社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

互いのプライバシ情報を共有せず ユーザの行動情報を相互利用するためのフレームワーク

山内　雅明† 　大下　裕一† 　村田　正幸†

† 大阪大学 大学院情報科学研究科 〒 565-0871 大阪府吹田市山田丘 1-5
E-mail: †{m-yamauchi,y-ohsita,murata}@ist.osaka-u.ac.jp

あらまし　ネットワーク経由で操作可能なホーム IoT 機器の普及に伴い、IoT 機器を対象としたサイバー攻撃も増加している。特に、攻撃者が家庭内の IoT 機器を不正に操作するといった攻撃は、生命の危機に直結する可能性があり、重大な問題となっている。このような不正操作攻撃に対して、ユーザの普段の行動を学習することで、検出する手法が考案されている。しかし、このような手法は、十分な学習データを長期間にわたって収集する必要があり、学習が十分に行われるまでの期間は、多量の誤検出を生じる可能性がある。そのような学習データの不足に対して、似たような行動をとりうる他家庭で収集されたデータを使う方法が効果的であると考えられる。しかし、複数の家庭から全ての行動データを収集して、その中から当該家庭と類似した行動をとるかどうかを判断するような方法には、個人情報が漏洩するといったリスクが存在する。そこで本研究では、各家庭での行動データを外部に送信せずに、似た行動をとる家庭の行動データのみを利用するためのフレームワークを提案する。本フレームワークでは、各家庭に行動を学習し、不正操作を検出するエージェントを設置する。各エージェントは、自家庭のユーザと似た行動に関する情報を保持し、同様の情報を保持するエージェント同士の情報を利用することで、似た行動をとるユーザのデータを利用する。
キーワード　異常検知、IoT、セキュリティ、フレームワーク、行動学習、スマートホーム

Framework to Utilize Others' Behavior without Sharing Privacy Information

Masaaki YAMAUCHI†, Yuichi OHSITA†, and Masayuki MURATA†

† Graduate School of Information Science and Technology, Osaka University
Yamadaoka 1-5, Suita, Osaka, 565-0871 Japan
E-mail: †{m-yamauchi,y-ohsita,murata}@ist.osaka-u.ac.jp

Abstract　A cyberattack to operate home IoT devices by attackers is a serious problem, which may damage the users. We have proposed a method to detect anomalous operations of home IoT devices by learning the users daily-life behaviors. However, the method needs to collect sufficient amount of users' behavior dataset. Before sufficient amount of dataset is collected, the method misdetects many legitimate operations. One approach to avoiding such misdetections is to use dataset collected in the other users' homes that have similar lifestyle. But, users do not want to share their private information. In this paper, we propose a framework to utilize the similar users' behavior data without sharing their private data. In this framework, each home has an agent to learn their behaviors and detect anomalous operations. When detecting anomalous operations, each agent cooperate with each other without sharing their private information.
Key words　Anomaly Detection, IoT, Security, Framework, Learning Behavior, Smart Home

1. はじめに

近年、パソコンやスマートフォンのみならず、冷蔵庫やエアコンといった日常生活で使用する様々な機器がインターネットに接続するようになっている。これらの、ネットワークに接続するデバイスは、IoT(Internet of Things) 機器と呼ばれており、ユーザはスマートフォンやタブレットなどを使って、IoT 機器の稼働状況や周辺状況を調べたり、IoT 機器を操作したりすることができ、その利便性から、現在も普及が進んでいる。

このような IoT 機器が増えるにつれ、それらの機器を狙ったサイバー攻撃を受けるリスク [1–4] や、スマートホームにおけるセキュリティリスク [5, 6] が増加する。すでに家庭内の IoT

機器を狙った攻撃は多く観測されており、IoT 機器を狙ったマルウェアも出現している [7,8]。また現在、IoT 機器を対象にした攻撃は、IoT 機器に侵入し、botnet を構築することで、DDoS 攻撃の踏み台として利用するものが主である [9,10]。

