利用者の推定・把握に関する関連研究や既存技術として，主にユーザ毎の認証 ID や機器毎の MAC アドレスなどで管理が行われている．しかし，近年は IoT 環境の普及によりネットワークに接続している端末数やその利用者が増加していることから，これら個々の ID や MAC アドレスを管理することは管理者の負担が増大する．また仮想化技術や MAC アドレスのランダム化などの発展により，MAC アドレスの変更が容易になっていることから，MAC アドレスによる端末認証も限界がある．

そこで，ネットワークに流れているトラフィックを解析することで，ネットワーク状態を推定する手法がある．従来のトラフィック解析では主に，ポートベース方式が用いられている．この手法ではパケットに含まれる宛先ポー

1 仙台高等専門学校
National Institute of Technology, Sendai College

a) a2111528@sendai-nct.jp
b) s1801121@sendai-nct.jp
c) izumi@sendai-nct.ac.jp
d) akiko@sendai-nct.ac.jp

ト番号を IANA(Internet Assigned Numbers Authority) で取り決められている，サービス毎に使用されるポート番号のリストによってサービスの種類を推定している．また，他にもペイロードベースによる解析も行われている．この手法ではパケットに含まれるペイロード部の中の文字列から，特定の文字列を抽出・照合しトラフィックデータの解析を行う．

他にもネットワーク状態を把握するために機械学習を用いるアプローチがある．例として AutoEncoder[4](以下，AE) を用いた手法が提案されている．AE はデータ生成や異常検知の際に用いられるニューラルネットワークの一種で，異常データが入力されると正常データを入力したときと比べて誤差の大きいデータを出力する．この性質を利用して Ly[5]らはトラフィックの異常検知手法を提案した．９つの商用 IoT デバイスから得られたボットネットトラフィックデータのデータセット[6]に対して AE を用いた手法を適用して，性能評価を実施した．その結果，良性トラフィックデータと悪性トラフィックデータを分類し，高い異常検知率を実現している．

また，Zheng[7]らは Convolutional Neural Network (CNN) を用いたトラフィック分類の手法を提案した．特徴量としてパケット長，送受信間隔，累積パケット長を送受信間隔で割った値であるバイトレートの 3 つの特徴量を用いて分類を行っている．さらに，様々な機械学習アルゴリズムの性能比較を行っており，ニューラルネットワークを利用した分類手法では特徴量抽出に必要な時間や推論時間が数理的な手法と比べて短縮できることを示した．

2.2 課題と提案

ネットワーク状態の推定に関する課題として，従来のトラフィック情報を用いたネットワークトラフィックの解析や推定が困難なことが挙げられる．その要因として，P2P やビデオストリーミングなどの複雑で動的なプロトコルの登場や，動的ポートやトンネリングなどの技術の発展などが挙げられる．これにより，これまで主に行われてきた IP アドレスや MAC アドレス，ポート番号を解析して端末や利用者，サービスの推定は困難である．また，利用者のプライバシ保護の観点から，暗号化されたセキュアな通信の利用が増加している．これにより通信の内容を参照することが不可能になるため，特定の文字列を照合するペイロードベースの解析を行うことも困難である．合わせて，ネットワークに接続されている端末が増加していることから，ネットワークトラフィック自体も増加傾向にあることから，ペイロードベースの解析は大量のディスク容量や高い処理能力が必要となる．

