一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
IN2017-58(2017-12)

スマートホームIoTにおけるユーザ行動の学習に基づく異常検知手法

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 〒 617-8550 京都府長岡京市馬場図所 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サイバー攻撃も発生するようになった。特に機器の不正操作については、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。しかし、このような機器の不正操作に用いられる通信は、通常のユーザが当該機器を操作する通信と同様であり、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の適用が困難である。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。手法の評価のため、研究室内に IoT 機器を設置してホームネットワーク環境を構築し、4 人の被験者に当該機器を使用してもらい、パケットを取得した。そのパケットデータに機器への不正操作パケットを混入し、不正操作の検出率を評価した。その結果、誤検知を 6.25%に抑え、99.6%の不正操作が検出可能であった。

キーワード　スマートホーム、IoT、セキュリティ、異常検知、不正操作検知、行動パターン

Anomaly Detection for Smart Home IoT based on Users' Behavior

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
1 Zusho Baba Nagaokakyo City Kyoto 617-8550, 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　Many devices such as air conditioners and refrigerator have become connected to the Internet, and become a target of the cyber-attacks. Especially, the operations by the attackers are serious problems, which may kill the users. However, such attacks are difficult to detect, because the operations by the attackers uses the same protocol as the operations by the users. In this paper, we propose a method to detect such attacks. Our method learns the behavior of the users at each condition defined by the time-of-day and information monitored by sensors such as temperature. Then, our method detects attacks by comparing the current behavior with the learned behavior for the condition corresponding to the current condition. We evaluate our method by using the data including the behavior of 4 users of the IoT devices. The results demonstrate 99.6% of attacks can be detected with 6.25% of false detections.

Key words　Smart Home, IoT, Security, Anomaly Detection, Spoofing Operation Detection, Behavior Pattern

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家電などの日常生活で使用する機器がインターネットに接続するようになった。それらの機器は IoT 機器と呼ばれ、ユーザはスマートフォンなどを使って IoT 機器を操作したり、IoT 機器の稼働状況や周辺状況をチェックしたりすることができる。このように機器がネットワークに接続することによって機器用途の可能性を広げている。しかし、家庭内に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が高まっている。すでに、家庭内の IoT 機器を狙った攻撃は観測されており [1]、IoT 機器を狙ったマルウェアも出現している [2]。現在発生している IoT 機器を狙った攻撃の多くは、IoT 機器に侵入し、DoS 攻撃などの攻撃の踏み台として利用するものである [3]〜[5]。しかしながら、IoT 機器は、現実の生活に密接に関係する機器であり、現実社会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 [6]。特に、IoT 機器の不正操作は、ユーザの意図とは異なる動作を機器にさせることにより、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攻撃も考えられ、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攻撃は、セキュリティソフトや IDS 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、既知の不正パケットのパターンマッチングや、トラヒックの統計情報に対して外れ値を検出することにより、異常の検出を行ってきた。しかしながら、不正操作時の通信は、ユーザが機器操作を行う際と同じプロトコルに従った通信であり、パケットの特徴や通信手順からは、不正操作の検出は困難である。また、機器の操作に必要なパケットは少数であるため、トラヒックの統計情報を用いても不正操作の検出は困難である。さらに、ユーザが実際に利用しているスマートフォンが感染したマルウェア踏み台として不正操作が行われる可能性もあり、操作元の端末情報を用いたとしても、不正操作とユーザの操作の区別は困難である。

そこで本研究では、ユーザのホーム IoT 機器操作に関する行動を学習し、学習結果をもとにホームネットワークに接続されたホーム IoT 機器への不正操作を検知する手法を提案する。提案手法では、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、不正操作の検出を行う。ホームゲートウェイでは、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おり、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。さらに、ホームゲートウェイは、宅外のネットワークや宅内のスマートフォンから、ホーム IoT 機器を操作する通信を中継するため、ホーム IoT 機器へのネットワーク経由の操作も把握可能である。

提案手法では、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、発生したイベント（機器操作、ユーザの入退室等）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。

本稿では、提案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た。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た。

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. 章で説明する。次に第 3. 章で提案手法の評価を行うための実験環境と評価結果について述べる。最後に、本稿のまとめと今後の課題を第 4. 章で述べる。

2. ホーム IoT 機器の不正操作検知

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 検知に用いるモデル

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。以降、$x_1, \cdots, x_n$ の n 種類のデータにより宅内の状況を定義するとする。この場合、宅内の状況は、n 次元空間上の点としてあらわすことができる。本稿では、n 次元空間を、各次元に対して複数の閾値を定め、格子状に分割するものとする。すなわち、各データ x_j について、基準値 $x_j^{(1)}, \cdots, x_j^{(k_j)}$ を用いて領域を分割すると、$x_j^{(i)} \leqq x_j < x_j^{(i+1)}$ の場合、j 番目のデータに関して i 番目の領域に分類される状況となる。

