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.

家庭活動の状況推定を用いたスマートホームネットワークの異常検出手法

田中　雅弘† 　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 〒661-8661 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-tanaka,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　本研究では、家庭活動の状況推定を用いたホーム IoT デバイスの不正検知手法を提案する。本手法では、宅内の状況に関連する状態を定義し、状態遷移モデルによって宅内の状況をモデル化する。そして、状態遷移確率と、センサー値を観測する確率、また各状態の各機器を操作する確率を学習する。そして、この方法を使用して、モデルを使用して不正な操作を検出する。実際の家庭環境で得られたデータを使用し、本手法を評価した。その結果、誤検出率の 20.1 % 未満で 72.3 % の検出率を達成し、時刻のみによって状況を定義する手法よりも高い検知精度を達成した。
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、状況推定

Anomaly Detection in Smart Home Networks using Situation Estimation in-Home Activities

Masahiro TANAKA†, 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 661-8661, Japan
††† Mitsubishi Electric Corporation Information Technology R&D Center
5-1-1 Ofuna Kamakura City Kanagawa 247-8501, Japan
E-mail: †{m-tanaka,m-yamauchi,y-ohsita,murata}@ist.osaka-u.ac.jp,
††Ueda.Kensuke@ce.MitsubishiElectric.co.jp, †††Kato.Yoshiaki@dh.MitsubishiElectric.co.jp

Abstract　In this paper, we propose a method to detect the anomalous operation of home IoT devices focusing on the condition. Our method defines the states related to the situation of the in-home activities and models the time series of the situation by a state transition model. Our method learns the state transition probabilities and the probability to observe sensor values or operate each device for each state from the monitored data. Then, our method detects anomalous operation by using the model. We evaluate our method by using the data obtained in the actual home environment. The results demonstrate that our method achieves 72.3 % of detection ratio with less than 20.1 % of the misdetection ratio, while the method that defines the conditions by only the time of day cannot achieve such accurate detection.
Key words　Smart Home, IoT, Security, Anomaly Detection, Spoofing Operation Detection, Situation Estimation

1. はじめに

近年、冷蔵庫やエアコンなどの家電製品がインターネットに接続されてはじめている。これらの機器は、IoT（Internet of Things）機器と呼ばれる。IoT 機器の数は毎年増加しており、IoT 機器の数が増加するにつれて、これらの機器がサイバー攻撃の標的になるリスクが増大している [1]〜[3]。実際、IoT 機器を標的とする多くのサイバー攻撃がすでに観測されている。特に、攻撃者による不正操作は深刻な問題につながるおそれがある。コンピュータやスマートフォンへの攻撃と異なり、日常的に使用される機器を操作することで、直接ユーザに危害を加えたり、損害を与える可能性がある [4]。さらに、多くのエネルギーを消費する IoT 機器を同時に操作することで、電力網が損傷する可能性があることが実証されている [5]。

従来、セキュリティソフトウェアや侵入検知システム（IDS）が、攻撃を検出するために使用される [6]。これらは、パケットの特性またはトラフィックの統計に基づいている。パケットを事前定義されたルールと比較するか、観測されたトラフィック統計の異常値を検出することにより、攻撃を検出する。ただし、IoT 機器での不正な操作は、ユーザによる正当な操作と同じプロトコルを使用するため、パケットの特性に基づく方法で不正操作を検出することは困難である。また、IoT 機器の動作に必要なパケットの数が少ないため、トラフィックの統計を使用して不正操作を検出することも困難である。さらに、攻撃者は、マルウェアに感染したユーザーが通常使用するスマートフォンまたはスマートスピーカーを介して、IoT 機器を操作する可能性がある。この場合、操作コマンドのソースでさえ、異常な操作の検出に使用することができない。

したがって、IoT 機器の不正操作を検出する方法が提案されている。我々は、ユーザの行動に基づい不正操作を検出する方法も提案している [7]。この手法では、IoT 機器の操作や家庭環境で観測されるユーザの行動を、一連の手順としてモデル化する。次に、事前定義された各状況において、操作の手順を学習する。そして、現在の手順を学習済みの手順と比較することにより、攻撃を検出する。