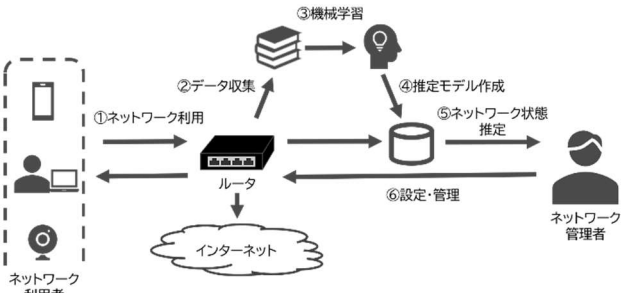

図 1　ネットワーク状態推定手法の概要

そこで，本研究では図 1 に示す概要に従い，トラフィック情報の統計的データを特徴量として，ニューラルネットワークを用いたネットワーク状態推定手法を提案する．推定には偽装や秘匿が困難である統計的特徴であるパケット長や送受信間隔などの統計的データを用いて，ネットワークに接続されている端末，利用者，サービスなどを推定する．これにより，ネットワークの障害の検出や利用者や端末のネットワーク利用状況などの把握を容易にし，ネットワーク管理者への支援を実現する．

3. ネットワーク推定手法の提案と設計

3.1 概要

本研究ではネットワーク状態を推定するために，宮本[8]の研究を基に以下の手順でトラフィックデータの解析を行う．

Step1. トラフィックデータの収集
　ネットワークを構築して様々な状況における通信トラフィックを観測しログデータとして蓄積する．

Step2. 特徴量の抽出
　トラフィックデータに含まれる様々な特徴量から，通信の内容を性格づけるような統計的特徴を抽出する．

Step3. 機械学習アルゴリズムによるデータ解析
　抽出によって得られたデータを基に機械学習によって異常検知や通信内容の推定を行う．

3.2 特徴量の設計

利用サービスの推定に用いるパラメータの検討を行うために表 1 に示す利用サービスの情報を利用する．また，これらのパラメータを基に実験に使用する特徴量を作成する．パラメータをもとに作成した 3 つの特徴量に加え，送信パケット・受信パケットの情報を加えた 4 つを特徴量とした．

パケット長：パケットの大きさを表している．用いているサービス毎に通信している内容が異なるため異なる種類のサービスを利用した際に異なる分布になることが考えられる．

パケット送受信間隔：前回キャプチャしたパケットの到

表 1　実験に使用するパラメータ

特徴量	データ型
パケット長	float
パケット送受信間隔	float
送信元 IP アドレス	string
宛先 IP アドレス	string

着時間と新しくキャプチャしたパケットの到着時間の差を表している．すなわちパケット毎の待機時間を表している．サービス毎にサーバで処理する量に違いが発生するためサービスの分類に有効であると考える．

パケットレート：パケット長をパケット送受信間隔で割った値で表される．これにより 1 秒あたりに転送されるパケットサイズを知ることができる．

送信/受信：送信元 IP アドレスと宛先 IP アドレスにより求めることができ，そのパケットが，自身が送信したものなのか，受信したものなのかを表す．ここでは，入力する特徴量を送信は 0，受信を 1 とする．パケットが送信と受信どちらに分類されるかは以下の式で表す．

$$\text{down} = \{x_i | desIP(x_i) = localIP\}$$
$$up = \{x_i | srcIP(x_i) = localIP\}$$

3.3 推定アルゴリズムの設計

トラフィックデータの解析はリアルタイムで行われるため，遅延の少ない機械学習アルゴリズムが好ましい．Zheng らの研究により，ランダムフォレストなどの数理ベースの学習アルゴリズムはニューラルネットワークベースの学習アルゴリズムに比べて推定に要する時間が多くかかることが知られている[7]．そこで本研究では推定にニューラルネットワークを用いる．

異常検知に用いる機械学習アルゴリズムとして AE を用いる．この手法は学習データとして異常データを必要としない点と，未知の異常に対しても有効である点に優れている．また，機器やサービスの推定では 2 値分類ではなく多クラス分類になる点，異常データとは異なり学習データを入手しやすい点，トラフィックデータが時系列データである点から，RNN[9]や GRU[10]，LSTM[11]などの学習アルゴリズムを検討している．

