Master's Thesis

Title

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

Supervisor

Professor Masayuki Murata

Author

Masahiro Tanaka

February 5th, 2020

Department of Information Networking

Graduate School of Information Science and Technology

Osaka University

Master's Thesis

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

Masahiro Tanaka

Abstract

Home appliances, such as refrigerators and air conditioners have become connected to the Internet. These devices are called IoT (Internet of Things) devices. As the number of IoT devices increases, the risk that these devices become the target of cyberattacks is increasing. In particular, the operations by attackers become a serious problem. The operations by attackers may harm users or make users unsafe.

Conventionally, security software and intrusion detection systems (IDSs) are used to detect attacks. However, anomalous operations are difficult to detect by the method based on the characteristics of the packets because anomalous operations on IoT devices use the same protocol as legitimate operations by users. The statistics of the traffic cannot also be used to detect anomalous operation, because the number of packets required to operate IoT devices is small. In addition, attackers may operate the IoT devices via malware-infected smartphones or smart speakers that the users usually use. In this case, even the source of the operation command cannot be used to detect anomalous operation.

Therefore, methods for detecting anomalous operation of IoT devices have been proposed. Our research team has also proposed a method to detect anomalous operation based on user behavior. This method models user behavior as a sequence of events, which includes the operation of IoT devices and other behavior monitored in the home environment. This method learns the sequences of events for each predefined condition. Then, this method detects attacks by comparing the current sequences of the events with the learned sequences.

However, the previous work did not discuss the definition of the condition; the method was evaluated with the conditions simply defined by the time of day. The previous work demonstrated that most of the anomalous operations can be detected even with such a simple definition of conditions by learning the sequences of events. But the method cannot detect accurately anomalous operations on the devices that are often used solely. To distinguish the anomalous operations on such devices from legitimate operations, a more sophisticated definition of conditions when the devices are operated is required.

In this thesis, we propose a method to detect the anomalous operation of home IoT devices focusing on the condition. We define the condition based on in-home activities. 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.

Keywords

Smart Home
IoT
Security
Anomaly Detection
Spoofing Operation Detection
Situation Estimation

Contents

List of Figures

List of Tables

1 Introduction

Home appliances, such as refrigerators and air conditioners have become connected to the Internet. These devices are called IoT (Internet of Things) devices. The number of IoT devices is increasing every year [1]. As the number of IoT devices increases, the risk that these devices become the target of cyberattacks is increasing [2–4]. In fact, many cyberattacks targeting IoT devices have already been observed.

In particular, the operations by attackers become a serious problem. The operations by attackers may harm users or make users unsafe [5]. Moreover, Soltan et al. demonstrated the possibility that the simultaneous operation of many energy-consuming IoT devices can damage the power grid [6].

Conventionally, security software and intrusion detection systems (IDSs) are used to detect attacks [7]. They detect attacks based on the characteristics of the packets or statistics of traffic; they detect attacks by comparing packets with predefined rules or detecting outliers in observed traffic statistics.

However, anomalous operations are difficult to detect by the method based on the characteristics of the packets because anomalous operations on IoT devices use the same protocol as legitimate operations by users. The statistics of the traffic cannot also be used to detect anomalous operation, because the number of packets required to operate IoT devices is small. In addition, attackers may operate the IoT devices via malware-infected smartphones or smart speakers that the users usually use. In this case, even the source of the operation command cannot be used to detect anomalous operation.

Therefore, methods for detecting anomalous operation of IoT devices have been proposed. Our research team has also proposed a method to detect anomalous operation based on user behavior [8]. This method models user behavior as a sequence of events, which includes the operation of IoT devices and other behavior monitored in the home environment. This method learns the sequences of events for each predefined condition. Then, this method detects attacks by comparing the current sequences of the events with the learned sequences.

However, the previous work did not discuss the definition of the condition; the method was evaluated with the conditions simply defined by the time of day. The previous work demonstrated that most of the anomalous operations can be detected even with such a simple definition of conditions by learning the sequences of events. But the method cannot detect accurately anomalous operations on the devices that are often used solely. To distinguish the anomalous operations on such devices from legitimate operations, a more sophisticated definition of conditions when the devices are operated is required.

In this thesis, we propose a method to detect the anomalous operation of home IoT devices focusing on the condition. We define the condition based on in-home activities. In-home activities are closely related to the tendency to use IoT devices. For example, the cooking stove is often operated in a situation where some of the users are preparing dinner but are never operated in a situation where all of the users are sleeping.

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. Then, 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; the estimated current state is updated periodically based on the monitored sensor values and operations, and anomalous operations are detected base on the estimated state.

We evaluated our method by using the data obtained in the actual home environment. The data is obtained by installing sensors and recording the time when home appliances are operated in the actual home environment.

The rest of this thesis is organized as follows. We first present the related work in section 2. We describe our method to detect anomalous operations in section 3. Then, we evaluate our method in section 4. Finllay, we conclude this work and discuss future issues in section 5.