ただし、以前の研究では、状況の定義については詳しく検討しておらず、時刻によって単純に定義された状況を用い手法を評価していた。前研究では、ユーザの行動のシーケンスを学習することにより、このような単純な状況の定義でも、ほとんどの不正な操作を検出できることが実証された。しかし、この手法では、しばしば単独で使用される機器での不正操作を正確に検出できないといった課題がある。そこで、そのような機器での不正な操作と正当な操作を区別するには、機器を操作するときの状況のより洗練された定義が必要であると考えられる。

そこで、本研究では、状況に焦点を当てたホーム IoT 機器の不正操作を検出する方法を提案する。本手法では、宅内の活動に基づいて状況を定義する。宅内の活動は、IoT 機器を使用する傾向と密接に関連している。たとえば、調理用コンロは、一部のユーザが夕食の準備している状況では使用されることが多く、すべてのユーザが寝ている状況では使用されない。本手法では、宅内の活動の状況に関する状態を定義し、状態遷移モデルによって状況の時系列をモデル化する。次に、本手法では、観測されたデータから、状態遷移確率と、各状態における、センサ値や機器の操作が観測される確率を計算することで、学習を行う。次に、本手法では、学習されたモデルを使用し、不正な操作を検出する。現在の状態の推定値は、観測されているセンサー値と機器操作に基づいて定期的に更新され、不正操作は推定された状態に基づいて検出される。

実際の家庭環境で得られたデータを使用し、方法を評価した。データは、センサーを設置し、家電製品が実際の家庭環境で操作された時間を記録することにより取得した。

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. 家庭活動の状況推定を用いたスマートホームネットワークの異常検出手法

家電製品の使用は状況に依存している。たとえば、コンロは、一部のユーザーが夕食を準備している状況でよく使用されるが、すべてのユーザーが寝ている状況では使用されない。そこで、このような宅内の活動の状況に着目して不正操作を検出する手法を提案する。本章では、まず、本手法で使用される宅内の活動のモデルについて説明する。 次に、宅内の活動がどのように学習され、異常な操作がどのように検出されるかを説明する。

2.1 宅内の活動モデル

本手法では、状態遷移モデルによって宅内の活動をモデル化する。モデルは、状態、状態遷移の確率、および各状態での機器操作確率によって定義される。

2.1.1 状態の定義

ユーザの状態と機器の状態の組み合わせによって、宅内の活動の状態を定義する。

a） ユーザの状態

ユーザの状態は、すべてのユーザが外出している状態、少なくとも 1 人のユーザが自宅にいて活動している状態、すべてのユーザが寝ている状態など、自宅でのユーザの活動によって定義される。これらの状態は、騒音センサなど、ユーザが設置したセンサから推定される。

以下、定義されたユーザの状態の数を l として、ユーザの状態 S_U を次のように定義する。

$$S_U = (s_1, s_2, s_3, ..., s_l) \tag{1}$$

b） 機器の状態

また、不正操作検出の対象となる機器の状態も定義する。本手法では、機器の状態として、以下の 4 つの状態として定義する。

- s_I: 使用中
- s_X: T_X 分以内に使用

- s_Y: 使用後 T_y 分以内
- s_N: その他

つまり、機器の状態は以下のように定義される。

$$S_O = (s_I, s_X, s_Y, s_N). \tag{2}$$

現在の状態を正確に識別することは困難である。特に、状態 s_X は、T_X 分後に機器が動作しているかどうかを確認することではじめて正確に識別ができる。ただし、ログデータにおいては、T_X 分後の機器操作ログを確認することで、ログデータに簡単にラベルを付けることがでる。