しかし、IoT 機器は現実の生活と密接に関係する機器であることから、IoT 機器の不正操作には、現実の生活に大きな影響を及ぼすような、従来の PC やスマートフォン等を対象とした攻撃とは異なる種類の攻撃を受けるリスクがある [11]。特に、ユーザの意図とは異なる動作を機器にさせる攻撃は、ユーザの不安感をあおるだけではなく、空調の設定温度を勝手に操作したり、ヘルスケア機器の設定を変更したり、人命に直結するような被害も考えられる。また、高電力の IoT 家電の電源が一斉に操作されることで、電力需要が大きく変動し、大規模な停電を引き起こすといったよう被害も考えられており、電力ネットワークなどの、他のインフラネットワークに対しても影響を与えることが考えられる [12]。そのため、IoT 機器の不正操作の防止は重要な課題となっている。

そのようなホーム IoT 機器への不正操作攻撃に対して、我々は、ユーザの行動を学習して検出する手法を提案した [13]。この手法では、IoT 機器の操作や、ユーザの入退室といった宅内で観測されるイベントの順序と、機器操作が行われた時間帯や気温、湿度といった宅内の状況を、ユーザの行動として学習する。学習後、宅内で行われた機器操作が、学習された行動と一致していれば、当該操作を正常操作であると判断し、そうでない場合は、不正操作として検出することで、誤検知を 20%以下に抑えて、95–100%の不正操作を検知することができている。一方で、この手法の問題点として、ユーザの行動に関するデータが十分に得られていない場合には、検知精度が大きく低下することが挙げられている。具体的には、ユーザの行動データ数が不足している場合や、特定の機器に関する機器操作回数が少ないような場合には、正常な行動パターンを学習することができず、多量の誤検知を生じてしまう。

この手法では、誤検出を防ぐために、正当なユーザーの行動に関する十分な量のデータが必要だが、各家庭で取得できるデータは限られている。このような、学習データの不足に対する一つのアプローチとして、クラウドなどに全てのユーザの行動データを収集し、一般的な行動パターンを解析するような方法も考えられるが、ユーザごとに異なる趣味、嗜好を持っており、そのようなユーザの行動様式に合わせた行動パターンを解析することは難しい。そこで、別のアプローチとして、自分以外の、似た行動様式をとるようなユーザのデータを利用するような方法が考えられる。ただし、類似した家庭の行動情報を利用するにあたり、類似した家庭かどうかを判定するために、各家庭における機器操作や入退室に関する情報や、家庭内のユーザ自身の属性に関する情報を直接やりとりすることは、プライバシの観点から好ましくない。また、クラウドなどデータを一か所に収集した場合においても、クラウド上のデータが攻撃者による不正アクセスによって流出するといった事件 [14] が実際に発生していることから、各ユーザの行動履歴や、各ユーザの行動データから学習された行動モデルといったデータが、意図せず流出してしまい、ユーザのプライバシを著しく侵害する可能性が考えられる。さらに、このような情報が流出し、どの家庭でどのような行動が行われているかという情報が第三者に知られることは、攻撃者が攻撃を行う際のヒントとなる情報となりうることから、セキュリティ上のリスクとなる可能性がある。このようなリスクから、外部に自身のプライバシ情報を含むような行動データを送信することなく、他家庭のデータを利用する方法が必要である。

そこで本研究では、個人情報を共有することなく、似た行動様式のユーザのデータを活用するためのフレームワークを提案する。このフレームワークでは、各家庭においてユーザの行動を学習して不正な操作を検出するエージェントが設置されており、各エージェントが、似た行動情報を保存している他のエージェントと協力することにより、データの不足による正常操作の誤検出を減らすことができる。また、その際、Tor [15] などの匿名で通信する方法を用いて、協力しているエージェントと、エージェントが設置されている家庭がリンクできないようになっている。

本稿の構成は以下の通りである。まず、関連研究について第 2. 章で説明する。次に、第 3. 章で、本フレームワークにおいて解決すべき課題を述べる。その後、行動情報を外部に送信せずに、類似した他家庭と協力して異常検知を行うためのフレームワークについて、第 4. 章で説明する。最後に、本稿のまとめと今後の課題を第 5. 章で述べる。