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、蓄積された木のな

か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 学習方法

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 1 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 1 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 学習対象の状態の選択

生成されたイベント系列の先頭の状態をもとに、学習対象の状態を選択する。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 木の学習

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。

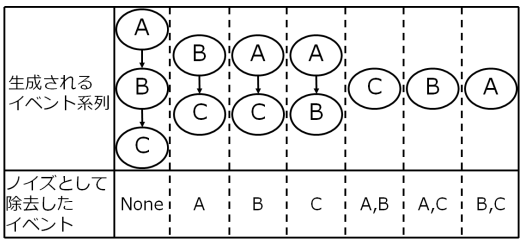


図 1: イベント A、イベント B、イベント C というイベントが連続して観測されたときに、考慮するイベント系列一覧

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 とし、異常検知適用時には、カウンタ値 n_d 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 検知方法

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。図 2 に、イベント A、イベント B、イベント C が連続して発生した際に、イベント C の異常検知のテスト用に生成されるイベント系列を示す。この場合、各イベント A、B についてそれぞれがノイズであることを考慮したイベント系列が生成される。

2.3.2 正常・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

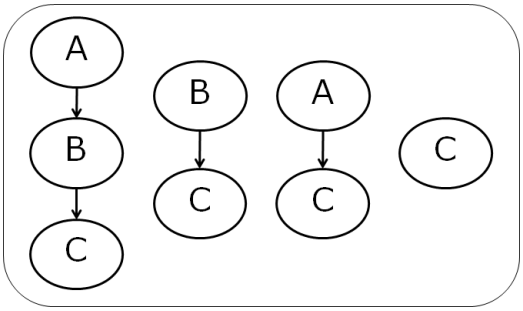


図 2: イベント A、B、C が連続して発生したときの検知対象のイベント C に関して生成されるイベント系列

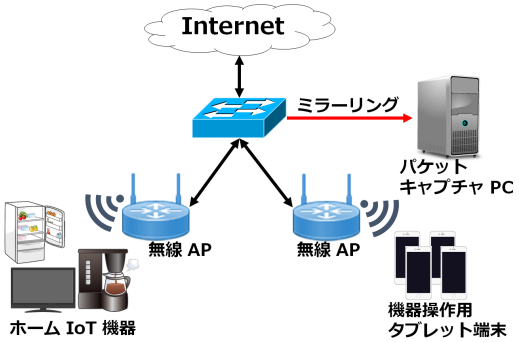


図 3: 研究室に設置した評価用仮想ホームネットワーク環境

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. 評　　価

3.1 評 価 環 境

3.1.1 評価用データセット

評価用データを取得するため、研究室内に、ネットワーク接続可能な冷蔵庫やヒータ、コーヒーメーカなどの全 15 種類の IoT 機器を設置し、図 3 のような仮想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、機器の操作用のタブレット端末をスマートフォンの代わりとして配布し、自由に機器を使用してもらいながら 2017 年 1 月の 1 か月間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、機器宛のパケットの有無から機器を操作したタイミング、操作用タブレット端末のネットワークへの参加離脱のタイミングからユーザの入退室のタイミングのデータを作成した。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、本データの取得期間は、1 か月と短く、室温や湿度が大きく変化しなかったことから、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。

3.1.2 評 価 手 順

本稿では、提案手法でユーザの行動を学習したのちに、正常なユーザの操作を誤検知しないか、あるいは、疑似的に混入した不正操作を検知できるかを評価する。

a） 誤検知率の評価

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) [7] 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ることを確認する。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。

3.2 評 価 結 果

本評価では、設置した機器のうち、不正操作によって火災が発生するなど最も深刻な脅威が考えられるヒータに焦点を当てた。

図 4 に表 1 に示したパラメータで提案手法を動作させた際に学習されたヒータの操作を含む行動パターンを示す。図 4 は、

学習されたイベントの順序と、そのイベントの順が学習内容に含まれる時間帯の関係を示している。 図 4 より、4 つの行動パターンとその行動パターンが行われる時間帯を確認することができる。多くの時間帯で確認された動作は、加湿器の操作後にヒータを操作するという行動パターンであり、被験者は、ヒータをつける前に加湿器をつけるという習慣があり、提案手法により、被験者の習慣を学習することができていると考えられる。また、昼から夕方にかけては、加湿器を操作後、ヒータを操作という行動や、ヒータを操作後、ユーザ 01 が退室するという行動が学習されている。これは、加湿器やヒータを操作しているのがユーザ 01 であり、ユーザ 01 が昼の休憩や帰宅時に、ヒータの電源を切ったのち、加湿器の電源を切るという習慣があり、提案手法がこの習慣を学習していると考えられる。また、この退席・帰宅時と思われる行動パターンは、12 時半以降にしか観測されておらず、午前中に同様のイベントが発生したとしても、異常であると検出することが可能な学習結果となっている。