c） 宅内の状態

宅内の状態 S は、ユーザの状態と機器の状態を組み合わせることで定義される。

$$S = S_U \cdot S_O = (s_1 s_I, s_1 s_X, ..., s_l s_N) \tag{3}$$

そして、S の状態間の状態遷移モデルを構築する。

2.1.2 状態遷移確率

本手法では、状態の各ペアの状態遷移確率が定義される。本手法では、時間をタイムスロットに分割し、各タイムスロットで次の状態に遷移する。

状態遷移の確率は時刻によって異なる。たとえば、昼間の睡眠状態への遷移確率は、夜間のそれとは大きく異なる。したがって、このモデルには、各時刻において状態遷移確率が定義されている。各日の k 番目のタイムスロットでの状態 i から状態 j への遷移確率 $a_k(i,j)$ は、

$$a_k(i,j) = P(S_k = j | S_{k-1} = i) \tag{4}$$

と定義される。ここで、S_k はタイムスロット k の状態である。

2.1.3 機器の操作確率

このモデルには、各状態における機器操作確率 $b(i,n)$ が定義される。状態 i において機器 n の操作される確率 $b\,(i,\,n)$ は、

$$b(i,n) = P(n \in x_t | S_t = i). \tag{5}$$

である。ここで、x_t はタイムスロット t での機器操作である。

2.2 宅内の行動モデルの学習方法

本章では、収集された宅内の活動のログからモデルを学習する方法を説明する。モデルを学習するために、最初にログの各タイムスロットにラベル付けを行う。次に、ラベル付けされたログデータに基づいて、状態遷移確率と機器操作確率を計算する。

2.2.1 ラベリング

ログデータをタイムスロットに分割し、各タイムスロットに状態を示すラベルを設定する。状態は、ユーザの状態と機器の状態の組み合わせによって定義さる。 つまり、ラベルは、ユーザの状態と機器の状態を設定することによって設定される。

両方の状態は、事前定義されたルールによって設定される。ユーザの状態は、事前定義されたルールに従ってセンサデータに基づいて設定される。機器の状態は、機器が操作された時間に基づいて設定される。たとえば、機器が t 番目のタイムスロットから $t+n$ 番目のタイムスロットまで動作したとき、$t - \frac{T_X}{\delta t}$ 番目のタイムスロットから $t-1$ 番目のタイムスロットに S_X の状態、t 番目のタイムスロットから $t+n$ 番目のタイムスロットに S_I の状態、そして、$t+n+1$ 番目のタイムスロットから $t+n+\frac{T_Y}{\delta t}$ 番目のタイムスロットに S_Y への状態のラベルを設定する。ここで、δt は 1 つのタイムスロットの長さである。

2.2.2 状態遷移確率の計算

時間 k での状態 i から状態 j への遷移確率は、次の方程式で与えられる。

$$P(S_{k+1} = j | S_k = i) = \frac{N_{k+1,j}}{N_{k,i}},\ i,j \in S \tag{6}$$

ここで、$N_{k,j}$ は学習データにおける、時間 k での状態 i のタイムスロット数である。

状態が遷移する時刻は日によって異なりますが、同様の状態遷移は同様の時間帯に発生する。したがって、各日の $k - T_Z$ 番目のタイムスロットから $k + T_Z$ 番目のタイムスロットまでのデータを考慮して、$a_k(i,j)$ を計算する。つまり、

$$a_k(i,j) = \frac{\sum_{K-T_Z \leq m \leq K+T_Z} P(S_{m+1} = j | S_m = i)}{D_k} \tag{7}$$

と定義される。ここで、D_k は学習データのタイムスロット数である。

2.2.3 機器操作確率の計算

状態 i において機器 n の操作確率 $b(i,n)$ は、

$$b(i,n) = \sum_k \frac{N_{k,i}^{(n)}}{N_{k,i}} \tag{8}$$

で計算される。ここで、$N_{k,i}$ は、各日の k 番目のタイムスロットで状態が i であるタイムスロットの数であり、$N_{k,i}^{(n)}$ は、状態が i で、デバイス n が k 番目のタイムスロットで動作するタイムスロットの数である。

