[招待講演] スマートホームにおけるユーザ行動の学習に基づく異常検知手法

–ICCE2019 報告–

山内　雅明† 　大下　裕一† 　村田　正幸† 　上田　健介†† 　加藤　嘉明†††

† 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
†† 三菱電機株式会社 先端技術総合研究所 〒 661-0001 兵庫県尼崎市塚口本町 8-1-1
††† 三菱電機株式会社 情報技術総合研究所 〒 247-8501 神奈川県鎌倉市大船 5 丁目 1 番 1 号
E-mail: †{m-yamauchi,y-ohsita,murata}@ist.osaka-u.ac.jp, ††Ueda.Kensuke@ce.MitsubishiElectric.co.jp,
†††Kato.Yoshiaki@dh.MitsubishiElectric.co.jp

あらまし　近年、家電のような機器までネットワークに接続されるようになり、それらの機器を対象とした不正操作のリスクが高まっている。しかし、このような機器の不正操作に用いられる通信は、既知の不正パケットとのパターンマッチング等の従来の攻撃検出手法での検知が困難である。そこで本研究では、ホームネットワーク接続機器への不正操作を検出する新たな手法を考案した。この手法では、時刻やセンサ等で観測された温度等の環境ごとに、ユーザが機器操作を行う順を行動パターンとして学習する。そして、機器操作が行われた際には、学習されたその環境下での機器操作の順と照合し、不一致であれば不正操作と検出する。本稿では、研究室内で収集した被験者の行動パターンをもとに、提案手法を評価し、検知精度および制約について考察した。
キーワード　異常検知, IoT, セキュリティ, スマートホーム, 行動パターン, 不正操作攻撃

[Invited Talk] Anomaly Detection for Smart Home Based on User Behavior

–ICCE2019 Report–

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

Kensuke UEDA††, and Yoshiaki KATO†††

† Graduate School of Information Science and Technology, Osaka University
Yamadaoka 1-5, Suita, Osaka, 565-0871 Japan
†† Mitsubishi Electric Corporation Advanced Technology R&D Center
8-1-1 Tsukaguchi-Honmachi Amagasaki City Hyogo 661-0001, Japan
††† Mitsubishi Electric Corporation Information Technology R&D Center
5-1-1 Ofuna Kamakura City Kanagawa 247-8501, Japan
E-mail: †{m-yamauchi,y-ohsita,murata}@ist.osaka-u.ac.jp, ††Ueda.Kensuke@ce.MitsubishiElectric.co.jp,
†††Kato.Yoshiaki@dh.MitsubishiElectric.co.jp

Abstract　The operations of home IoT devices by attackers can cause serious problems. However, such attacks are difficult to detect. In this paper, we propose a method to detect such attacks based on user behavior. We model user behavior as a sequence of events. Our method learns sequences of events for each one of a predefined set of conditions and detects attacks by comparing the sequences of the events including the current operation with the learned sequences. We evaluate our method by using data collected by monitoring the behavior of four users. Based on the results of this evaluation, we demonstrate the accuracy of our method and discuss the limitations of our method.
Key words　Anomaly Detection, IoT, Security, Smart Home, Behavior Pattern, Operation by Attackers

1. はじめに

近年、パソコンやスマートフォンのみならず、冷蔵庫やエアコンなどの家電やペースメーカなどのヘルスケア機器が、IoT 機器として、インターネットに接続するようになっている。ユーザはスマートフォンやタブレットに加えて、Google Home [1] や Amazon Echo [2] といった AI スピーカなどを使って、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る。

しかし、インターネットに接続する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も高まっており [3–6]、実際に、IoT 機器を狙った攻撃やマルウェア [7,8] が観測されている。また、現在発生している IoT 機器を標的とした攻撃のほとんどは、IoT 機器に侵入し、ボットネットを構築することで、DoS 攻撃などの踏み台として利用するものである [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、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、攻撃者によって IoT 機器が操作されるような、IoT 機器の不正操作攻撃は、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と、人命に直結するような攻撃も考えられる。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。

