1

Evaluation of Functional Estimation Methods in IoT Devices at Intervals of a Few Seconds by Communication Traffic Analysis

Yuichi HATTORI* [1], Yutaka ARAKAWA [2], Sozo INOUE [3]
[13]Department of Life Science and Systems Engineering, Graduate School of Life Science and Systems Engineering, Kyushu Institute of Technology,
[2]Department of Advanced Information Technology, Faculty of Information Science and Electrical Engineering, Kyushu University

Abstract

In recent years, IoT devices have become widespread in households, and IoT devices with various functions are sold and used in various situations. However, current IoT devices are black boxes in operation, and there is no way to detect when an IoT device is communicating in a suspicious manner. Therefore, we are aiming to realize a framework called the IoT activity tracker that has a function of access control, which can detect what kind of communication IoT devices are doing and allow only appropriate communication based on it, and a function that enables users to understand the operation status of IoT devices by visualizing what kind of communication IoT devices are doing. To achieve the IoT activity tracker, it is necessary to estimate the function in a few seconds of communication traffic. In this study, we used 8 models of IoT devices to estimate functions at intervals of a few seconds, and estimated 3 functions, including a state in which nothing is being executed, using features at intervals of 1 second. As a result, it was confirmed that the function could be estimated with an accuracy of 83% or higher for 5 of the 8 models, respectively.

[1] hattori.yuichi636@mail.kyutech.jp
[2] arakawa@ait.kyushu-u.ac.jp
[3] sozo@brain.kyutech.ac.jp

1 Introduction

In recent years, IoT devices have become widespread in households, and IoT devices with various functions are sold and used in various situations. These devices are expected to become even more prevalent in the future; according to a survey by Japan's Ministry of Internal Affairs and Communications, the number of IoT devices worldwide in 2021 was about 29.2 billion and predicted to increase to 40 billion by 2024[7]. For example, well-known IoT devices used in the home include smart speakers such as Google Home and Amazon Echo. These devices are equipped with a voice user interface (VUI) that allows users to use their voice to perform various functions such as searching the Internet, operating home appliances, and playing music. Some devices are also equipped with cameras, allowing video calls with other IoT devices and smartphones. Network cameras are also readily available from home centers and mail-order sites and are being used in conjunction with smartphones and smart speakers for applications such as watching over children and crime prevention. These IoT devices are essentially designed to work with the cloud, and their functionality allows them to work with smartphones and other devices. These IoT devices are connected to dedicated cloud-like servers and other systems via Wi-Fi networks in the home and provide services by collecting and analyzing the data produced by the devices. Users can access these systems from their smartphones to control their devices and view information.

According to the NICTER[10] observation report for FY2022, a cyber-attack observation and analysis system conducted by National Institute of Information and Communications Technology(NICT), which aims to understand the general trends of indiscriminate cyber-attacks, active IoT BOT infection activities, such as Mirai subspecies, have been observed since last year, and the number of hosts in Japan has increased to approximately 5000 at its peak[9].

Since IoT devices are designed to be connected to external networks, they pose many problems in terms of information security, and there have been incidents of them being used as a springboard for various personal information leaks and attacks. For example, it has been confirmed that home routers send data to third parties even when the function for linking with services provided by third parties is turned off from the management screen[15].

Various precautions need to be taken when using IoT devices. In particular, we believe the following 3 points need to be considered.

1. The diversity of IoT devices is so high that it is difficult to continuously update the security of all devices. New devices are being released all the time, but the rate of firmware updates is not keeping pace with that for PCs. Devices manufactured by large companies are more likely to receive consistent and regular firmware updates and support, whereas devices manufactured by smaller companies

may not receive firmware updates or support due to factors such as early service termination or bankruptcy of the company itself.

2. The activity of IoT devices is a black box, often operating independently of the user's intentions regarding what data the device is sending and where. After the device has been initially connected to the network, the user often does not know which server the IoT device is connected to, what protocols they are using, or how often they connect to the network. More recently, as a result of incidents in Zoom video conferences, it has been discovered that network communications may be routed through certain countries[16]. Also, the route used for network communication is usually encrypted, which means that ordinary users cannot check it.
3. Unlike PCs, users cannot install fraud detection systems, such as anti-virus software, on IoT devices.