RNN は再帰型ニューラルネットワークとも呼称され，時系列データなどのシーケンスデータを扱うことができるニューラルネットワークモデルの一種である．前時刻までの情報と現在のデータの２つの入力に基づいて，状態を推論することが可能である．例えばある時間tにおける入力データx_tが与えられた時の隠れ状態h_tは以下のように定義される．

$$h_t = \tanh(Wh_{t-1} + Wx_t + b)$$

ここでwは重み，bはバイアスを表すパラメータである．活性化関数に主には$tanh$が用いられており，値を-1 から+1 の範囲で正規化を行う．しかし，RNN 上で誤差を伝播していく過程で勾配が消失する勾配消失問題と，長期的な特徴を持つデータにおいて重みを大きくすべきか小さくすべきか決定することができない重み衝突問題が発生する．

これを解決したのが LSTM である．時系列データには長期的な関係性と短期的な関係性が存在するが，そのような関係性を表現するためにはどの程度過去の情報を保持するか，あるいはどの程度忘却するかを判断しなくてはならない．そこで長期的な記憶を可能にする記憶セルc_t及び忘却ゲートz_tを用いることによって勾配消失問題を解決した．また，重み衝突問題に対しては入力信号の通過具合を調整する入力ゲートi_t，出力信号の通過具合を調整する出力ゲートo_tを用意することにより解消を図った．以下に各変数の定義を示す．

$$z_t = \sigma(W_{zx}x_t + W_{zh}h_{t-1} + b_z)$$
$$i_t = \sigma(W_{ix}x_t + W_{ih}h_{t-1} + b_i)$$
$$o_t = \sigma(W_{ox}x_t + W_{oh}h_{t-1} + b_o)$$
$$c_t = z_t \odot c_{t-1} + i_t \odot tanh(W_{cx}x_t + W_{ch}h_{t-1} + b_c)$$
$$h_t = o_t \odot tanh(c_t)$$

しかし，LSTM にも計算コストが大きくなるという問題点が存在する．そこで記憶セルと隠れ状態を一つにまとめて，かつ忘却ゲートと入力ゲートを一つにまとめることによって計算コストを低減させた手法が Gated Recurrent Unit (GRU) である．以下に各変数の定義を示す．

$$r_t = \sigma\left(W_{ir}x_t + b_{ir} + W_{hr}h_{(t-1)} + b_{hr}\right)$$
$$z_t = \sigma\left(W_{iz}x_t + b_{iz} + W_{hz}h_{(t-1)} + b_{hz}\right)$$
$$n_t = \tanh\left(W_{in}x_t + b_{in} + r_t \odot \left(W_{hn}h_{(t-1)} + b_{hn}\right)\right)$$
$$h_t = (1 - z_t) \odot n_t + z_t \odot h_{(t-1)}$$

RNN ではデータは入力層，隠れ層，出力層の順で伝播されて結果が出力される．RNN では隠れ層が活性化関数 1

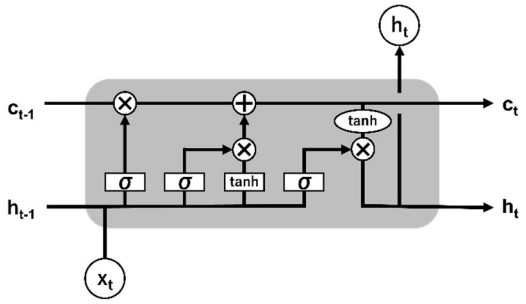

図 2　LSTM ブロックの構造

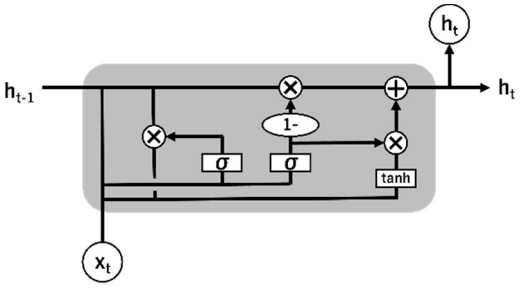

図 3　GRU ブロックの構造

つだけであるのに対し，LSTM や GRU は複数の活性化関数により複雑な演算が行われる．この演算部はブロックと呼ばれる．LSTM 及び GRU ブロックを図 2，図 3 に示す．