従来、ネットワークを介したサイバー攻撃に対して、セキュリティソフトや IDS(Intrusion Detection Systems) の導入による対策が取られてきた。セキュリティソフトや IDS では、通信パケットを事前定義されたルールを比較する、パターンマッチングによって攻撃を検出してきた。しかしながら、IoT 機器に対する不正操作時の通信パケットは、ユーザが機器操作を行う際と同じ正常なプロトコルに従った通信であるため、パケット発生パターンの特徴や通信手順からは不正操作の検出は困難である。特に、攻撃者が、正規のユーザのスマートフォンや AI スピーカに侵入し、侵入端末を介してパケットを送信した場合、そのパケットを正規のユーザーが送信したパケットと区別することは困難である。

そこで本研究では、ホームネットワークと宅外のネットワーク間のすべてのパケットを監視することができるホームゲートウェイにおいて、ホーム IoT 機器の不正操作を検出する手法を提案する。提案手法では、ゲートウェイが、時刻や宅内のセンサの観測値などをもとに、宅内の状況を分類し、各状況において、発生した機器操作や、ユーザの入退室といったユーザの行動順序を学習する。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。

評価のために、家庭用 IoT デバイスを複数設置し、研究室内にホームネットワークを構築した。研究室内の 4 人の学生を被験者として選択し、設置した IoT 機器を数か月間使用してもらった。その際、ホームネットワーク上を流れるパケットを観測し、IoT 機器の操作が行われた時間を記録した。このようにして得られたデータのうち、記録された IoT 機器の操作を正常な操作とし、当該データに不正操作を混入した際に、本手法によって当該操作が検出可能かどうかを評価した。

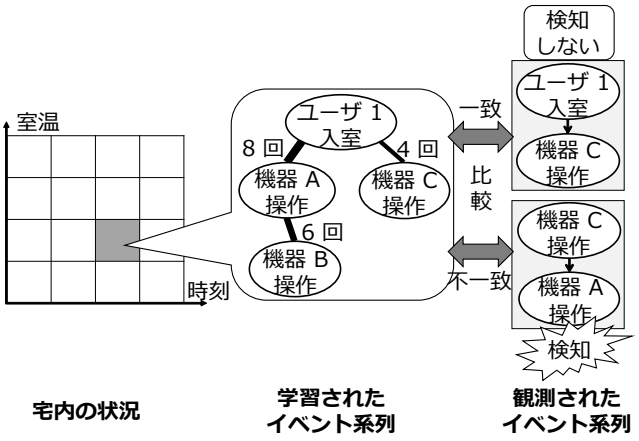

図 1: 異常検知モデルの概要図

本稿の構成は以下の通りである。まずホーム IoT 機器の不正操作を検知するための提案手法の内容について第 2. 章で説明し、パラメータ設定手法について第 3. 章で説明する。次に第 4. 章で提案手法の評価について述べる。最後に、本稿のまとめと今後の課題を第 5. 章で述べる。

2. スマートホーム IoT 機器の異常検知

本章では、攻撃者によるホーム IoT 機器の不正操作を検知する手法を提案する。各家庭において、各ユーザは状況に応じて、自身の行動パターンが存在する。例えば、帰宅時に室温が低ければ、ヒータをつけ、加湿器をつけるといった行動をとるが、室温が高い場合には、ヒータをつけることはない。また、機器を操作する順番についても、ヒータを先につける、加湿器を先につけるといったユーザごとの特性があると考えられる。提案手法では、このような家庭内の行動パターンを、ホームゲートウェイで観測可能な機器の操作、入退室、温度等のセンサから得られる情報から学習し、異常検知に利用する。

2.1 異常検知モデル

図 1 に、本手法の異常検知モデルを示した。

2.1.1 宅内の状況

提案手法では、センサから得られるデータと時刻をもとに、現在の宅内の状況を定義する。状況の要素を c_i という変数で示す。ここで、インデックス i は 1 から i^{max} の値をとるものとする。例えば、c_1 は時刻、c_2 は室温の値を示す変数である。このような連続値に対して、複数の閾値を用いることで離散化し、状況を分割する。例えば、$c_i^{(j)} \leqq c_i \leqq c_i^{(j+1)}$($c_i^{(j)}$ は i 番目の変数の j 番目の閾値) を満たす c_i の値は、その変数の j 番目の領域に分類される。