2 Related Work

2.1 Anomaly Detection Method

Several methods for detecting anomalous operation of IoT devices have been proposed. Amraoui et al. proposed a security framework that continuously authenticates smart home users [9]. This method allows only authorized user to control their IoT devices and preventing them in case of performing abnormal and dangerous control actions. This method learns a normal operation from the user access log and the usage data of the IoT device by the One-Class Support Vector Machine (OCSVM). Then, this method detects anomalous operations by the learned model. Ramapatruni et al. proposed a method to identify anomalous activities that can occur in a smart home environment by using an HMM (Hidden Markov Model) [10]. This method creates an HMM from test data collected from multiple sensors and smart devices. Then it detects anomalous operation by checking whether the current operation matches the model. However, these methods focus on modeling a single user, and cannot be applied to the home where multiple users live. On the other hand, this thesis models the conditions focusing on the state of a home instead of the state of a user.

Our research team has also proposed a method to detect anomalous operation based on user behavior [8]. This method models user behavior as a sequence of events, which includes the operation of IoT devices and other behavior monitored in the home environment. This method learns the sequences of events for each predefined condition. Then, this method detects attacks by comparing the current sequences of the events with the learned sequences. However, the previous work did not discuss the definition of the condition; the method was evaluated with the conditions simply defined by the time of day. The previous work demonstrated that most of the anomalous operations can be detected even with such a simple definition of conditions by learning the sequences of events. But the method cannot detect accurately anomalous operations on the devices that are often used solely. To distinguish the anomalous operations on such devices from legitimate operations, a more sophisticated definition of conditions when the devices are operated is required, which is discussed in this thesis.

2.2 In-Home Activity Identification

This thesis focus on the estimation of conditions of in-home activities. There are several methods for recognizing human behavior in homes using various sensing devices. Ueda et al. proposed a method to learn the behavior of the user based on the position information of the user in the home, and predict the behavior in the home [11]. They use a machine learning technique to identify various daily activities in a home from positioning sensors equipped by inhabitants and power meters attached to appliances. Nakahara et al. proposed a method for logging micro-motion of in-home daily activity using a mobile robot with Kinect [12]. Those methods accurately identifies in-home activities but requires additional devices that directly monitor a person such as positioning sensors or a mobile robot with Kinect. On the other hand, this thesis discusses a method focusing on activities of home appliances and using a small sensor that only monitors the environment in a home. If we can use such additional sensors, our method can work with the existing in-home activity identification methods to improve the accuracy of the detection of anomalous operations.

3 Anomaly Detection in Smart Home Networks using Situation Estimation on In-Home Activities

The usage of home appliances depends on situations. For example, the cooking stove often used in a situation where some of the users are preparing dinner, but never used in a situation where all of the users are sleeping. Therefore, we propose a method to detect anomalous operation focusing on such a situation of in-home activities. In this section, we first explain the model of home activities used in our method. Then, we explain how home activities are learned and how anomalous operations are detected.

3.1 Model of In-Home Activities

In this thesis, we model in-home activities by the state transition model. The model is defined by the states, the state transition probabilities, and the probabilities of operating devices in each state.

3.1.1 Definition of States

We define the state of in-home activities by a combination of the state of the users and the state of the devices.

State of the Users The state of the users is defined by the activities of the users in a home such as a state that all users are out of home, a state that at least one users are at home and active, a state that all users are sleeping and so on. These states are estimated from sensors deployed by the users such as a noise sensor.

Hereafter, we denote the number of defined states of the users by l, define the set of the states of users S_U by

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

State of the Device We also define the state of the device whose operations are a target of anomaly detection. In this method, we define four states for the device;

- s_I: in use
- s_X: used within T_X minutes

- s_Y: within T_y minutes after device operation
- s_N: others

That is, the set of the state of the device is

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

It is difficult to accurately identify the current state; especially the state s_X can be accurately identified after T_X minutes by checking whether the device is operated. But we can easily label the log data by checking the log after T_X minutes.

State of Home The state of the home S is defined by combining the state of the user and the state of the device. That is,

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

We construct the state transition model between the states in S.

3.1.2 State Transition Probabilities

In this method, the state transition probability for each pair of states is defined. In this thesis, we divide time into time slots, and we make a transition to the next state at each time slot.

The state transition probabilities depend on the time of day. For example, the transition probability to sleep state during day time is significantly different from that at night. Therefore, our model includes the definition of state transition probabilities for each time of day. The transition probability $a_k(i, j)$ from the state i to the state j at the kth time slot in each day is defined by the following equation.

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

where S_k is the state at the time slot k

3.1.3 Probabilities of Operating Device

This model includes the definition of the probabilities of operating device $b(i, n)$ for each state. The probability of operating device $b(i, n)$ of device n at state i is defined by

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

where x_t is the set of devices operated at time slot t.