4. 実験・評価

4.1 実験概要

提案手法の性能を評価するために，実際にトラフィックデータを収集して，実験を行った．本稿ではトラフィックデータから利用しているサービスを推定することに着目して実験を行った．まず，実験 1 として，トラフィックデータの特徴量とサービスの相関関係を調査し，どの特徴量を利用することで，サービスの推定精度を高めることができるか検討した．次に実験 2 として，実験 1 で検討した特徴量を利用して，トラフィックデータに対してサービス推定の実験を行った．

4.2 実験環境

本研究の実験環境を図 4 に示す．トラフィックデータを収集するため，研究室内に専用ネットワークを構築して通信のログデータを収集した．本研究室のネットワークは学内プロキシを経由した通信となっている．ネットワーク上すべての機器のログデータを収集するため，ルータのポートミラーリング機能を用いて観測用 PC でトラフィックデータを収集する．ポートミラーリングとはルータなどが持つ機能の一つで，あるポートが送受信するデータを同時に別なポートに送出する機能のことである．観測用 PC では Linux を搭載しており，tcpdump を用いてすべてのパケットを収集した．収集するトラフィックデータは 1 時間おきに別のキャプチャファイルとして保存される．

サービスの推定のためのデータ収集を行い，データセットを作成した(以下，研究室データセット)．具体的にはデータ生成用の PC では一定時間ごとに PC が自動的に操作するソフトウエアを導入し，以下のサービスのトラフィックデータの収集を行った．

・**動画のストリーミング再生(streaming)**：Microsoft Edge 上で YouTube の再生を行った．

・**E メールの送信**：PC 上に Thunderbird をインストールし，研究のために作成した Gmail アカウントを用いて 5 分毎にメールの送信を行った．メールの送信には SMTP が用いられている．

・**クラウド上での文書編集**：Microsoft Teams 上に作成したテキストファイルを 1 分毎に 50 文字程度の文章を追加した．

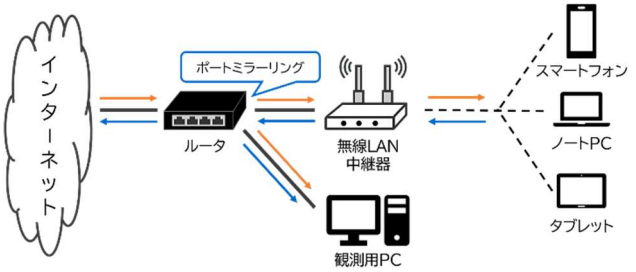

図 4　実験のネットワーク構成

・**ping 送信**：Google の DNS サーバである 8.8.8.8 に ping コマンドを実行した．実行の際には-t オプションを付加して ping を送出し続けるようにした．ping コマンドでは ICMP が用いられている．

・**ビデオ会議**：Microsoft Teams 上でカメラ及びマイクを ON にした状態で Web 会議を開いてトラフィックのキャプチャを行った．

また，収集するトラフィックデータはネットワーク利用者のプライバシ保護の観点からペイロードを含まないヘッダ情報のみを収集し，正確なトラフィックデータを収集するために，収集されるサービスのみを実行した状態で収集を行った．

4.3 実験 1: トラフィックデータの特徴量とサービスの相関関係の調査

利用サービスの推定に用いる特徴量の検討を行うために利用サービスの情報を含む 50 個の特徴量を持つデータセットを使用し，相関比を用いてトラフィックデータの各特徴量と利用サービスの相関関係を調査した．相関比とは量的データと質的データの相関を算出する統計量である．相関比は 0 から 1 の値をとり，1 に近づくほど相関関係が強く，サービス推定に有用だと考えられる．相関が認められる 0.4 を超えた特徴量は，ペイロードにより得られるデータを除く 47 項目中 16 項目であった．表 2 にその結果を示す．