Therefore, we propose a framework called the IoT activity tracker for the safe use of IoT devices around the home[5]. The IoT activity tracker identifies the types of IoT devices and their triggering functions based on communication traffic pattern analysis, so that the user knows which IoT devices in the home are performing what kind of communication. At the same time, it allows users to easily control the communication related to the function, such as temporarily or permanently blocking it, through their smartphones. Smartphone permissions are visible and can be managed. We propose to set permissions for each smartphone app for IoT devices in the home. We also propose a feature that allows permissions to be visualized and easily configured for each function, similarly to permission settings on a smartphone. To realize our proposed functionality, it is important to analyze the communication traffic to determine which functions are executed by which IoT devices. In previous studies[17], the accuracy was 91% for the estimation of a total of 16 execution functions for a total of 8 IoT devices of 4 types, 2 models each, and 73% for the estimation of 8 types of execution functions only. However, conventional methods compute and estimate features from all communication traffic when a function is executed, and thus require detection of the execution and termination of the function in order to use them for communication control. Therefore, it is difficult to control communication from a few seconds of communication. In this paper, to solve this problem, we used machine learning to estimate the execution state of IoT device functions by using feature values per second, and evaluated the accuracy of the estimation. As with previous methods, we used feature values that do not contain personally identifiable information extracted by calculating the amount of communication traffic. Then, function estimation was performed for eight models of IoT devices for function estimation at intervals of a few seconds, using features at intervals of one second for estimation of three functions, including the state in which nothing is being executed. As a result, we confirmed that functions could be estimated with an accuracy of 83% or better for 5 of the 8 models. The communication traffic used was the communication traffic for 8 different functions of 8 different IoT devices distributed in Japan, including smart speakers, smart cameras, smart remote controls, smart plugs, and 2 each of 4 different types of IoT devices, which were collected in previous studies[17].

The structure of this paper is as follows. In Section 2, we describe related work on IoT traffic analysis. In Section 3, we describe the functional estimation methods in IoT devices at intervals of a few seconds by communication traffic analysis, and its evaluation is presented in Section 4. In Section 5, we discuss the our proposal. Finally, we conclude our paper in Section 6.

2 Related Work

Smart home and IoT devices have been studied in a variety of ways. In this section, we describe related work on IoT device identification and privacy.

2.1 Research describing end-user security and privacy concerns with smart homes

Zeng et al. studied end-user security and privacy concerns with smart homes[18]. They conducted interviews with 15 people living in smart homes to learn about how they used their smart homes and to understand their security- and privacy-related attitudes, expectations, and actions. On the basis of these interviews, they concluded that users are not particularly interested in the security of smart home devices. However, they claimed that creating a device information visualization system would be a potential way to increase interest in device-related security concerns for the end user. Thus, our research not only helps to detect unauthorized communication but also increases awareness among users of device-related security.

2.2 Research describing vulnerabilities of IoT communication privacy

Apthorpe et al. reported privacy vulnerabilities of encrypted IoT traffic[1]. By analyzing four commercially available smart home devices (Sense sleep monitor, Nest Cam indoor security camera, Wemo remote switch, Amazon Echo smart speaker), they demonstrated that the rate of network traffic can reveal user activity. This is because user behavior can be estimated using only the transmission and reception rates of encrypted traffic, as IoT devices transform real-world information into network traffic. Therefore, they can warn users about potential privacy threats. Of course, whereas it is important to protect traffic information that could enable potential attackers to estimate user behavior, it is also important to visualize activity information and report it to users for security monitoring purposes.

In this study, user behavior is estimated from communication traffic rates, but only specific behaviors are estimated, such as "asking questions" for smart speakers and "motion detection" for smart cameras. Our study classifies the execution of several functions, including stationary states.

Dong et al. investigated how personal information can be leaked from network traffic generated by smart home networks[3]. They proposed a framework for device identification using the temporal relationship between packets, which identifies the device type with high accuracy. The results suggest that IoT network communications, even when protected by encryption and morphed by network gateways, pose significant challenges to user privacy. These studies in which activity information is presented to users by analyzing the network traffic of IoT devices help to detect suspicious network communication.

This study identifies IoT devices but does not classify their functions. Our study does classify functions. As a result, our research will also raise the issue of privacy in IoT devices.

2.3 IoT device identification by network traffic analysis

Although we identify a function by analyzing the network traffic of an IoT device in this study, the identification of IoT devices has been addressed in previous research.