3.2 How to Learn Model of Home Activities

In this subsection, we explain how to learn the model from the stored log of the home activities. To learn the model, we first set a label for each time slot in the log. Then, we calculate the transition probabilities and probabilities of operating devices based on the labeled log data.

3.2.1 Labeling

We divide the log data into time slots and set a label indicating the state to each time slot. The state is defined by the combination of the state of users and the state of the device. That is, the label is set by setting the state of users and the state of device.

Both states are set by the predefined rule. The state of users are set based on the sensor data according to the predefined rules. The status of the device is set based on the time the device was operated. For example, the device is operated from tth time slot to $t + n$th time slot, we set the state from $t - \frac{T_X}{\delta t}$th time slot to $t - 1$ time slot to S_X, the state from tth time slot to $t + n$ time slot to S_I, and the state from $t + n + 1$th time slot to $t + n + \frac{T_Y}{\delta t}$ time slot to S_Y where δt is the length of one time slot.

3.2.2 Calculation of State Transition Probability

The probability of transition from state i to state j at time k is given by the following equation,

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

where $N_{k,j}$ is the number of time slots in state i at time k in the learning data.

The time of day of the state transition depends on the day, but a similar state transition occurs at a similar time of day. Therefore, we calculate $a_k(i,j)$, considering the data from $k - T_Z$th time slot to $k + T_Z$ time slot for each day. That is,

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

where D_k is the number of time slots in the training data.

3.2.3 Calculation of Probabilities of Operating Device

The probability $b(i,n)$ of operating the device n at the state i is calculated by

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

where $N_{k,i}$ is the number of time slots whose state is i at kth time slot in each day, and $N_{k,i}^{(n)}$ is the number of time slots whose state is i and the device n is operated at kth time slot.

3.3 Anomalous Operation Detection using Situation Estimation on In-Home Activities

In our method, we detect anomalous operation by using the learned model. The detection is based on the probabilities of the state where the device can be operated. In this section, we denote the probability that the state at the time slot t is estimated as i by $\alpha_t(i)$, and the observed result of device operation at the time slot t by x_t.

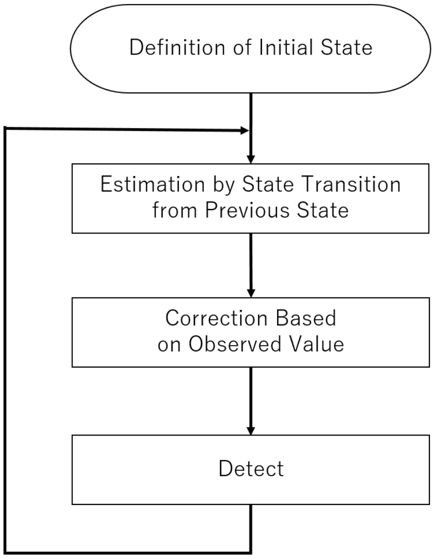
Definition of Initial State
Estimation by State Transition from Previous State
Correction Based on Observed Value
Detect

Figure 1: Estimated Value Update Flow

3.3.1 Definition of Initial State

When we start the system, we do not have the information on the current state. Thus, we initialize $\alpha_0(i)$ so that all states have the same probability

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

where C is the number of states.

3.3.2 State Update

The detection system update the probability of each state α at each time slot by the following steps.

Estimation by State Transition from Previous State We first update $\hat{\alpha}_t(i)$ by unsing the learned state transition probability $a_k(i, j)$. The esimated current state $hat\ alpha_t(i)$ is obained by

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

where $T(t-1)$ is a function for obtaining the time of day corresponding to the time slot $t-1$.

Correction Based on Observed Value We correct $\hat{\alpha}_t(i)$ by using observation value x_t. x_t is defined by the set of operated devices at the time slot t; $n \in x_t$ if a device n is operated at time slot t. By this definition, the probability $P(x_t|S_t = i)$ is obtained by

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

where

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

Then, $\alpha_t(i)$ can be estimated by

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

3.3.3 Detection

The device can be operated at the state S_X or S_I. Thus, if the device is operated when the estimated state is S_X or S_I, the operation can be regarded as legitimate. But if the device is operated in the other states, the operation is abnormal.

Therefore, our method detect anomalous operations by checking the probability of the states of S_X and S_I. That is, we detect anomalous operations at the time slot t if the following equation is satisfied.

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

4 Evaluation

4.1 Data collection

We collected data used to evaluate our method in real homes. To collect data, we constructed a system shown in Figure 2. The system is constructed of IoT buttons and an edge computer. In this system, the edge computer stores the time when a user pushes a button.

We deployed this system in real homes. Then, we asked the subjects living in the homes to push the button when the home appliance corresponding to the button is operated. Then, we obtain the log data stored in the edge computer. Table 1 shows the list of home appliances whose corresponding buttons are deployed.