特徴量の抽出で相関比が最も高かった特徴量は宛先ポート番号であったが，近年では動的ポートなどの技術によりポートベースの分類は困難になっている．また，開始時刻などの特徴量が高くなっている理由として連続したサービスの利用が考えられ，実際のサービス推定では適用されない可能性がある．一方で，これらの特徴量はネットワー

表 2　サービスとの相関比が 0.4 を超えた特徴量

特徴量	相関比
宛先ポート番号	0.935
フローの終了時刻	0.678
フローの開始時刻	0.677
順方向フローの開始時刻	0.677
送信元 IP アドレス	0.676
逆方向フローの最小パケット長	0.622
プロトコル番号	0.606
フローが終了した原因	0.548
逆方向フローの開始時刻	0.534
逆方向フローの終了時刻	0.534
逆方向フローの期間	0.513
順方向フローの終了時刻	0.513
順方向フローの期間	0.493
フローの期間	0.492
フローの最小パケット長	0.462
順方向の最小パケット長	0.452

表 3　使用した研究室データセット

サービス	形態	パケット数
streaming	動画ストリーミング	50,000
edit	クラウド文書編集	50,000
ping	ping 送信	10,228
video	ビデオ通話	50,000
mail	メール送信	24,026

表 4　使用した ISCX データセット

サービス	形態	パケット数
streaming	動画ストリーミング	39,742
audio	音楽ストリーミング	22,746
video	ビデオ通話	100,000
voip	音声通話	100,000
file	ファイル転送	65,323

クの使用時間帯であるとも言えるためユーザ推定には用いることが可能であることが考えられる．

4.4 実験 2:サービス推定の評価

4.4.1 実験内容

トラフィックデータに対して提案手法を用いたサービス推定の精度評価を行った．機械学習を行うためにクラウド上でプログラミング言語を実行することができる Google Colaboratory を利用した．ニューラルネットワークによるサービスの分類をおこなうため，機械学習モデルを作成して評価を行った．機械学習ライブラリは PyTorch1.10.2 を利用した．学習アルゴリズムとしてトラフィックデータを時系列データとして扱うことが可能である RNN，GRU 及び，LSTM を利用した．

データセットとして実際に研究室で収集された研究室データセット及び，ISCX が提供する VPN-nonVPN traffic dataset[12]を用いた．研究室データセットはおよそ 2 週間にわたり収集され，5 つのサービスの情報で構成されている．使用したデータを表 3 に示す．また VPN-nonVPN traffic dataset は一般的に使用されているサービスのトラフィックデータを生成するために Skype や Facebook などサービスからデータが収集された．データセット内には通常のセッションと VPN 経由で収集されたセッションの 2 種類のトラフィックデータが含まれるが，本研究では通常のセッションにおけるトラフィックデータのみを使用した．使用したデータを表 4 に示す．

RNN，GRU 及び LSTM の時系列シーケンスとして，トラフィックデータを時系列データとみなして，データを切り分けて入力とした．データは 0.8 の割合で学習データ，0.2 の割合でテストデータとした．さらに学習データを 0.8 の割合でトレーニングデータ，0.2 の割合で検証データとした．各アルゴリズムのレイヤー数は 2 とし，それぞれの実験で 100 エポックずつ学習を行い，評価指標として F 値 (F-measure)で評価をおこなう．定義を以下に示す．

$$F = 2 \times \frac{Recall \cdot Precision}{Recall+Precis}$$

このうち$Recall$は感度とも呼ばれ，実際に正であるデータのうち，正であると予測された者の割合を表す．一方$Precision$は適合率と呼ばれ，正と予測したデータのうち，実際に正であるものの割合を表す．F 値はこれらの値の調和平均であるため，バランス良くモデルの性能評価を行うことが可能である．