2.3 宅内の活動に関する状況推定を用いた不正操作検知

本手法では、学習したモデルを使用して不正操作の検出を行う。検出は、機器を操作できる状態の確率に基づいている。本章では、タイムスロット t において状態 i と推定される確率 $\alpha_t(i)$ と、タイムスロット t の機器操作の観測結果 x_t によって定義する。

2.3.1 初期状態の定義

システムの起動時には、現在の状態に関する情報が得られていない。したがって、すべての状態の確率が同じになるように、$\alpha_0(i)$ を初期化する。

$$\alpha_0(i) = \frac{1}{C} \tag{9}$$

ここで、C は状態の数である。

2.3.2 状態の更新

検出システムは、次の手順で各タイムスロットで各状態の確率 α を更新する。

a） 前の状態からの状態遷移による推定

最初に、学習した状態遷移確率 $a_k(i,j)$ を用いて、$\hat{\alpha}_t(i)$ を更新する。推定された現在の状態 $\hat{\alpha}_t(i)$ は

$$\hat{\alpha}_t(i) = \sum_c \alpha_{t-1}(c) a_{T(t-1)}(c,i) \tag{10}$$

である。ここで、$T(t-1)$ はタイムスロット $t-1$ に対応する時刻を取得するための関数である。

b） 観測値による補正

観測値 x_t を用いて、$\hat{\alpha}_t(i)$ を補正する。x_t はタイムスロットで操作さされた機器によって定義される。機器 n がタイムスロット t で操作された場合、$n \in x_t$ である。この定義により、確率 $P(x_t|S_t = i)$ は、

$$P(x_t|S_t = i) = \prod_n \beta(x_t, i, n) \tag{11}$$

である。ここで、

$$\beta(x_t, i, n) = \begin{cases} b(i,n) & n \in x_t \\ 1 & n \notin x_t \end{cases} \tag{12}$$

次に、$\alpha_t(i)$ は次のように推定される。

$$\alpha_t(i) = \frac{P(x_t|S_t = i)\hat{\alpha}_t(i)}{\sum_j P(x_t|S_t = j)\hat{\alpha}_t(i)} \tag{13}$$

2.3.3 検　　知

機器は状態 S_X または S_I で操作される。したがって、推定状態が S_X または S_I のときに機器が操作された場合、その操作は正当であると見なすことができる。 一方で、機器が他の状態で動作している場合、不正な操作であるとみなすことができる。

したがって、本手法では、S_X および S_I の状態の確率をチェックすることにより、不正な操作を検出する。つまり、次の式が満たされる場合、タイムスロット t で異常な操作を検出する。

$$\alpha_t(S_X) + \alpha_t(S_I) \leq \theta \tag{14}$$

3. 評　　価

3.1 データ取集

本手法を評価するため、実際の家庭でデータを収集した。データを収集するために、システムを構築した。本システムは、IoTボタンとエッジコンピュータで構成されている。本システムでは、エッジコンピュータはユーザがボタンを押した時間を記録する。

このシステムを実際の家庭に展開した。 次に、ボタンに対応する家電製品が操作されたとき、家に住んでいる被験者にボタンを押すように依頼した。そして、エッジコンピュータに保存されているログデータを取得する。表 1 に、対応するボタンが設置されている家電製品のリストを示す。

また、環境センサも家庭に配置した。 環境センサとして NETATMO Smart Home Weather Station [8] を使用した。 表 2 に、センサから取得したセンサデータを示す。

本評価では、2018 年 12 月から 2019 年 3 月までの 4 か月間に収集されたデータを使用した。また、本評価では、タイムスロットの長さを 1 分に設定した。

表 1: 収集した機器操作

機器/イベント	行動
ユーザの位置	帰宅/外出
照明	ON/OFF
エアコン	冷房 ON/暖房 ON/ドライ ON/上げる/下げる/OFF
扇風機	ON/OFF
ヒーター	ON/OFF
洗濯機	ON
冷蔵庫	OPEN
TV	ON/OFF
コンロ	ON/OFF
電子レンジ	ON
オーブン	ON
炊飯器	ON