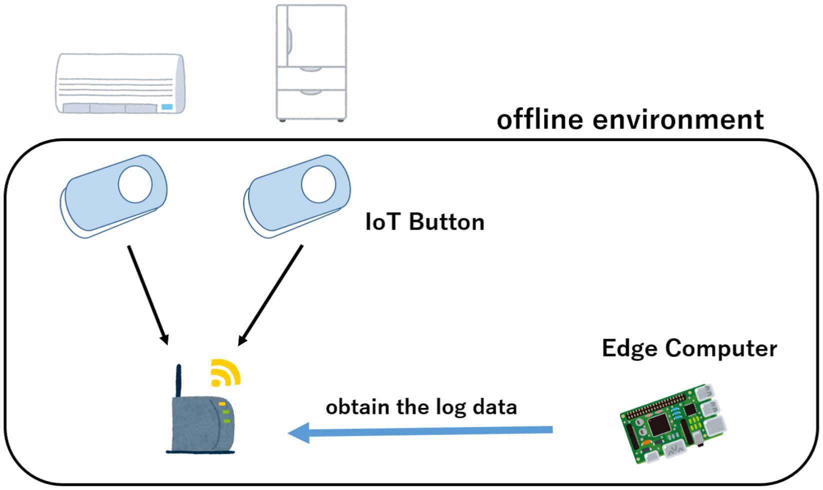

Figure 2: Data Collection Environment

In addition, we also deployed environmental sensors in the homes. We used NETATMO Smart Home Weather Station [13] as the environmental sensors. Table 2 shows the sensor data obtained from the sensor.

Table 1: Collected Device Operations

Device/Event	Action
Users Position	Entry/Exit
Lighting	ON/OFF
Air Conditioner	Cooling ON/Heating ON/Dry ON/Raise/Lower/OFF
Electric Fan	ON/OFF
Heater	ON/OFF
Washing Machine	ON
Refrigerator	OPEN
TV	ON/OFF
Cooking Stove	ON/OFF
Microwave	ON
Toaster Oven	ON
Rice Cooker	ON

Table 2: Collected Sensor Data

Sensor Data	Range	Accuracy
Room Temperature	0°C $\sim$ 50°C	±0.5°C
Humidity	0 $\sim$ 100%	±3%
Barometric Pressure	260 $\sim$ 1260mbar	±1mbar
CO2	0 $\sim$ 5000ppm	±50ppm
Noise	35 $\sim$ 120dB	

In this evaluation, we use the data collected for four months from December 2018 to March 2019. In this evaluation, we set the length of the time slot to one minute.

4.2 Settings

4.2.1 Detection Target

In this evaluation, we focus on the cooking stoves; anomalous operations on the cooking stoves are the target of detection. The cooking stoves are frequently used in a real home. Moreover, the anomalous operations on cooking stoves cause serious problems such as a fire.

4.2.2 Labeling Rule

In our method, the rules to label the log data is required to be defined in advance. In this evaluation, we use the following rules.

- Out of home: All subjects have left and the number of people in the house is zero.
- Sleeping: The state that all members of the home are sleeping. In this evaluation, this state is defined by the state that at least one subject is at home, the value of the noise sensor is less than a threshold, and no devices are used within a predefined time.
- Active: other than the above.

In this evaluation, the target device are cooking stoves operation. The state of devices is defined as follows.

- Cooking appliances are in use.
- Cooking appliances will be operated within T_X minutes
- Within T_Y minutes after cooking appliances are used
- Other case

The home we collected the dataset has cooking stoves, a microwave oven, an oven toaster, and a rice cooker. We define the state that cooking appliances are in use by the state that at least one of the above appliances are used within 15 minutes. Thus, T_y is set to a large value than 15 minutes.

The state of the house is defined by the combination of the state of users and the state of the devices. That is, the states of in-home activity are as follows.

- Outing × Cooking appliances in used
- Outing × Cooking appliances operated within T_X minutes

  ...

- Active × Cooking appliances within T_y minutes after device operation
- Active × Cooking appliances not used

Figure 3 shows the state transition model defined by the above states. In this figure, the states and transitions that never occur are omitted in.

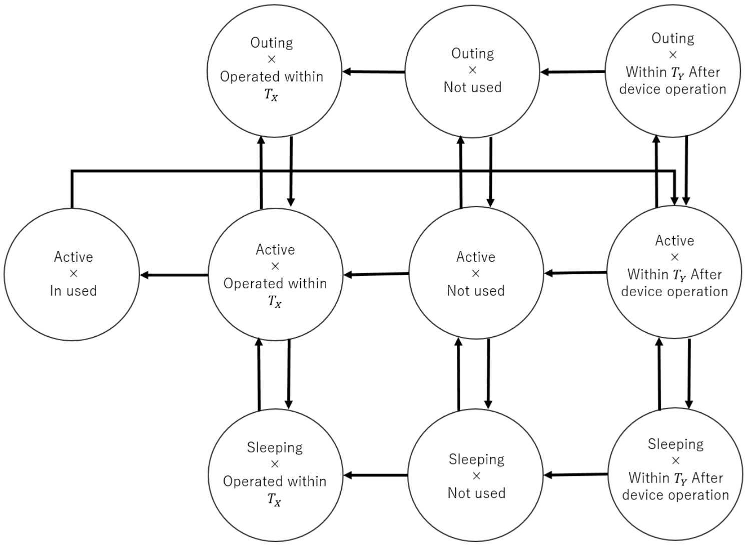
Outing × Operated within T_X
Outing × Not used
Outing × Within T_Y After device operation
Active × In used
Active × Operated within T_X
Active × Not used
Active × Within T_Y After device operation
Sleeping × Operated within T_X
Sleeping × Not used
Sleeping × Within T_Y After device operation