2. 関 連 研 究

2.1 宅内の行動パターンを基にした IoT 異常検知手法

宅内に設置されているホーム IoT 機器を第三者が不正に操作する攻撃に対して、宅内のユーザの行動情報をもとに検出する手法が提案されている [13]。この手法では、家庭内のすべてのホーム IoT 機器が接続しているホームゲートウェイにおいて、検知を行う。ホームゲートウェイは、家庭内のホーム IoT 機器の他、家庭内に配置されたセンサやスマートフォンとも接続しているため、時間帯、室温、湿度といったセンサから得られる環境情報や、スマートフォンの接続・離脱といった情報からユーザの在・不在といった情報を把握することができる [16]。ホームゲートウェイにおいて、まず、時刻やセンサの観測内容をもとに、宅内の状況を分類する。そして、各状況において、発生した機器操作およびユーザの入退室の順序を学習する。新たな機器操作が発生した場合は、現在の宅内の状況に対応する、学習されたイベントの順序を確認し、発生した機器操作が学習されたイベントの順序と異なる場合に異常として検出する。

この異常検知手法の評価にあたり、研究室内にホーム IoT 機器を複数台設置して仮想ホームネットワーク環境を構築し、4 名の被験者に、設置したホーム IoT 機器を利用しながら普段通りの生活を 1 か月間行ってもらい、ホームネットワーク内に発生するパケットを観測、機器操作が発生するタイミングを記録している。そして、このデータをもとに提案手法の学習を行い、不正操作が混入した際に検出できるかの検証を行っている。

その結果、当該操作に関するイベントの順序を観測できた機

器に関しては、95–100%の不正操作を検知することができている。しかし、イベントの順序を観測できなかった機器操作 (単発操作) や、学習データ数が少ない機器の操作、学習が不十分あまり頻繁に行われないレアな機器操作に関しては、誤検出されていることが報告されている。

2.2 送信元の秘匿化技術

各家庭のエージェント間が通信を行う際に、エージェントの送信元情報を隠す必要がある。このような送信元の秘匿化技術として、Tor [15] を用いることを考えている。Tor は、代表的な匿名通信のサービスの一つである。Tor ネットワークを介して通信を行うことで、送信元の IP アドレスを通信相手に知られることなく通信を行うことができるというものである。送信する IP アドレスのみを秘匿化し、通信するデータ自体は暗号化しない。本フレームワークにおいては、データ部を暗号化する必要がないことから、Tor を利用して匿名通信を行うことを前提としている。

3. 要　　件

本フレームワークは、スマートホーム内の行動情報に基づくホーム IoT 機器に対する不正操作の検出を行うエージェントが、学習が十分に行われなかった際に、互いに協力することで、検知精度を向上させることを目指している。各家庭内に配置されたエージェントが、スマートホーム内のユーザの正常な行動を学習し、その行動から外れた機器操作を、不正操作として検出する。ユーザの行動を学習するのに十分なデータが得られない場合、正常な行動を正常であると判断できず、正常な操作の誤検出が多発してしまう。多量の誤検出を避けるため、他の家庭における行動データを利用する方法が考えられるが、その際、以下のような条件を満たす必要がある。

3.1 行動履歴などの個人に関する情報を外部に送信せずに協力

他の家庭における行動データを利用するにあたり、ユーザの行動履歴を全て共有することや、性別や職業といったパーソナルな情報を共有することは、個人に関する情報が漏洩するリスクがある。例えば、各ユーザがクラウドに全ての行動履歴を収集し、解析を行うような方法には、クラウドからデータが流出することで、攻撃者にヒントとなる情報を与える危険性が存在する。そのため、行動履歴などの個人に関する情報を外部に送信することなく、他家庭のデータを利用する方法が必要である。

3.2 似た行動をとるユーザが存在する家庭のエージェントとのみ協力

本フレームワークでは、行動履歴などの個人に関わる情報を外部に送信しない一方で、自身と似た行動をとるユーザのエージェントと協力する必要がある。他家庭と協力することで、誤検出が減少する一方で、全ての家庭のデータを利用してしまうと、実際には当該家庭内で行われないような行動まで正常であると判定されてしまい、不正操作の検出率が低下する恐れがある。そこで、検出率の低下を抑えつつ、誤検出を減らすために、行動履歴などの情報を外部に送信しない状況下で、似た行動をとる家庭のエージェントのみと協力する手法を考案する。

4. 互いのプライバシ情報を共有せずユーザの行動情報を相互利用するためのフレームワーク

4.1 概　　要

本フレームワークの全体像を、図 1 に示した。各家庭には、宅内のユーザの行動を学習して不正操作を検出するための「異常検知エージェント」が配置されている。各異常検知エージェントは、「識別子のデータベース」を保持しており、エージェントが送受信する「判定依頼」に付与された識別子に関する情報が保存される。また、「匿名通信ネットワーク」は、Tor [15] などを用いて送信者の IP アドレスを隠した状態で判定依頼をやりとりするものである。