表 1 に示したパラメータにおける、検知率、誤検知率を表 2 に示す。表 2 より、誤検知を 6.25%に抑えて 99.6%の不正操作を検出することができたことが分かる。これは、提案手法がユーザの機器操作に起因するイベントの発生順を学習することができ、学習した順序に従った機器操作ができない限り、不正として検出することができるためである。

次にパラメータが検知率、誤検知率に与える影響について評価を行った。パラメータの中でも、α_i の値は、各状況の学習用データ数や状況認識の粒度に影響を与え、検知性能への影響も大きいと考えられる。また、n_i の値も、学習されるイベントの順序に影響を与え、n_i の値が小さいと、多くの種類の系列が学習結果に残り、誤検知を減らすことができる反面、正常と判定されるパターンが増え、検知率の悪化を招く可能性がある。逆に、n_i の値が大きいと、ノイズ的に混入したイベントは除去され、頻繁に発生する系列のみを残した学習結果を得ることができるものの、ユーザが通常の操作で発生させる頻度の少ない操作手順は学習結果から除外されるため、誤検知を増やしてしまう可能性がある。そこで、本稿では、α_i の値、n_i の値を変化させて、検出率、誤検出率を評価した。

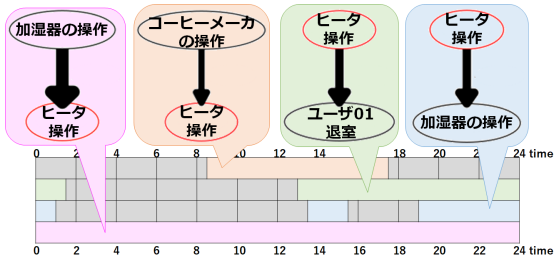


図 4: 学習された行動パターン

表 1: 評価時のパラメータ設定

T	n_1	n_i $(i \geqq 2)$	α_i
300	9	3	31200

表 2: 評価結果

検知率 (検知数/混入不正操作数)	誤検知率 (誤検知数/正常操作数)
0.9962 (2889/2900)	0.0625 (1/16)

図 5 に n_1 の値、α_i の値を変化させた場合の検知率、誤検知率の関係、図 6 に $n_i(i \geqq 2)$ と α_i の値を変化させた場合の検知率、誤検知率の関係を示す。いずれの図も横軸が α_i の値、縦軸が検知率、あるいは誤検知率を示し、n_1 や $n_i(i \geqq 2)$ を異なる値に設定した複数の線を描画している。いずれの評価においても、T は 300 秒とし、n_1 を変化させる場合は、$n_i(i \geqq 2)$ は 3 とし、$n_i(i \geqq 2)$ を変化させる場合は、n_1 を 9 とした。また、$n_i(i \geqq 2)$ を変化させる際には、$n_i(i \geqq 2)$ はすべて同一の値に設定した。

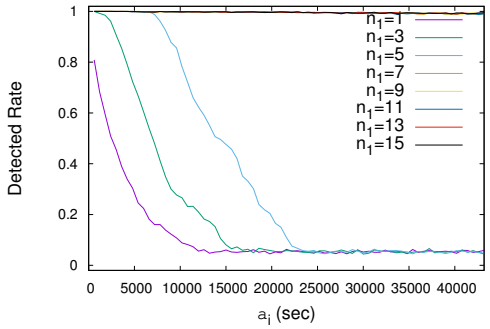
図 5a より n_1 が小さい場合は、検知率が著しく低下することが分かる。これは、学習時に生成されたヒータの操作のみからなるイベント系列も学習結果として反映されるためである。その結果、機器の操作順に関係なく、ヒータが操作されたことのある時間帯の操作はすべて正常と検知してしまうためである。それに対して、n_1 が 7 以上の場合、99%以上の高い検知率を達成可能である。n_1 を大きくすることにより、単一の機器操作しか含まないイベント系列は学習結果に残らず、学習された順での機器操作が行われないと、不正操作として検出できるためである。

図 6 より、$n_i(i \geqq 2)$ が大きくなるにつれ、検知率が上がる一方、誤検知率も上がることが分かる。これは、$n_i(i \geqq 2)$ が大きくなるにつれ、頻繁に観測されたイベント系列のみ、不正操作の検出に用いられるようになるためである。その結果、機器の操作の頻度が低い時間帯や、あまり行われない順序での機器操作の発生を不正操作と検出しやすくなる一方、実際のユーザが行った、頻度の低い操作順での操作も不正として検出されるようになる。また、図 5a、6b より、α_i の値も検知率、誤検知率に大きく影響を与え、α_i の値を大きくすると、検知率、誤検知率ともに下がることが分かる。これは、α_i を大きくすることにより、観測された各イベント系列が、より多くの時間帯での学習に利用されるためである。その結果、α_i が小さい場合は、限られた時間帯の機器操作しか正常と判定しなかったのに対して、α_i が大きくなると、時間帯によらず、学習されたイベントの発生順と合致さえしていれば、正常であると判定されるようになる。