Figure 3: State Transition Model Used for Evaluation

4.3 Metrics

In this evaluation, because we have only a limited number of legitimate operations in our collected data, we use Leave-One-Out Cross-Validation (LOOCV) [14]. LOOCV separates a dataset into multiple smaller datasets, trains using the datasets except one of the dataset, and validates the accuracy by using the excluded dataset as the test data. Then, we summerize the all results.

In this evaluation, we divide the data into small datasets so that each dataset includes data for each day. We set one of the small datasets as the test data, and the others as the training data.

4.3.1 Detection Ratio

In this evaluation, we added anomalous operations of the cooking stoves. Then, we calculate the detection rate of them. One anomalous operation is added for each time slot. Then, we count the anomalous operations detected by our method. We define the detection rate by the ratio of the number of detected anomalous operations to the number of added anomalous operations.

4.3.2 Misdetection Ratio

We define the misdetection ratio by the raio of the number of mistakenly detected legitimate operations to the number of legitimate operations.

4.4 Compared Method

In this thesis, we focus on the estimation of in-home conditions. To demonstrate the effectiveness of our estimation for the detection of anomalous operations, we compare our method with the method that defines the condition by only the time of day.

We also discuss the impact of the parameters of our method, T_X, T_Y, and T_Z. Moreover, we discuss the importance of correction of the estimated states using the monitored value. To discuss the above point, we also compare our method with the method that does not use the monitored information to estimate the current state. That is, this method uses only the state transition probabilities.

4.5 Result

Figure 4 compares the results of our method with those of the method defining the conditions by only the time of day. In this evaluation, we set the parameters of our method by $T_X = 30$, $T_Y = 30$, and $T_Z = 30$. This figure compares the method by an ROC (Receiver Operatorating Characteristic) curve. .

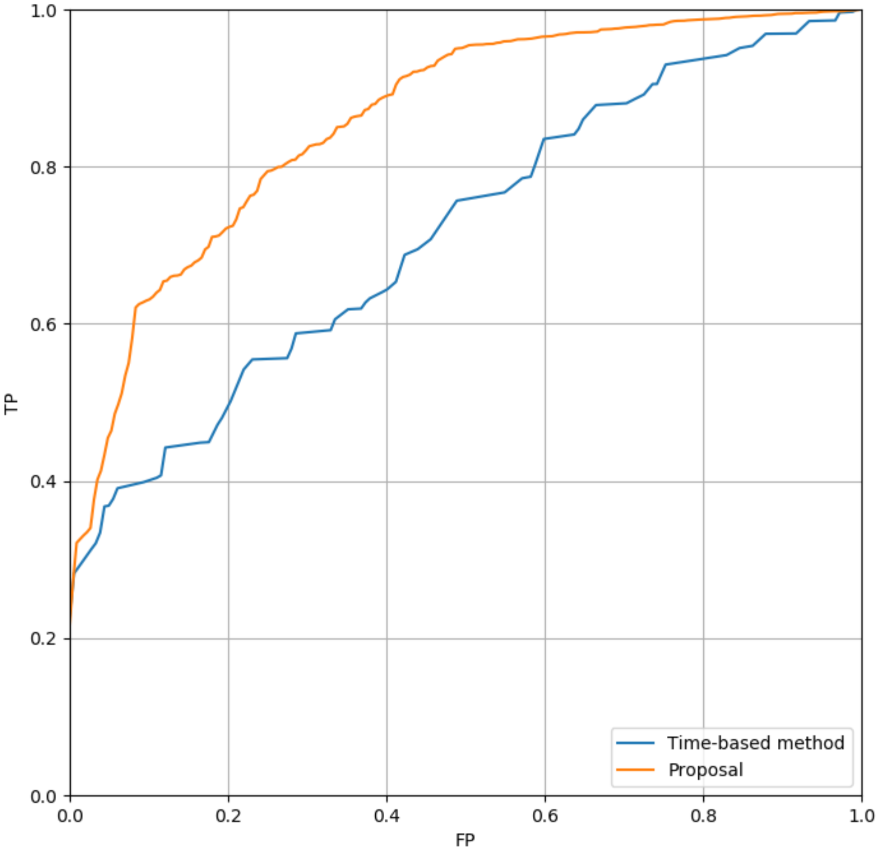

Figure 4: Comparison with Time Only Method

The results shows that our method detect anomalous operations more accurately than the mothod defining the conditions by the time of day. This is because our method accurately estimates the state that cooking stoves tend to be used.