本フレームワークは、学習データの不足によって正常かどうか判断できないような機器操作が行われた家庭におけるエージェントが、送信者が誰かという情報を秘匿化し、当該機器操作に関する情報を判定依頼として送信することで、他家庭のエージェントから当該機器操作の正常／異常の回答を得ることで、他家庭のデータを利用して異常検知を行うためのものである。まず、判定を依頼する家庭のエージェントが、正常かどうか判断できない機器操作に関する情報を、判定依頼として匿名のネットワークに送信する。似た行動をとる家庭のエージェントは、判定依頼に含まれる機器操作が、自身のもつ学習モデルによって、正常と判定される場合は「正」、異常と判定される場合は「誤」、学習データの不足などによって判定できない場合は「不明」と、匿名で返信する。また、似た行動をとらない家庭のエージェントは、判定を行わない。これらの返信結果をもとに、判定を依頼した家庭のエージェントは、当該操作が正常

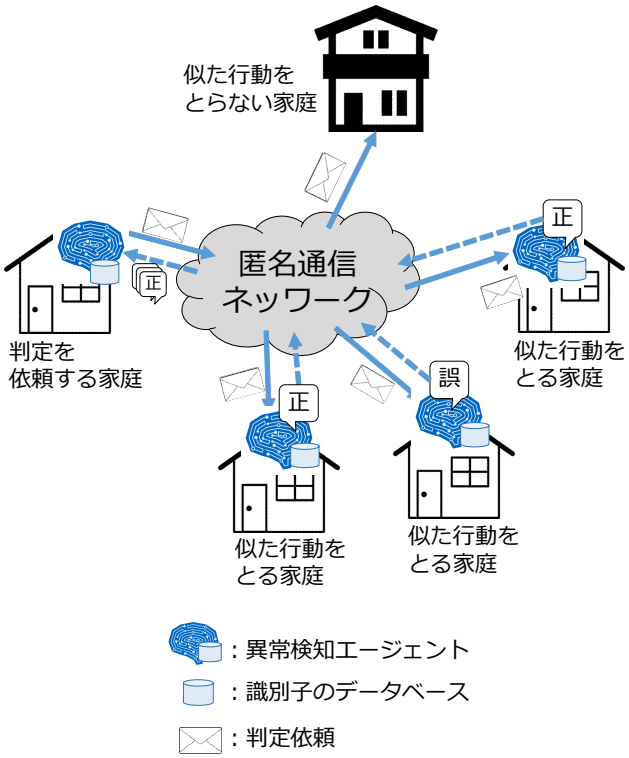

図 1: フレームワークの概要

か異常かの判断を行う。

また、似た家庭かどうかを判断するための方法として、まず、判定を依頼する家庭のエージェントは、判定依頼を送信する際に、判定依頼に対して識別子を割り当てて送信する。また、似た行動をとる家庭のエージェントが、判定依頼に含まれる機器操作が正常であると判断されて「正」と回答した場合、当該判定依頼の識別子を、当該エージェントのデータベースに保存する。それによって、同じ行動情報を正常であると判定した家庭のエージェント同士が、同一の識別子を保存することになる。この、同一の識別子を保持する家庭のエージェント同士を、似た行動をとる家庭とする。その後、判定依頼を送信する際に、判定を依頼する家庭のエージェントの識別子データベースに保存されている識別子から、複数の識別子を取り出し、判定依頼の中に含める。同一の識別子を保持するエージェントからのみ回答を得ることで、行動履歴や個人の情報を共有せず、似た家庭のエージェントと協力することができる。