表 2: 収集したセンサデータ

センサデータ	範囲	精度
室温	0°C ∼ 50°C	±0.5°C
湿度	0 ∼ 100%	±3%
気圧	260 ∼ 1260mbar	±1mbar
CO2	0 ∼ 5000ppm	±50ppm
騒音	35 ∼ 120dB	

3.2 セッティング

3.2.1 検 知 対 象

本評価では、コンロに焦点を当て、コンロの不正な操作を検知の対象とする。コンロは、実際の家庭で頻繁に使用される。さらに、コンロの不正な操作は、火災などの深刻な問題を引き起こす可能性がある。

3.2.2 ラベリングルール

本手法では、ログデータにラベルを付けるルールを事前に定義する必要がある。本評価では、次のルールを使用する。

- 外出中：すべての被験者が外出し、家の人数がゼロの状態。
- 睡眠中: 家のすべての被験者が寝ている状態。 本評価では、この状態は、少なくとも 1 人の被験者が自宅にいて、騒音センサの値がしきい値未満であり、事前定義された時間内に機器が使用されていない状態によって定義される。
- 活動中: 上記以外の状態。

本評価はコンロ操作を検知のターゲットとしている。そのため、機器の状態は以下のように定義される。

- 調理機器使用中
- T_X 分以内に調理機器が使用される
- 調理機器が使用されて T_Y 分以内
- 調理機器が使用されていない

データセットを収集した家には、調理機器として、コンロ、電子レンジ、オーブントースタ、炊飯器がある。調理器具が使用されている状態は、上記の器具の少なくとも 1 つが 15 分以内に使用されている状態によって定義される。したがって、T_y は 15 分より大きな値に設定される。

宅内の活動の状態は、ユーザの状態と機器の状態の組み合わせによって定義される。つまり、宅内の活動の状態は以下のようになる。

- 外出中 × 調理機器使用中
- 外出中 × T_X 分以内に調理機器が使用される

  ...
- 活動中 × 調理機器が使用されて T_Y 分以内
- 活動中 × 調理機器が使用されていない

図 1 に、上記の状態で定義された状態遷移モデルを示す。 この図では、決して発生しない状態と遷移は省略されている。

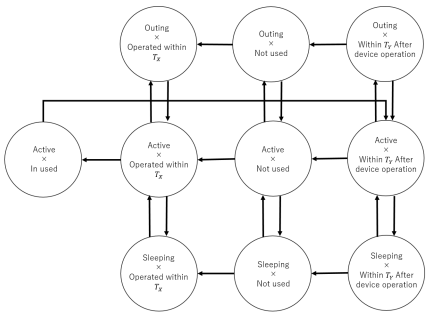

図 1: 評価に用いた状態遷移モデル

3.3 評価指標

本評価では、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) [9] により評価を行った。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。

3.3.1 検知率

本評価では、コンロの不正な操作をテストデータに追加し、それらの検出率を計算した。本評価では、タイムスロットごとに 1 つの不正操作が追加される。 次に、本手法で検出された不正操作をカウントする。追加された不正操作の数に対する検出された不正操作の数の比率によって検出率を定義する。

3.3.2 誤検知率

誤検出率は、誤って検出された正常操作の数と、正常操作の総数の比率によって定義される。

3.4 比較手法

本手法では、宅内の状態の推定に焦点を当てている。そのため、不正操作を検出するための推定の有効性を実証するために、この方法を時刻だけで状況を定義する手法と比較を行う。

3.5 結果

図 2 は、本手法の結果と、時刻のみで状況を定義した手法の結果を比較している。本評価では、手法のパラメータを $T_X = 30$、$T_Y = 30$、および $T_Z = 30$ とした。この図では、ROC（Receiver Operatorating Characteristic）曲線によって手法を比較している。