We also evaluate the impact of parameters of our method.

Figure 5 shows the impact of parameter T_X. In this figure, T_X is set to 0, 5, and 60, where $T_Y = 30$ and $T_Z = 30$. Note that the case of $T_X = 0$ is the case that the state of the time before using the cooking appliances does not exist.

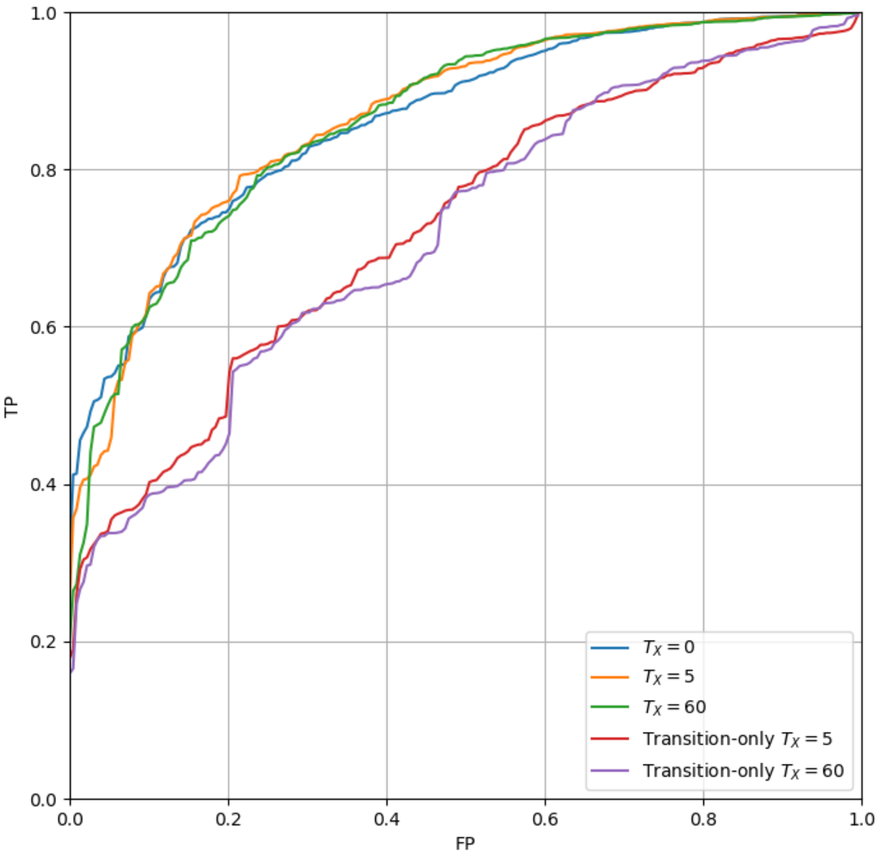

Figure 5: Comparison ROC Curves of Existing Studies at T_X

The results indicate that T_X does not have a large impact on the detection of anomalous operations. If T_X is set to short, the probability of the state S_X becomes also small. But even in such a case, by setting the threshold θ to a small value, we can achieve a similar detection performance.

We also compare the impact of T_X on the method using only the state transition model. The results indicate that the detection rate of the method using only the state transition model is significantly smaller than our method. That is, the correction of the estimated states based on the observed information is required to accurately estimate the state. This figure also indicates the correction of the estimated states also mitigates the impact of T_X.

We also investigate the impact of T_Y. We set T_Y to 0, 30, and 180, where $T_X = 30$ and $T_Z = 30$. Figure 6 shows the results.