4.2 判定を依頼する家庭における動作手順

判定を依頼するエージェントは、自家庭で行われた機器操作が、自家庭のデータを用いても正常か異常かを判定できない場合に、他家庭に対して判定依頼を送信し、その回答結果をもとに判断を行う。その動作手順を、図 2 に示した。まず、家庭内で機器操作が発生した場合、当該操作が正常な操作か不正な操作かを、異常検知を行うエージェントに送信する。異常検知エージェントは、当該操作が正常かどうかを自家庭のデータを用いて判断する。自家庭のデータにおいて判断が可能な場合は、本フレームワークを利用せず、家庭内で正常／異常を決定し、異常であれば機器操作の通信をドロップしてユーザに通知する。自家庭のデータから判断が出来ない場合は、識別子のデータベースから複数の識別子を取り出し、行動情報とともに判定依頼として作成して、識別子を割り当ててから、匿名の通信ネットワークを介して、他家庭にブロードキャストする。送信した依頼に対する回答を受信後、「正」の回答数をもとに、当該操作の正常／異常を決定し、異常であればユーザに通知する。

判定を依頼する家庭では、判定を依頼したい機器操作に関する行動情報と、以前に正常であると判定した判定依頼の識別子を外部に送信するが、Tor [15] 等を用いた匿名通信ネットワークを介することで、送信者情報を秘匿化するため、機器操作を含む行動内容と、判定を依頼した家庭のユーザ自身が紐づかないため、依頼者の行動や普段行うような行動が他人に知られることはない。また、ダミーの判定依頼を送信することで、判定依頼に含まれている行動情報が、実際に行われた行動かどうか、という情報を隠す方法も考えられる。さらに、判定依頼に含まれる行動情報についても、一部の情報にノイズを与えることで、判定依頼に含まれる行動の情報自体も隠す方法も考えられる。例えば、実際に操作が行われた時刻に対してノイズを与えて操作時刻をずらすことで、実際に機器操作が行われた時間を特定されないようにすることも考えられる。

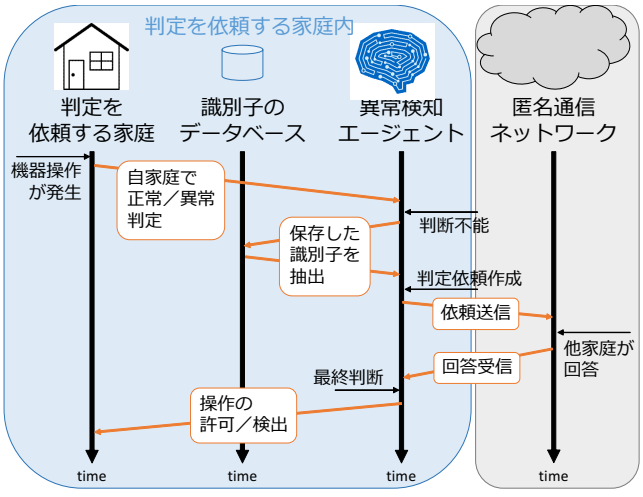

図 2: 判定を依頼する家庭における動作手順

4.3 判定に協力する家庭における動作手順

判定依頼を受け取ったエージェントは、当該判定依頼がまず、自家庭の行動と類似した家庭から送られたものかどうかを判定し、似た家庭であれば自家庭の学習モデルを用いて正常／異常の判定を行い、判定結果を回答する。図 3 に、判定依頼を受け取った家庭のエージェントの動作をフローチャートとして示した。判定依頼に含まれている複数の識別子が、自身の識別子データベースにも含まれているかどうかを判断し、識別子が含まれている場合は、回答を行い、含まれていない場合は、回答せずに処理を終了する。

回答を行う家庭は、図 4 にも示した通り、自身の学習モデルを用いて、当該判定依頼に含まれる行動の正常／異常を判定し、正常と判定されれば「正」と匿名で回答した後に、当該判定依頼の識別子をエージェントの識別子データベースに保存し、異