Meidan et al. proposed a method for the identification of IoT devices and non-IoT devices using network traffic analysis with machine learning[6]. By analyzing a saved file that contains traffic information of devices connected to Wi-Fi, they identified the devices in two stages using supervised machine learning while abstracting features such as source address, destination address and port number. In the first stage, they identified whether a device is an IoT device. In the second stage, they identified the device class from a list of registered identified IoT devices. As a result, they identified the types of IoT devices with 99.281% accuracy.

Sivanathan et al. proposed a method of identifying IoT devices in a smart city and on a campus. They set 21 IoT devices on a campus and collected traffic data for 3 weeks[14]. Then, by analyzing wide network traffic (e.g., traffic load, signaling patterns, and distribution of active and sleep times), they identified the devices using a supervised learning algorithm. As a result, they identified the types of IoT devices with 95% accuracy.

Sivanathan et al. developed a modular device classification architecture and used unsupervised clustering methods to identify 10 devices with an accuracy of over 94% using actual IoT device traffic[12]. They also developed a modular device classification architecture with a clustering model that identifies behavioral changes with an accuracy of over 94% for 12 devices using actual IoT device traffic[13].

Although these studies identified devices and detected changes in behavior with a high degree of accuracy, they were not able to identify device functions. In this study, we identify the functions of devices.

2.4 Security system for IoT device using network gateway

Miettinen et al. proposed a system that can automatically identify the types of IoT devices connected to a network, limit the communication of vulnerable devices, and minimize damage[8]. Their proposed approach was to identify IoT devices by profiling the communication behavior specific to each type of device. Although the system controlled the communication of vulnerable devices based on the results of device estimation, it did not control the communication based on the functions of the devices. Our proposed system controls communication at the function level of the devices.

2.5 Smartphone permissions vs smart home permissions

The management of usage resources (communications, sensors, external storage) related to smartphones is an important issue from the perspectives of privacy and security.

Currently, smartphone permissions are visible and can be managed in two different ways: by setting permissions for each app and by setting apps for each permission. There are also four types of permissions on Android devices: all the time (location only), ask every time, allow only while using the app and do not allow[4]. In the past, location information was obtained by applications without user consent, raising privacy issues, so this type of functionality was implemented.

For a smart home, an IoT device is the equivalent of an app on a smartphone. For smart homes, as with smartphones in the past, we do not know which IoT devices are doing what. Another problem is that IoT devices may unnecessarily communicate with third-party destinations[15] In other words, it is necessary to control the resources used in the smart home, just as we do with smartphones today. Our proposed IoT activity tracker can control the resources used in a smart home, and this paper describes a communication traffic control mechanism to control the resources.

2.6 Malicious software detection with network traffic analysis

Network traffic analysis is also often used in the detection of malicious software.

Bendiab et al. proposed proposing a novel IoT malware traffic analysis approach using deep learning and visual representation for faster detection and classification of new malware. They created a dataset of 1000 pcap files of normal and malware traffic that are collected from different network traffic sources. After analyzing them, malware traffic was detected with 94.50% accuracy[2].

Nobakht et al. proposed an advanced and intelligent IoT malware detection model based on deep learning and ensemble learning algorithms called DEMD-IoT (Deep Ensemble Malware Detection for IoT). They evaluated the DEMD-IoT using IoT-23 dataset, which contains IoT network traffic. As a result, 99.9% accuracy was achieved. [11].

This research does not detect malicious communications, but rather classifies the communication traffic of the normal execution functions of IoT devices. Our goal is to create an environment in which users can better control necessary communications by classifying normally executing functions from communication traffic.

3 Functional Estimation Methods in IoT Devices at Intervals of a Few Seconds by Communication Traffic Analysis

In this section, we describe our proposed IoT activity tracker, the dataset used for estimation, and function estimation method.

3.1 IoT activity tracker

Figure 1 shows the outline of the IoT activity tracker. The IoT activity tracker consists of an edge router and a management system. The edge router is installed at home and the management system is installed in the cloud. The IoT activity tracker is intended for use in the home, in an environment where multiple IoT devices are connected to a router, either wired or wirelessly. In other words, it assumes an environment in which the router collects the communication traffic sent and received from all connected devices. This router part is called an edge router in the IoT activity tracker. The system is provided as a web application that enables users to visualize the usage status based on the communication traffic collected by the edge router and to configure the communication availability of IoT devices installed in the smart home using smartphone and reflect the settings in the edge router. The Web application that provides these functions, located in the cloud, is called a management system in the IoT activity tracker.