評価の結果、本手法によって、時刻だけで状況を定義する手法よりも高い検出率を達成した。これは、本手法がコンロが使用される傾向がある状態を正確に推定するためであると考えられる。

また、提案手法で誤検知される正常操作について詳しく調べると、「睡眠中」だと判断されているものが多く存在した。これは、本実験環境において、ユーザーの睡眠状態の推定に用いることができるセンサーが騒音センサーしかないことが原因である。本研究では、騒音センサーの値が閾値を下回ると、「睡眠中」と判別する。しかしながら、このルールでは、睡眠はしていないものの、宅内で静かにすごしている場合は、「睡眠中」と誤って判別される。その結果、本来はユーザーが起きており、調理機器を使用する可能性がある時間帯であっても、誤って睡眠中であると判断し、機器操作が行われる可能性が低いと誤った判断を行ってしまう。この問題を防ぐための方法としては、センサーの追加や、部屋の電気がついているかなどの情報をもとに宅内の状態の定義をすることが考えられる。

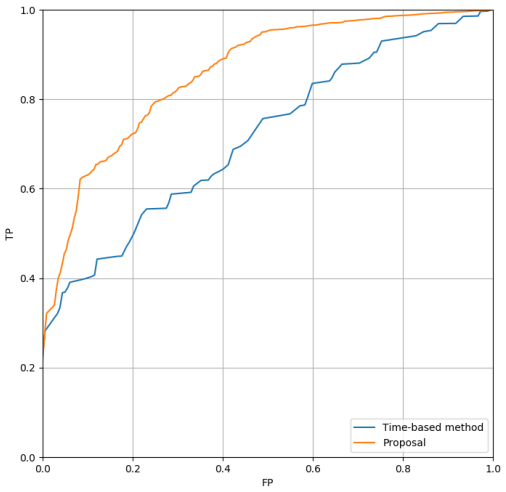

図 2: 時刻のみで状況を定義した手法との比較

4. おわりに

本稿では、状況に焦点を当てた、ホーム IoT 機器の不正操作を検知する手法を提案した。本手法では、宅内の活動の状況に

関連する状態を定義し、状態遷移モデルによって状況の時系列をモデル化する。次に、状態遷移の確率と、各状態ごとに、観測されるセンサの値や機器が操作される確率をデータから学習し、モデルを使用して不正な操作を検出する。

実際の家庭環境で得られたデータを使用し、手法の評価を行った。その結果、誤検出率の 20.1 % 未満で 72.3 % の検出率を達成し、時刻のみによって状況を定義する手法よりも高い検知精度を達成した。

本研究では、宅内の状態の推定に焦点を当てているため、本手法のモデルと同時に、行動の手順などの別のモデルも使用して、不正操作を検出することが可能であると考えられる。そのため、本手法とそのような手法を組み合わせることで、不正操作のより正確な検出を行うことができる可能性があり、これは今後の課題の一つである。

文　　献

[1] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, “Sok: Security evaluation of home-based iot deployments,” IEEE S&P, pp.208–226, 2019.

[2] 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, 2015.

[3] 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, pp.593–606 2017.

[4] 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, 2014.

[5] S. Soltan, P. Mittal, and H.V. Poor, “Blackiot: Iot botnet of high wattage devices can disrupt the power grid,” 27th USENIX Security Symposium (USENIX Security 18), pp.15–32, 2018.

[6] B.B. Zarpelão, R.S. Miani, C.T. Kawakani, and S.C. deAlvarenga, “A survey of intrusion detection in internet of things,” Journal of Network and Computer Applications, vol.84, pp.25–37, 2017.

[7] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, “Anomaly detection for smart home based on user behavior,” 2019 IEEE International Conference on Consumer Electronics (ICCE)IEEE, pp.1–6 2019.

[8] “NETATMO Smart Home Weather Station,” `https://www.netatmo.com/en-us/weather`.

[9] N.M. Nasrabadi, “Pattern recognition and machine learning,” Journal of electronic imaging, vol.16, no.4, p.049901, 2007.