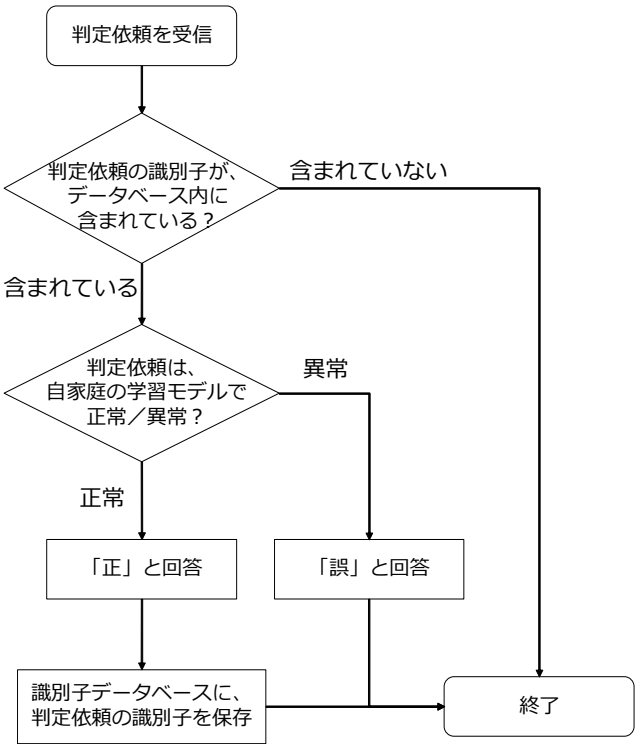

図 3: 判定依頼を受け取った家庭における動作のフローチャート

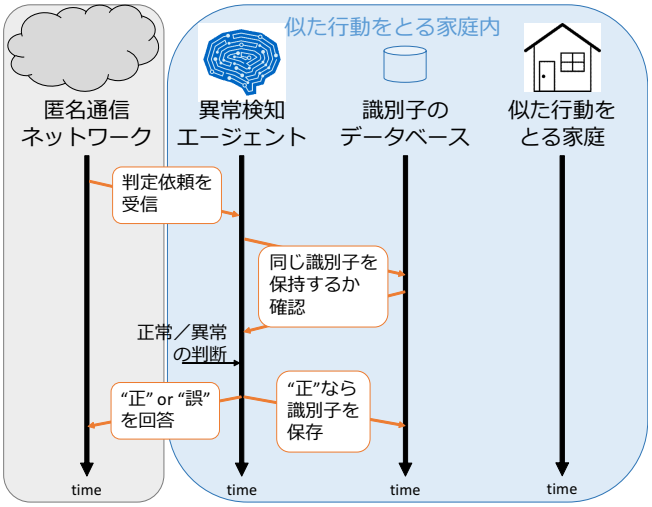

図 4: 判定依頼に回答する、似た家庭における動作手順

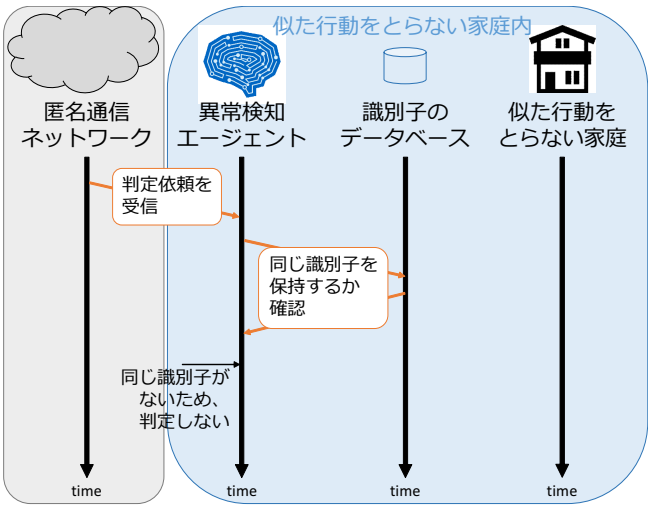

図 5: 判定依頼に回答しない、似た行動をとらない家庭における動作手順

常と判定されれば「誤」と匿名で回答し、識別子は保存しない。また、データ不足により、判定が困難な場合は、「不明」と匿名で回答し、識別子は保存しない。また、回答を行わない家庭では、図 5 に示した通り、回答自体を行わずに処理を終了する。

判定を依頼された家庭においては、判定依頼に対して、Tor [15] 等を用いた匿名通信ネットワークを介して回答を行うため、「正」「誤」「不明」の回答内容と、誰が回答を行ったかという情報がリンクされず、回答した家庭が行う行動の情報が知られることはない。また、回答を行っていない家庭においても、回答の送信者が特定されず、誰が回答を行っていないか分からないことから、回答しなかった家庭において行われないような行動の情報が知られることはない。