4.4.2 データの正規化

実験で使用する特徴量は，その分布に大きな差がある．これをそのまま機械学習に用いると分類の際に値の大きな特徴量の影響が大きくなってしまう．そのためデータを正規化して 0 から 1 の範囲に収まるように処理を施す．本研究では MinMaxScaler を用いた．

$$x_{norm,i} = \frac{x_i - x_{min}}{x_{max} - x_{min}}$$

ここでx_{norm}は正規化されたデータ，x_{min}はデータの最小値，x_{max}はデータの最大値を表す．

4.4.3 損失関数

機械学習を行うためには，分類モデルがどの程度の精度を持っているのかを評価するための指標が必要になる．本研究では損失関数として，分類問題に広く使用される交差エントロピー誤差を用いた．

4.4.4 最適化手法

ニューラルネットワークで精度を向上させるためには損失関数の値を最小化する必要がある．そこで重みやバイアスを調整することによって，損失関数を最小化する手法が最適か手法である．本研究では最適化手法として Adam [13]を使用した．

4.4.5 実験結果

研究室データセットおよび ISCX データセットに対して RNN，GRU，LSTM のそれぞれの手法を用いてサービスの推定を行った．各サービスに対する予測した結果を表 5，表 6 に示す．時系列シーケンスとして 10 個に切り分けて

表 5　研究室データセットに対する評価

	streaming	edit	ping	video	mail
RNN	0.9692	0.9953	**1.0000**	0.9696	0.8817
GRU	**0.9805**	**0.9984**	0.9976	**0.9815**	**0.9255**
LSTM	0.9682	0.9963	0.9930	0.9750	0.8900

表 6　ISCX データセットに対する評価

	streaming	audio	voip	video	file
RNN	0.9544	0.9161	0.9985	0.9977	0.9917
GRU	**0.9630**	**0.9326**	**0.9995**	**0.9979**	**0.9981**
LSTM	0.9509	0.9097	**0.9995**	0.9974	0.9947