2.1.2 ユーザの行動順序

提案手法では、上記で定義した宅内の状況の各領域について、当該領域でのイベントの順序を学習する。本稿では、イベント

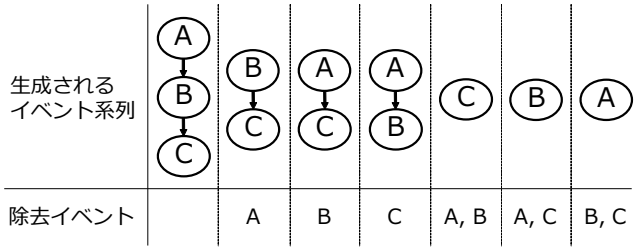

図 2: イベント A、B、C が連続して観測された場合、学習するイベント系列

は、ホームゲートウェイで把握可能な各ユーザの入退室、機器の操作をイベントとしてみなす。そして、前のイベント発生から T 秒以内に発生したイベントは連続したイベントとみなし、イベントの系列を構築する。イベントの系列は、最初に発生したイベントを根、最後のイベントを葉とする複数の木としてモデル化が可能である。このようにモデル化することにより、イベントの系列が与えられた場合、当該系列に含まれる一連のイベントで、根から葉まで到達できる経路が、蓄積された木の中にあるかを調べることにより、蓄積されたイベント系列に含まれるイベント系列であるのかを確認することができる。

2.2 学習手法

提案手法では、観測されたイベントの系列を学習することにより、ユーザの通常の動作を学習する。本学習は、イベントの系列を生成、宅内の状況を表す空間から学習対象の領域を選択、木の更新の手順を各イベント系列に対して繰り返すことにより、行われる。

2.2.1 イベント系列の生成

観測されたイベントを、前のイベント発生から T 秒以内に発生したイベントは連続したイベントとみなすことにより、系列を作成する。ただし、一般的に宅内には複数のユーザが存在するため、生成されたイベント系列には、あるユーザが行う一連の行動に起因するイベントの間に、別のユーザの行動がノイズとして混入することも考えられる。そのため、このようなノイズを除去し、本質的なイベントの系列を学習することが必要となる。本提案手法では、連続して発生したイベントの系列に対して、別ユーザの行動がノイズとして混入することを考慮して、間のイベントを除去することにより、学習用のイベント系列を生成する。図 2 に生成されたイベント系列の例を示す。この例では、イベント A、イベント B、イベント C というイベントが連続して観測されている。この場合、図 2 に含まれるようなイベント系列を生成することにより、各イベントが別ユーザの行動に起因するノイズであった場合を考慮した系列を生成することができる。

2.2.2 学習対象の状況の選択

生成されたイベント系列の先頭の状況をもとに、学習対象の状況を選択する。その際、生成されたイベント系列を、現在の状況に合致している領域の学習のみではなく、周辺の領域の学習に用いる。具体的には、現在の状況を表す各観測値 x_i に対して、$x_i - \alpha_i$ 以上 $x_i + \alpha_i$ 以下に該当する領域であれば、現在のイベント系列を用いた学習を行う対象である領域とみなす。これにより、20 時台に発生したイベントの系列を 19 時台や 21 時台といった類似した環境の学習に用いることが可能となり、少ないイベントの系列で、各状況に対応したイベントの順を学習することが可能となる。