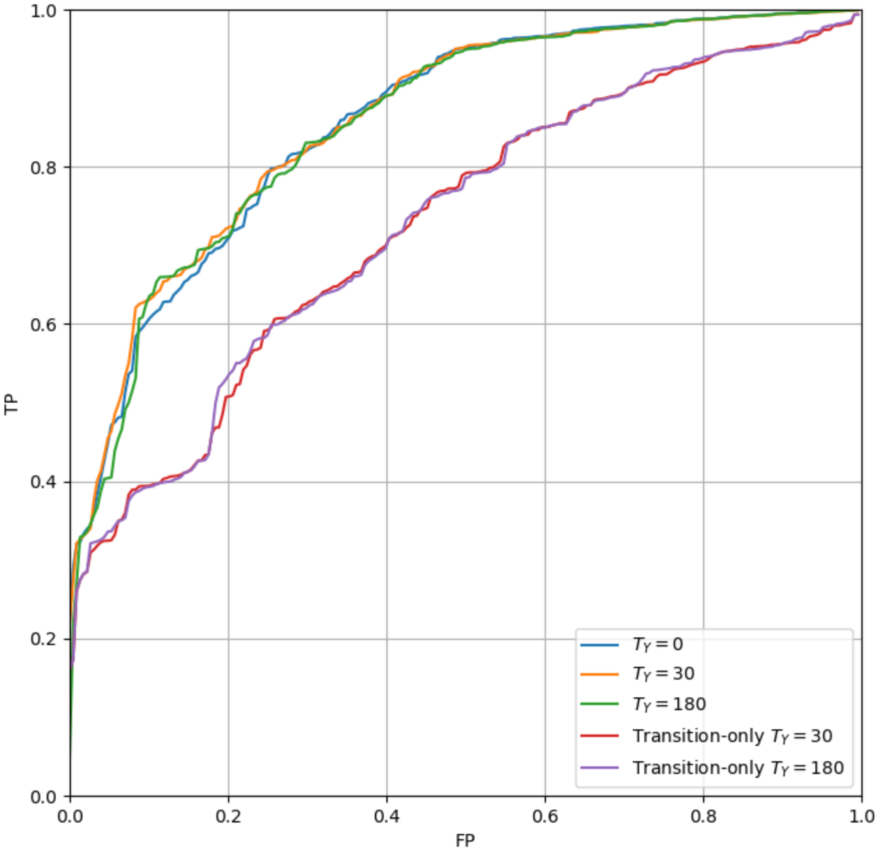

Figure 6: Comparison ROC Curves of Existing Studies at T_Y

Similar to T_X, T_Y does not have a large impact on detection performance. We also compare the impact of T_Y on the method using only the state transition model. The results show that T_Y does not have a large impact even on the method using only the state transition probabilities. This is because the difference between S_Y and S_N is small. As a result, the state S_Y does not have an impact on the detections of anomalous operations. If we can clearly distinguish S_Y from S_N by adding more sensors and so on, S_Y may become important.

Finally, we investigate the impact of T_Z. We set T_Z to 30, 60, and 720, where $T_X = 30$ and $T_Y = 30$. Note that the case of $T_Z = 720$ is the case that we do not divide the state transition probabilities by the time of day. Figure 7 shows the results.

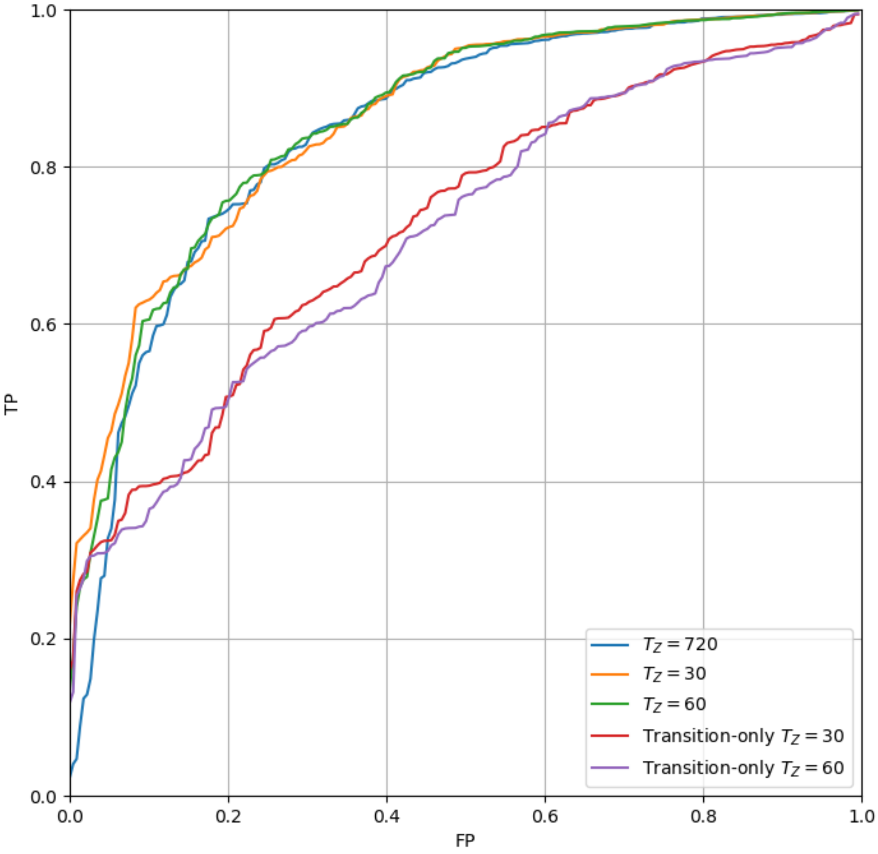

Figure 7: Comparison ROC Curves of Existing Studies at T_Z

Similar to T_X and T_Y, T_Z does not have a large impact on detection performance. We also compare the impact of T_Z on the method using only the state transition model.

Simialr to T_X, the results indicate that the correction of the estimated states mitigates the impact of T_Z.