5. おわりに

本稿では、各家庭で異常検知を行うエージェントが、学習が不十分な場合に、行動履歴などの情報をできるかぎり共有せず、似た行動をとるユーザのエージェントと協力して異常検知を行うためのフレームワークを考案した。本フレームワークでは、自家庭と似た行動を含む判定依頼の識別子を保存し、同じ識別子を保持するエージェントと協力することによって、行動履歴などの個人に関する情報を共有せず、似た行動をとるユーザのエージェントと協力して異常検知を行うことを可能としている。

今後は、本フレームワークを実装し、異常検知手法 [13] と同様の評価環境において、 1 つの家庭のデータのみを用いた場合の検知精度、全家庭のデータを用いて評価を行った場合の検知精度と比較し、評価を行う予定である。加えて、家庭数の増減による検知精度の変化についても評価を行う予定である。

さらに、本フレームワークは、積極的に攻撃を行おうとする攻撃者がいないということを想定し、そのうえで個人に関わる情報を外部に送出しないモデルとなっている。フレームワークの参加者に攻撃者が存在した場合など、フレームワークに対する攻撃への対策についても検討する予定である。

文　献

[1] I. Lee and K. Lee, “The Internet of Things (IoT): Applications, investments, and challenges for enterprises,” Business Horizons, vol.58, no.4, pp.431–440, July 2015.

[2] M.U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, “A critical analysis on the security concerns of internet of things (IoT),” International Journal of Computer Applications, vol.111, no.7, pp.1–6, Feb. 2015.

[3] B.L.R. Stojkoska and K.V. Trivodaliev, “A review of Internet of Things for smart home: Challenges and solutions,” Journal of Cleaner Production, vol.140, no.3, pp.1454–1464, Jan. 2017.

[4] M. Capellupo, J. Liranzo, M.Z.A. Bhuiyan, T. Hayajneh, and G. Wang, “Security and Attack Vector Analysis of IoT Devices,” Proceedings of International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, vol.10658, pp.593–606, Springer International Publishing, Dec. 2017.

[5] D.K. Madhugundu, F. Ahmed, and B. Roy, “A survey on security issues and challenges in iot based smart home,” Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018., pp.423–427, 2018.

[6] V. Moustaka, Z. Theodosiou, A. Vakali, and A. Kounoudes, “Smart Cities at Risk!: Privacy and Security Borderlines from Social Networking in Cities,” Proceedings of AW4City 2018: 4th International Smart City Workshop, pp.905–910, April 2018.

[7] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J.A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, “Understanding the Mirai Botnet,” Proceedings of the 26th USENIX Security Symposium, pp.1093–1110, USENIX Association, Vancouver, BC, Aug. 2017.

[8] D. Palmer, “120,000 IoT cameras vulnerable to new Persirai botnet say researchers,” https://www.zdnet.com/article/120000-iot-cameras-vulnerable-to-new-persirai-botnet-say-researchers/, May 2017.

[9] Y.M.P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, “IoTPOT: A Novel Honeypot for Revealing Current IoT Threats,” Journal of Information Processing, vol.24, no.3, pp.522–533, May 2016.

[10] M. Lyu, D. Sherratt, A. Sivanathan, H.H. Gharakheili, A. Radford, and V. Sivaraman, “Quantifying the Reflective DDoS Attack Capability of Household IoT Devices,” Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp.46–51, WiSec ’17,

ACM, New York, NY, USA, July 2017.

[11] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," IEEE Communications Surveys Tutorials, vol.16, no.4, pp.1933–1954, April 2014.

[12] S. Soltan, P. Mittal, and H.V. Poor, "BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid," Proceedings of 27th USENIX Security Symposium (USENIX Security 18), pp.15–32, USENIX Association, Baltimore, MD, Aug. 2018.

[13] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, "Anomaly Detection for Smart Home IoT Based on Users' Behavior," Proceedings of 2019 IEEE International Conference on Consumer Electronics (ICCE), pp.1–6, Las Vegas, Nevada., Jan. 2019.

[14] "Seattle tech worker arrested for data theft involving large financial services company |usao-wdwa |department of justice". accessed: 2020-2-13. https://www.justice.gov/usao-wdwa/pr/seattle-tech-worker-arrested-data-theft-involving-large-financial-services-company

[15] "Tor project |anonymity online". accessed: 2020-2-9. https://www.torproject.org/

[16] N. Apthorpe, D. Reisman, and N. Feamster, "A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic," arXiv preprint arXiv:1705.06805, pp.1–6, May 2017.