2.2.3 イベント系列木の更新

提案手法では、学習対象の領域を選択後、当該領域に対応する木を更新することを繰り返すことにより、イベントの順を学習する。この学習は、生成された各イベント系列に対して、イベント系列の先頭が根、イベント系列の最後のイベントが葉となるような経路を持つ木ができるように、木にノードとリンクを追加する。その後、各系列において、系列の先頭が根、最後のイベントが葉となる経路上にあるノードのカウンタを 1 増加させる。この手順を繰り返すことにより、木構造のノードのうち、頻繁に行われる行動に関連したノードは、対応するカウンタの値が大きくなり、ノイズとして混入した別ユーザの行動に起因するイベントに関するノードは、対応するカウンタ値は小さいままとなる。そのため、構築された木のうち、カウンタ値の小さなノードを除去した木を用いることにより、ユーザの一連の行動に起因するイベントの順を記録した木を構築することができる。ただし、本学習方法では、短いイベント系列は生成されやすく、長い系列は生成されにくいという点を考慮する必要がある。そこで、上述のカウンタ値に対する閾値は、当該ノードの深さに応じて変える。ここでは、深さ d のノードのカウンタ値に対する閾値を $n_d \times L_{num}$(L_{num}:検知対象の機器の総操作回数) とし、異常検知適用時には、カウンタ値 $n_d \times L_{num}$ よりも小さいノードは除外する。また、本提案手法では、木の根から葉まで到達できるかが判定の基準となる。そのため、ノードを除外した結果、ノード除外前に葉となっていたノードが配下に含まれていないノードについても除外する。

2.3 検知手法

新たな機器操作が発生した場合、当該機器動作を含むイベント系列を生成し、そのイベント系列の順に学習済みの木を探索し、葉まで到達できるかを調べることにより、異常の検知を行う。

2.3.1 イベント系列の生成

異常判定時に用いるイベント系列も、学習用のイベント系列と同様に、前のイベント発生から T 秒以内に発生したイベントは連続したイベントとみなしつつ、別ユーザの行動に起因するノイズとなるイベントの混入を考慮して行う。ただし、異常検出を行う際には、この機器操作のイベントが異常か正常かを見分けたいといった、正常・異常の判断を行いたい対象のイベントが明確に決まっている。そのため、イベント系列生成の際には、対象のイベントを含むイベント系列のみを生成する。

2.3.2 正常および異常の判定

生成された各イベント系列について、現在の状況に対応する領域を選択し、選択した領域に対応する木の集合を探索する。各イベント系列を用いた探索は、木の根から行い、イベント系列の先頭に対応する木の根を持つ木の根に移動する。その後、イベント系列の確認対象となる次のイベントに対応するノードが、現在位置の子ノードにあるかを調べ、子ノードに存在する

場合は、そのノードに遷移する。この手順を繰り返し、木の葉まで到達できた場合は、学習したユーザの行動と合致するとみなすことができる。

上記の探索をすべての生成されたイベント系列に対して行う。一つでも根から葉まで到達できる系列が存在すれば、その操作は正常な操作であると判定する。また、すべてのイベント系列において、系列の先頭から最後までのイベントに該当する遷移が木の中に存在しない場合は、異常と判定する。イベント系列の先頭から最後までの遷移が木の中にあるものの、葉まで到達することができなかった場合は、その後のイベントを待たなければ、機器操作が正常であったか異常であったかを判定できない。この場合、T 秒待ち、新たなイベントが発生しない場合は、学習した順でのイベントが発生していないので、異常として検出する。また、T 秒待ち、新たなイベントが発生した場合は、当該イベントを含むイベント系列を再度生成し、木の探索を行うことにより、正常・異常の判定を行う。

3. パラメータ設定

本手法では T、α、n_d の 3 種類のパラメータを持つ。これらのパラメータ設定手法については、本稿では、スペースの関係で割愛する。詳細については、文献 [12] を参照されたい。

4. 評　　価

4.1 評 価 環 境

4.1.1 評価用データセット

評価用データセットを取得するため、研究室内に、ネットワーク接続可能なヒータや冷蔵庫、テレビなどの家電や、温度計などのセンサといった、15 種類のホーム IoT 機器を設置したホームネットワーク環境を構築した。ホームネットワーク上のユーザとして 4 人の被験者を用意して、自由に機器を使用してもらいながら、自然に生活してもらった。その間、ホームネットワーク上を流れる全ての通信パケットをキャプチャし、機器操作が行われた時刻と、センサの観測値を記録した。また、ホームネットワークに、ユーザのスマートフォンが接続しているかどうかという情報から、ユーザが入退室した時刻も記録した。また、実験環境内に配置したセンサから温度、湿度、騒音に関するデータを取得した。ただし、本実験環境である研究室内は、一定の室温に保たれるように常に制御されているため、室温や湿度が大きく変化しなかったことから、本評価において、状況の定義にはセンサデータは用いず、時刻のみ用いることとした。