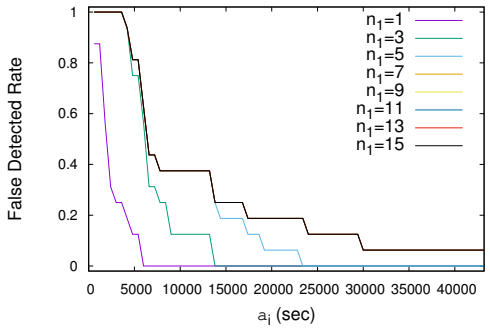
以上の評価結果より、提案手法は適切にパラメータを設定することにより、誤検知を 6.25%に抑えて 99.6%の不正操作を検出でき、高い検出性能を達成することが分かった。ただし、検出性能はパラメータに依存し、適切なパラメータは、機器の使用頻度等の環境に依存する可能性がある。提案手法におけるパラメータの設定方法については、今後検討を行う予定である。

4. おわりに

本稿では、ホームネットワークに接続された機器に対する不正操作を検出する手法を考案した。この手法では、時刻やセン

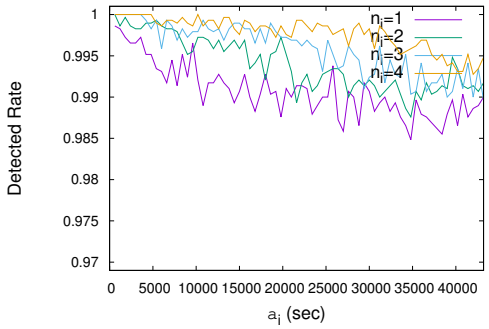


(a) 検知率

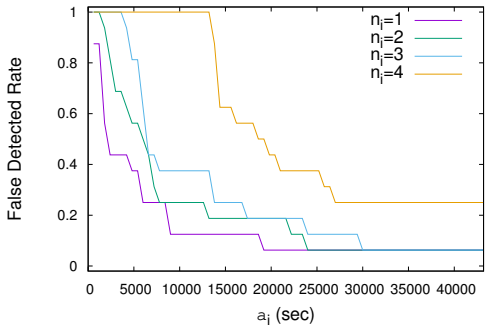


(b) 誤検知率

図 5: n_1、α_i と検知率と誤検知率の関係



(a) 検知率



(b) 誤検知率

図 6: $n_i (i \geqq 2)$、α_i と検知率と誤検知率の関係

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、研究室内に IoT 機器を設置してホームネットワーク環境を構築し、4 人の被験者に当該機器を使用してもらい、パケットを取得した。そのパケットデータに機器への不正操作パケットを混入し、不正操作の検出を評価した。その結果、誤検知を 6.25%に抑えて 99.6%の不正操作を検出可能であることを確認した。

ただし、本稿の評価は、攻撃者が特定の一台の機器に対してのみ不正操作を行った場合に関する評価にとどまっている。攻撃者が複数の機器に対して不正操作が可能である場合、攻撃者が意図的にイベント系列を生成することも可能となるため、このような場合の検知性能についても今後検討を行う予定である。

また、本稿の評価は、ヒータに焦点をあて、被験者のヒータの利用があった 1 か月分のデータのみを用いて行っていた。その結果、同時期に観測されたデータを用いた結果、温度等のセンサデータは同程度の値となり、機器操作の状況の定義に時刻のみを用いていた。今後は、評価に用いるデータを増やし、センサデータを活用して状況を定義した場合についても評価するとともに、ヒータ以外の機器を対象とした評価も行う予定である。

文　　献

[1] K. Xu, F. Wang, and X. Jia, “Secure the Internet, one home at a time,” Security and Communication Networks, vol.9, no.16, pp.3821–3832, July 2016.

[2] 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,” 26th USENIX Security Symposium (USENIX Security 17), pp.1093–1110, USENIX Association, Vancouver, BC, Aug. 2017. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[3] K. Yoshioka, “IoT マルウエア大量感染の現状と対策,” 日経コンピュータ，2016 年 8 月 18 日号，pp.78–81，Aug. 2016. 感染 IoT 機器は 60 種類以上 ビデオレコーダーの感染が多数.

[4] 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.

[5] 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. http://doi.acm.org/10.1145/3098243.3098264

[6] 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.

[7] C.M. Bishop, Pattern Recognition and Machine Learning (Information Science and Statistics), Springer-Verlag New York, Inc., Secaucus, NJ, USA, Feb. 2006.