3.2 Dataset used for Estimation

The dataset used was a total of 16 different communication traffic datasets of 8 models, 2 for each of the 4 types of IoT devices collected in the previous

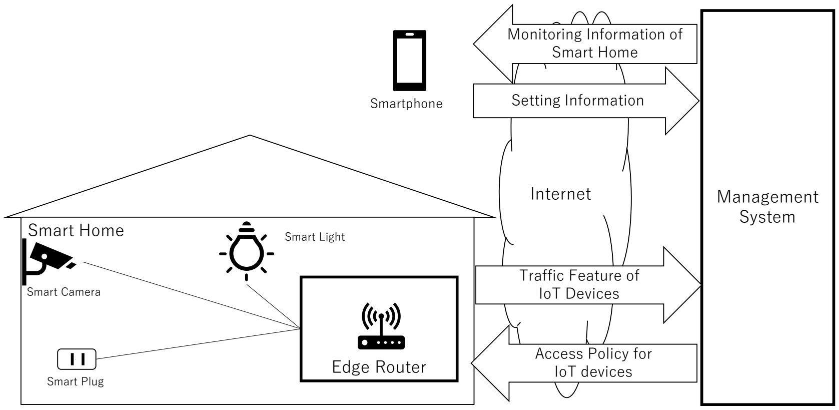


FIGURE 1: Outline of IoT activity tracker

TABLE 1: List of IoT devices for communication traffic used

	Device Type	Name	Developer
1	Smart Camera	Ranger 2	Imou
2		Mi 360°	Xiaomi
3	Smart Remote Controller	SwitchBot Hub Mini	SwitchBot
4		Nature Remo	Nature
5	Smart Speaker	Amazon Echo Show	Amazon
6		Google Home Mini	Google
7	Smart Plug	SwitchBot Plug	SwitchBot
8		WiFi Smart Plug	TP-Link

study[17]. The list of IoT devices and functions are shown in Table 1 and Table 2.

3.3 Function Estimation Method

It is important to analyze which function of which IoT device is executed from the communication traffic as an important function to control the communication availability of the IoT devices of the IoT activity meter described in Section 3.1. The proposed method estimates the functions of IoT devices by learning their communication traffic patterns through machine learning. In the previous study, the accuracy was 91% for the estimation of 16 execution functions for a total of 8 models, 2 for each of the 4 types of IoT devices, and 73% for the estimation of 8 types of execution functions only. However,

TABLE 2: List of functions of IoT devices for communication traffic used

	Device Type	Function
1	Smart Camera	Talk to smart camera
2		Change camera direction(Rotate left, 3sec)
3	Smart Remote Controller	Turn on the TV
4		Mute the TV
5	Smart Speaker	Play music(10sec)
6		Ask for today's weather
7	Smart Plug	Turn on power
8		Turn off power

conventional methods compute and estimate features from all communication traffic when a function is executed, and thus require detection of the execution and termination of the function in order to use them for communication control. Therefore, it is difficult to control communication from a few seconds of communication. It also does not take into account the state in which IoT devices are not doing their functions. To solve this problem, we propose a method to estimate the execution state of IoT device functions using machine learning every second. To build an estimation model to be used in an actual IoT activity meter, we evaluated the accuracy of each device using the communication traffic of IoT devices distributed in Japan, as described in Section 3.2. The features were computed using the communication traffic up to 3 seconds before each second, and only those that did not contain personally identifiable information were used. Using features related to the individual or manufacturer, such as destination IP or MAC address, would improve accuracy, but would need to be updated as new products are added. There are also privacy concerns when using them. Therefore, we focused on features derived from the volume of communication. The calculated features are shown in Table 3 and 4. The importance of the features was calculated from among them using a random forest algorithm, and the features up to the 39th feature in order of importance were used. The machine learning algorithm used was random forest algorithm, which is supervised machine learning, and was evaluated by 10-fold cross-validation.

4 Evaluation

To test the validity of the functional estimation method, a random forest algorithm was used and evaluated by cross-validation of 10 segments.