4.1.2 評 価 手 順

本稿では、検知率、誤検知率の二つの指標を用いて評価を行う。

a) 誤 検 知 率

本評価では、正常なユーザの操作が誤って不正操作と判別されないかを確認する。本評価を行うためには、正常なユーザの挙動に関するデータセットを、学習用データセットとテスト用データセットに分け、学習用データセットで学習を行ったのちに、テスト用データセットを入力とした際の誤検知について調べる。本稿では、本評価に用いることができる機器使用のデータが限られているため、Leave-One-Out Cross-Validation(LOOCV) [13] により、誤検知率の評価を行った。LOOCV では、データを一定間隔に分割し、分割されたデータのうち、特定の一個分以外を学習データ、残りの一個分のデータをテストデータとして検証を行い、それを全ての分割された各データに対してそれぞれ評価を行う。本稿では、1 か月分のデータを 1 日単位で分割し、ある 1 日以外の日時のデータを学習用データ、残りの 1 日間のデータをテストデータとして利用した。そして、テストデータ中に含まれる機器操作のうち、誤って異常であると判定されてしまった操作数と、テストデータに含まれる総操作数をカウントした。そして、LOOCV における全評価結果において、テストデータに含まれる総操作数に対する誤って異常であると判定されてしまった操作数の割合を誤検知率とした。

b) 検知率の評価

本評価では、テストデータに対して加えた不正操作を提案手法が検出できことを確認する。本評価にあたり、誤検知率の評価とそろえるために、1 か月分のデータを 1 日単位で分割し、ある 1 日以外の日時のデータを学習用データ、残りの 1 日間のデータをテストデータとして利用した。そして、攻撃者は特定の一台の機器にしか、不正操作を試みないと仮定し、各 1 日間のテストデータに対して不正操作パケットを 100 回分ランダムな時刻に混入し、学習用データから学習した行動パターンをもとにテストデータの検証を行った。検証では、混入した全不正操作のうち、不正操作であると判定できたものの割合を検知率と定義し、評価に用いた。

4.2 評 価 結 果

1 か月間 (2017 年 1 月) と、3 か月間× 2 回 (2017 年 4,6,8 月と、2017 年 5,7,9 月) のデータセットを用いて評価を行った。この 3 種類のデータセットは、データセットごとに被験者の学生を変えている。ただし、各データセット内では、被験者は同一である。1 か月間のデータを用いて、冬によく使われるようなヒータや加湿器などの機器操作について考察し、3 か月間のデータを用いて、より長い期間学習データが存在した場合についての考察と、夏によく使われるような扇風機などの機器操作について考察する。

表 1: 2017 年 1 月の検知結果

	検知率	検知数 /計	誤検知率	誤検知数 /計
コーヒーメーカ	0.157	346/2200	0.000	0/48
ヒータ	0.959	2110/2200	0.182	2/11
加湿器	0.080	176/2200	0.000	0/38
テレビ A	1.000	2200/2200	1.000	8/8
テレビ B	1.000	2200/2200	0.000	0/2

4.2.1 1 か月間のデータによる評価結果

まず、2017 年 1 月の 1 か月間の結果に対して評価を行う。本評価では、最初の 1 週間のデータをパラメータ設定に用い、残りの 3 週間のデータを使用して、LOOCV を用いてテストを行った。また、LOOCV を用いた際、最初の 1 週間のデータも学習データとして利用した。表 1 に評価結果を示した。まず、

ヒータに関しては、95%以上の不正操作を検知することができた。これは、イベント順序が正しく学習されたためである。本評価データセットにおいては、ヒータに関して、3 つの行動パターンが学習された。加湿器を操作した後にヒータを操作するという行動パターンと、9 時から 17 時の時間帯においてヒータを操作した後にコーヒーメーカを操作するという行動パターン、午後の時間帯においてヒータを操作した後にユーザ 01 が退室するという行動パターンである。不正な操作コマンドが送信されたとしても、これらの行動パターンに一致しなければ、不正操作として検知した。