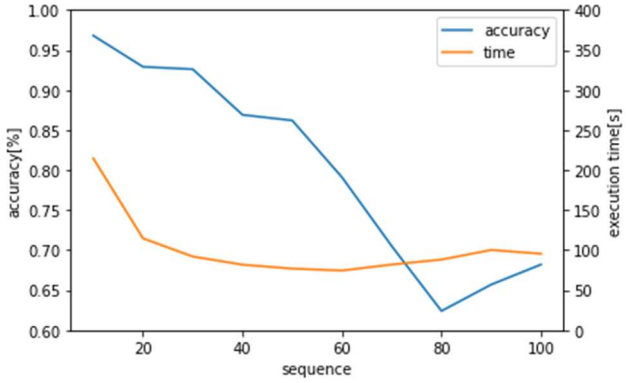

図 5　RNN のシーケンスごとの精度と時間の変化

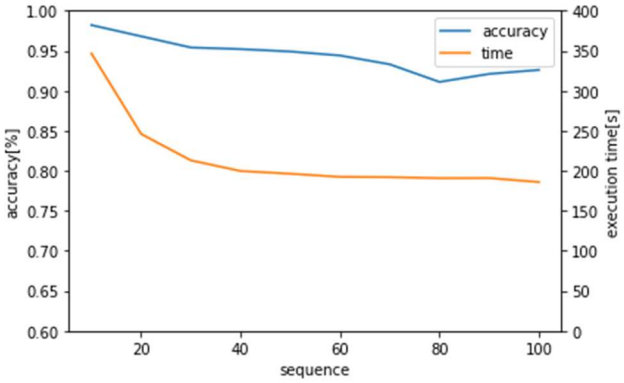

図 6　GRU のシーケンスごとの精度と時間の変化

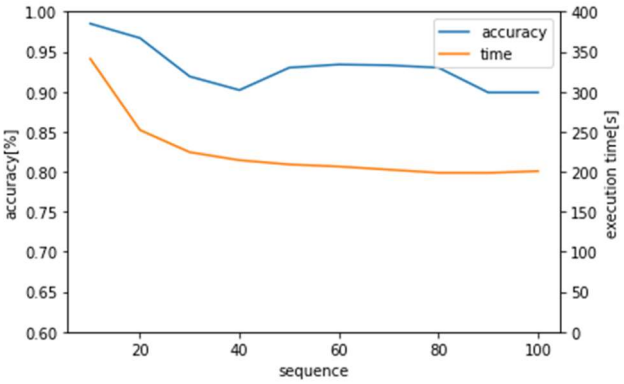

図 7　LSTM のシーケンスごとの精度と時間の変化

入力した．研究室データセット，ISCX データセット共に GRU が最も性能が高かった．

次に入力するシーケンス数の違いによる精度と実行時間の変化を調査した．各学習アルゴリズムを用い，シーケンス数を 10~100 の間で変化させて実験を行った．使用するデータセットは研究室データセットを用いた．

結果として，すべての学習アルゴリズムでシーケンス数を増加させると精度及び実行時間ともに低下することが確認された．特に実行時間は 20 シーケンスまでは急激に低下していたが，それ以降はほぼ変わらない値となった．GRU と LSTM は精度，実行時間ともにあまり変わらない結果となった．

5. おわりに

本研究では，ネットワークの状態の把握を容易にすることでネットワーク管理者の負担を軽減することを目的とし，ニューラルネットワークを用いたネットワーク状態の推定手法を提案した．実験結果として GRU を用いたモデルが最も高い精度で分類が可能であった．

今後は，異常検知を行うための AE の実装や，CNN などの他のニューラルネットワークを実装し，性能比較などを行う．また，トラフィックデータの収集も継続して行い，現在使用している機器以外にも IoT 機器のような様々な機器の通信トラフィック及び，他のサービスや操作の内容を変えて実環境を想定したデータを収集する．さらに，利用しているユーザや利用機器の推定を行う．

参考文献.

[1] 総務省:IoT デバイスの急速な普及.令和 3 年度版情報通信白書〈https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd105220.html〉(参照 2022-07-09)
[2] http archive:Report: State of the Web.〈https://httparchive.org/reports/state-of-the-web#pctHttps〉(参照 2022-07-09)
[3] IPA:ネットワーク管理に関する知識. OSS モデルカリキュラムの学習ガイダンス〈https://www.ipa.go.jp/files/000056032.pdf〉(参照 2022-07-20)
[4] Geoffrey E., et al.: Reducing the Dimensionality of Data with Neural Networks, Science 313 (5786): pp.504-507(2006)
[5] Ly Vu, et al.: Deep Transfer Learning for IoT Attack Detection, IEEE Access, Vol. 8, pp.107335-107344 (2020)
[6] Meidan Y., et al.: N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders, IEEE Pervasive Computing, vol. 17, no. 3, pp. 12-22 (2018)
[7] Wu Z., et al.: Online Multimedia Traffic Classification From the QoS Perspective Using Deep Learning, Computer Networks, Vol. 204, No. 26 (2022)
[8] 宮本大輔:探索データ解析を目指すトラフィック解析についての一検討, 情報処理学会研究報告, Vol.2018-DPS-174, No.2 (2018)
[9] Elman J. L.: Finding Structure in Time, Cognitive Science, Vol.14, No.2, pp.179-211 (1990)
[10] Cho K, et al.: On the Properties of Neural Machine Translation: Encoder-Decoder Approaches, Eighth Workshop on Syntax, Semantics and Structure in Statistical Translation (2014)
[11] Gers F.A., et al.; Learning to Forget: Continual Prediction with LSTM, 1999 Ninth International Conference on Artificial Neural Networks ICANN 99, pp.850-855 (1999)
[12] Gil G. D. et al.: Characterization of Encrypted and VPN Traffic Using Time-Related Features, the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016), pp. 407-414 (2016)
[13] Diederik P, et al.: A Method for Stochastic Optimization, the 3rd International Conference for Learning Representations (ICLR 2015) (2015)