In addition, since the focus of this study is on classification of functions,

TABLE 3: List of calculated feature values 1

No.	**Feature Value**
1	Number of packets sent in 1 sec
2	Maximum packet size sent in 1 sec
3	Minimum packet size sent in 1 sec
4	Number of packets received in 1 sec
5	Maximum packet size received in 1 sec
6	Minimum packet size received in 1 sec
7	Number of TCP packets in 1 sec
8	Number of UDP packets in 1 sec
9	Maximum TCP packet size in 1 sec
10	Minimum TCP packet size in 1 sec
11	Maximum UDP packet size in 1 sec
12	Minimum UDP packet size in 1 sec
13	Number of source IPs in 1 sec
14	Number of destination IPs in 1 sec
15	Mean of packet size sent in 1 sec
16	Variance of packet size sent in 1 sec
17	Standard deviation of packet size sent in 1 sec
18	Mean of packet size received in 1 sec
19	Variance of packet size received in 1 sec
20	Standard deviation of packet size received in 1 sec
21	Mean of TCP packet size in 1 sec
22	Variance of TCP packet size in 1 sec
23	Standard deviation of TCP packet size in 1 sec
24	Mean of UDP packet size in 1 sec
25	Variance of UDP packet size in 1 sec
26	Standard deviation of UDP packet size in 1 sec
27	Number of packets sent in 2 sec
28	Maximum packet size sent in 2 sec
29	Minimum packet size sent in 2 sec
30	Number of packets received in 2 sec
31	Maximum packet size received in 2 sec
32	Minimum packet size received in 2 sec
33	Number of TCP packets in 2 sec
34	Number of UDP packets in 2 sec
35	Maximum TCP packet size in 2 sec
36	Minimum TCP packet size in 2 sec
37	Maximum UDP packet size in 2 sec
38	Minimum UDP packet size in 2 sec
39	Number of source IPs in 2 sec
40	Number of destination IPs in 2 sec

TABLE 4: List of calculated feature values 2

No.	Feature Value
41	Mean of packet size sent in 2 sec
42	Variance of packet size sent in 2 sec
43	Standard deviation of packet size sent in 2 sec
44	Mean of packet size received in 2 sec
45	Variance of packet size received in 2 sec
46	Standard deviation of packet size received in 2 sec
47	Mean of TCP packet size in 2 sec
48	Variance of TCP packet size in 2 sec
49	Standard deviation of TCP packet size in 2 sec
50	Mean of UDP packet size in 2 sec
51	Variance of UDP packet size in 2 sec
52	Standard deviation of UDP packet size in 2 sec
53	Number of packets sent in 3 sec
54	Maximum packet size sent in 3 sec
55	Minimum packet size sent in 3 sec
56	Number of packets received in 3 sec
57	Maximum packet size received in 3 sec
58	Minimum packet size received in 3 sec
59	Number of TCP packets in 3 sec
60	Number of UDP packets in 3 sec
61	Maximum TCP packet size in 3 sec
62	Minimum TCP packet size in 3 sec
63	Maximum UDP packet size in 3 sec
64	Minimum UDP packet size in 3 sec
65	Number of source IPs in 3 sec
66	Number of destination IPs in 3 sec
67	Mean of packet size sent in 3 sec
68	Variance of packet size sent in 3 sec
69	Standard deviation of packet size sent in 3 sec
70	Mean of packet size received in 3 sec
71	Variance of packet size received in 3 sec
72	Standard deviation of packet size received in 3 sec
73	Mean of TCP packet size in 3 sec
74	Variance of TCP packet size in 3 sec
75	Standard deviation of TCP packet size in 3 sec
76	Mean of UDP packet size in 3 sec
77	Variance of UDP packet size in 3 sec
78	Standard deviation of UDP packet size in 3 sec

classification of devices was not performed. Therefore, we evaluated the functional estimation method as if the devices were already classified.

For each model, features of up to the 39th importance were used. The importance of the features for each model are shown in Figure 2 and Figure 3. No contribution was made with respect to UDP-related features in all models. Smart speakers with more communication contribute more features related to 1 sec, and smart plugs contribute more features related to sent packet size.

As a result, 5 of the 8 models could be classified with an accuracy of 83% or better, but three models were not classified well, with an accuracy in the 60% range. The confusion matrix for each model is shown in Table5-Table12, and its class labels are listed in Table13. Table14 lists the classification accuracy of the function estimation results for each model. In particular, the accuracy of both smart remote controls is lower than that of the other two models. This is partly due to the fact that the number of communications required to execute the function is small, but the smart remote control transmits infrared signals for the function for which it receives instructions, and the actual communications are almost identical, making it difficult to classify them based on communication traffic information alone. The accuracy of the smart camera Mi 360° is also considered to be low because there is almost no difference in the actual communication. The difference between the accuracy of Ranger 2, another smart camera, and that of Mi 360° is due to the difference in communication between the two cameras, which are implemented by different developers. As for the part where the stationary state is misrecognized, the misrecognition is considered to have occurred because IoT devices may be communicating in some way even though they are stationary.