一方で、ヒータの誤検知した正常操作数は 2 回分であった。誤検知された操作は、ヒーターの操作後に加湿器を操作するという行動パターンに関する操作であったが、この行動パターンは一か月間に発生した回数が少なかったことから、行動パターンとして学習されず、誤検知された。

また、表 1 において、コーヒーメーカと加湿器の検知率が低かった。これは、コーヒーメーカと加湿器の操作の多くが**単発操作** (当該操作の前後に、他のイベントが存在せず、イベント順序が学習されないような機器操作) であったことが原因である。さらに、これらの機器が、一日のうちの様々な時刻に操作されたことも原因の一つである。このような、様々な時刻に行われた単発操作を、異常として検知しないようにパラメータを設定したため、ほとんどの操作を正常な操作であると判断してしまった。

さらに、表 1 のテレビについては、全ての不正操作を検知することができた。しかし、テレビ A については、誤検知率が高くなってしまった。これは、正常な行動パターンを学習するための操作数が少なかったことと、テレビ A の操作に関する行動パターンが毎回異なったことが原因である。その結果、テレビ A の操作に関する行動パターンが、正常な行動パターンであると学習されず、不正操作として検知されてしまった。多くの行動パターンが学習に利用された、テレビ B に関しては、誤検知数が少なかった。

4.2.2 3 か月間のデータによる評価結果

次に、2017 年 4,6,8 月の 3 か月間および 2017 年 5,7,9 月の 3 か月間のデータの検知結果に対して評価を行った。各月の初めの 1 週間をパラメータ設定期間とし、各月の残りの 3 週間のデータを用いてテストを行った。また、LOOCV を用いたテストの際には、初めの 1 週間のデータも学習データとして利用した。 表 2 と 3 に評価結果を示した。コーヒーメーカ以外の機器に関しては、98%以上の不正操作が検知できた。これは、扇風機が入室直後に操作されるような、機器操作に関する、正常な行動パターンを、複数回学習することができたためである。

また、テレビの誤検知率については、表 1 の 1 か月間の結果よりも低くなっている。これは、行動パターンを学習するための学習データ数が増加したためである。その結果、正常な操作パケットに対して、同様の行動パターンが学習されているため、当該操作が正常であると判断できるようになった。しかし、学習データが増えたにも関わらず、コーヒーメーカの検知率は高くなかった。さらに、表 2 のテレビ B の誤検知率と、表 3 の扇風機 B とテレビ A の誤検知率に関しても、あまり改善されず、高いままであった。これらは、単発操作によるものである。したがって、不正操作の検知率を向上し、正常操作の誤検知率を低減させるためには、このような正常な単発操作を学習および検知できるような手法が必要である。このような手法の考案は、今後の課題である。

表 2: 2017 年 4,6,8 月の検知結果

	検知率	検知数/計	誤検知率	誤検知数/計
コーヒーメーカ	0.611	3908/6400	0.058	3/52
扇風機 A	0.998	6384/6400	0.000	0/9
扇風機 B	0.999	6399/6400	0.000	0/6
テレビ A	0.996	6377/6400	0.171	7/41
テレビ B	1.000	6400/6400	0.400	4/10
テレビ C	0.999	6397/6400	0.000	0/10
テレビ D	0.999	6398/6400	0.111	1/9

表 3: 2017 年 5,7,9 月の検知結果

	検知率	検知数/計	誤検知率	誤検知数/計
コーヒーメーカ	0.057	368/6500	0.000	0/89
扇風機 A	0.991	6439/6500	0.074	2/27
扇風機 B	0.986	6409/6500	0.302	13/43
テレビ A	0.998	6485/6500	0.231	3/13
テレビ B	0.999	6497/6500	0.077	1/13
テレビ C	0.999	6496/6500	0.000	0/3

4.2.3 考　　察

提案手法では、正常操作に関するイベント順序が学習できるような機器に関しては、95–100%の不正操作を検知することができた。しかし、数回の誤検知が発生してしまうことも分かった。これらは、操作の前後に他のイベントが存在しないような単発操作と、あまり頻繁に行われないような行動パターンに関するレアな機器操作が原因である。