4.6 Discussion

The results in the previous subsection indicates that our method achieves higher detection rate than the method defining the condition by only the time of day. This is because our method accurately estimates the state that cooking stoves tend to be used.

In addition, the impact of the correction of the estimated states based on the monitored information has a large impact on the accurate detection of the anomalous operations. This is because the number of states of home to be estimated is small. The state of the home does not change frequently. As a result, the state transition probabilities are estimated as small values. This is why the impact of the correction of the estimated states is larger than that of the state transition. If we can define the states of home in more fine granularity, the number of states becomes large and the state transition probabilities from a state to another state may be large. In this case, the state transtion probabiites becomes more important.

The accuracy of the sensors has also impact on the accuracy of the detection. In our evaluation, the state of sleeping is defined by the values of the noise sensor. However, this definition may cause the labeling errors; if the users are active but the noise level is small, we mistakenly label the case as sleeping. Such labeling errors may have an impact on the detection performance. If we have sensors that are used to accurately estimate the state of users, our method can achieve more accurate detection.

5 Conclusion and Future Work

In this thesis, we proposed 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. Then, 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 evaluated 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.

This thesis focuses on the estimation of the condition of the home. But another model such as sequences of the operations can be used for the detection of anomalous operations. The combination of our method and such methods may achieve more accurate detection of the anomalous operations, which is one of our future research topics.

Acknowledgments

This thesis would not accomplish without a lot of great support from many people. First, I would like to express my deepest gratitude to Professor Masayuki Murata of Osaka University, for providing me with the opportunity to research with a talented team of researchers. His creative suggestions, insightful comments, and patient encouragement have been essential for my research activity.

Furthermore, I would like to show my greatest appreciation to Associate Professor Yuichi Ohsita of Osaka University. He devoted a great deal of time for me and gave me a lot of advice about my research. Without his continuous support, my work would not be accomplished. In addition, he enthusiastically taught me the way of thinking and writing. They must be invaluable skills in the future of my life. Moreover, I would like to show my appreciation to Associate Professor Shin'ichi Arakawa, Assistant Professor Daichi Kominami, and Specially Appointed Assistant Professor Tatsuya Otoshi of Osaka University for appreciated comments and support. Their kindnesses on my behalf were invaluable, and I am forever in debt.

I am grateful to Dr. Yoshiaki Kato, Dr. Akira Ishihara, Dr. Takeshi Yoneda, Dr.Shotaro Miwa, Dr. Isao Otsuka, Mr. Tsutomu Yoshikawa, Mr. Masao Noguchi, and Mr.Kensuke Ueda of Mitsubishi Electric Corporation for providing me many valuable comments. The opportunity of discussion at the Mitsubishi Electric Cybersecurity ResearchAlliance Laboratories improved my explanation capability. I am also grateful to Professor Toru Fujiwara, Assistant Professor Naoto Yanai of OsakaUniversity, and Assistant Professor Yuya Tarutani of Okayama University, for their adviceof my research and experimental environment. Their advice from different perspective points of view was always informative and helpful.

Moreover, I would like to thank Mr. Masaaki Yamauchi. He gives insightful comments and suggestions. I would like to thank all the members of Advanced Network Architecture Research Laboratory at the Graduate School of Information Science and Technology, Osaka University,for their inciting discussions and fellowship.

Last, but not least, I thank my family for their invaluable support and constant encouragement during my master studies.

References

[1] K. L. Lueth *et al.*, "State of the iot 2018: Number of iot devices now at 7b–market accelerating," *IoT Analytics*, vol. 8, 2018.

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

[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, 2015.

[4] M. Capellupo, J. Liranzo, M. Z. A. Bhuiyan, T. Hayajneh, and G. Wang, "Security and attack vector analysis of iot devices," in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage.* Springer, 2017, pp. 593–606.

[5] 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.

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

[7] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, 2017.

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

[9] N. Amraoui, A. Besrour, R. Ksantini, and B. Zouari, "Implicit and continuous authentication of smart home users," in *International Conference on Advanced Information Networking and Applications.* Springer, 2019, pp. 1228–1239.

[10] S. Ramapatruni, S. N. Narayanan, S. Mittal, A. Joshi, and K. Joshi, "Anomaly detection models for smart home security," in *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS).* IEEE, 2019, pp. 19–24.

[11] K. Ueda, M. Tamai, and K. Yasumoto, "A method for recognizing living activities in homes using positioning sensor and power meters," in *2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops).* IEEE, 2015, pp. 354–359.

[12] K. Nakahara, H. Yamaguchi, and T. Higashino, "In-home activity and micro-motion logging using mobile robot with kinect," in *Adjunct Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services*, 2016, pp. 106–111.

[13] "NETATMO Smart Home Weather Station," https://www.netatmo.com/en-us/weather.

[14] N. M. Nasrabadi, "Pattern recognition and machine learning," *Journal of electronic imaging*, vol. 16, no. 4, p. 049901, 2007.