提案手法では、機器操作やユーザの入退室といったイベントの順序を比較することで、不正操作の検知を達成した。しかし、単発操作の正常異常を判定する際には、順序の情報は利用できず、状況に関する情報のみが利用可能となるため、状況の情報のみで当該操作が正常であることを判定する必要がある。

正常な単発操作を学習するための一つのアプローチとしては、当該操作に関連するイベントを観測できるセンサを設置することが挙げられる。例えば、加湿器に関する操作は、貯水タンクが空になった後に行われることが考えられる。もし、貯水タンクの残量を観測できるようなセンサを設置すれば、当該操作に関するイベントとして観測することができるようになり、加湿器の当該操作は、単発操作ではなくなる。別のアプローチとして、状況を定義するための情報をより多く利用することが挙げられる。本評価においては、時刻に関する情報のみを状況の定義に利用したが、より多くの情報を用いて状況を細かく定義することで、正常な操作が行われる状況と、その他の状況を区別することができれば、正常な単一操作を区別することがで

きるようになる。正常な単発操作を区別する新たな手法に関しては、今後の課題である。

また、家庭内で十分な学習データが得られないような場合や、頻繁に行われないような行動パターンに関するレアな操作による、正常操作の誤検知を減らすことも、課題の一つである。アプローチとして、他の家庭におけるデータを学習に利用することが挙げられるが、そのアプローチにはいくつかの問題点が残る。一つの問題点は、各家庭における行動パターンの違いである。行動パターンの異なる家庭におけるデータは学習データに適さないと考えられることから、ユーザが似たような行動をしている他の家庭からデータを取得する方法が必要である。さらに、もう一つの問題点として、他の家庭の行動情報をやりとりすることで、プライバシが問題視されることも考えられる。そのため、個人に関する情報を交換せずに、他の家庭からのデータを使用する方法が必要となる。このような手法を考案することも、今後の課題の一つである。

5. まとめと今後の課題

本研究では、ホーム IoT 機器の不正操作を検知する手法を提案した。本手法は、時刻やセンサの値によって定義された状況ごとの、ユーザの行動順序を学習する。新たな操作パケットが観測された際、現在の宅内状況における学習済みの行動パターンと比較し、行動パターンから外れた操作を、不正操作として検知する。

評価環境として、研究室内に複数の IoT 機器を設置し、4 人の学生を被験者として、機器を日常的に使用してもらい、機器操作が行われた時刻を記録した。このデータを用いて、本手法の検知率および誤検知率について評価したところ、複数の機器を操作したり、入退室の前後に操作するような行動順序が学習された機器においては、誤検知を月に数回程度に抑えて、95–100%の不正操作を検知することができた。しかし、本手法では、行動順序が学習されないような、単発操作に関しては、検知が困難であった。また、頻繁に行われないような、レアな行動パターンについても、誤検知率が増加する原因となった。これらの、単発操作やレアな行動パターンの検知が、今後の課題である。

謝　　辞

本研究は、三菱電機サイバーセキュリティ協働研究所における成果である。

文　　献

[1] “Google Home”. https://home.google.com
[2] “Amazon Echo”. https://www.amazon.com/echo
[3] 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)
[4] 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, (February 2015)
[5] 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, Part.3, pp.1454–1464, (January 2017)
[6] M. Capellupo, J. Liranzo, M.Z.A. Bhuiyan, T. Hayajneh, and G. Wang : “Security and Attack Vector Analysis of IoT Devices,” International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage-Springer, vol.10658, pp.593–606, (December 2017)
[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,” in Proceedings of the 26th USENIX Security Symposium, USENIX Association, pp.1093–1110, (August 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,” in Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp.46–51, (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] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato : “Anomaly Detection for Smart Home IoT Based on Users’ Behavior,” in proceedings of 2019 IEEE International Conference on Consumer Electronics, pp.1–6, (January 2019)
[13] C.M. Bishop : Pattern Recognition and Machine Learning (Information Science and Statistics), Springer-Verlag New York, Inc., Secaucus, NJ, USA, (February 2006)