TABLE 5: Confusion matrix of function estimation results(Ranger 2:Smart Camera)

	0	**1**	**2**
0	10	0	0
1	0	10	0
2	0	0	10

TABLE 6: Confusion matrix of function estimation results(Mi 360°:Smart Camera)

	0	**1**	**2**
0	10	0	0
1	2	5	3
2	0	5	5

5 Discussion

In this section, we discuss several important issues: impact of IoT device settings, impact of IoT device updates, different function but similar communication traffic, etc.

TABLE 7: Confusion matrix of function estimation results(SwitchBot Hub Mini:Smart Remote Controller)

	0	**3**	**4**
0	18	0	1
3	0	15	4
4	0	15	4

TABLE 8: Confusion matrix of function estimation results(Nature Remo:Smart Remote Controller)

	0	**3**	**4**
0	10	0	0
3	1	5	4
4	0	5	5

TABLE 9: Confusion matrix of function estimation results(Amazon Echo Show:Smart Speaker)

	0	**5**	**6**
0	70	0	2
5	0	59	13
6	0	6	66

TABLE 10: Confusion matrix of function estimation results(Google Home Mini:Smart Speaker)

	0	**5**	**6**
0	33	3	2
5	1	27	7
6	2	2	30

TABLE 11: Confusion matrix of function estimation results(SwitchBot Plug:Smart Plug)

	0	**7**	**8**
0	10	0	0
7	0	9	1
8	0	0	10

TABLE 12: Confusion matrix of function estimation results(WiFi Smart Plug:Smart Plug)

	0	**7**	**8**
0	10	0	0
7	0	7	3
8	0	2	8

TABLE 13: Class labels of Table 5-12

Class Label	**Detail**
0	Stationary state
1	Change camera direction(Rotate left, 3sec)
2	Talk to smart camera
3	Mute the TV
4	Turn on the TV
5	Play music(10sec)
6	Ask for today's weather
7	Turn off power
8	Turn on power

TABLE 14: List of classification accuracy of function estimation results for each device

	Device Type	Name	Accuracy
1	Smart Camera	Ranger 2	100%
2		Mi 360°	67%
3	Smart Remote Controller	SwitchBot Hub Mini	65%
4		Nature Remo	67%
5	Smart Speaker	Amazon Echo Show	90%
6		Google Home Mini	83%
7	Smart Plug	SwitchBot Plug	97%
8		WiFi Smart Plug	83%

5.1 Impact of IoT device settings

In this paper, data was collected and evaluated in Japanese because the target language was IoT devices distributed in Japan. However, IoT devices are distributed in various countries, and even similar functions may have different characteristics depending on language settings, location information, and other factors. Therefore, the impact of IoT device configuration should also be considered.

5.2 Impact of IoT device updates

IoT devices are subject to periodic software updates, which may cause changes in communication destinations and traffic. Application updates must also be considered for IoT devices that allow additional third-party applications to be installed, such as smart speakers. Therefore, it is necessary to build a mechanism to collect communication traffic after an update and perform learning.

5.3 Functions that are performed regardless of the user's actions

The functions estimated in this study are those that are executed by the user giving instructions, and those that are not executed by the user. However, IoT devices are communicating through updates and other means even without instructions from the user. Unlike functions that are executed by the user's instructions, it is difficult to collect communication traffic because functions cannot be executed at arbitrary times.

5.4 Different function but similar communication traffic

Many IoT devices communicate over HTTPS and are encrypted. Since this method does not check the contents of the communication, it uses feature values such as the size of packets during transmission and the number of packets during reception. In addition, many IoT devices receive and send data in formats such as JSON, and some communications occur only a few times, with little difference in content. In particular, in the case of smart remote controls, there is little difference in the content because commands are basically sent to an infrared transmitter regardless of which function is used. Therefore, it is difficult to classify them based on communication traffic alone. In order to actually detect these functions, it is necessary to link them with existing action recognition technology and to link them with the room occupancy status.

5.5 How much accuracy is needed to realize an IoT activity tracker?

Our proposed IoT activity tracker has the ability to temporarily or permanently block communication of certain functions of IoT devices based on communication traffic pattern analysis. In order to actually control communication traffic in an IoT activity meter, high accuracy is required because normal communication must not be interfered with. Therefore, to use the system in a real environment, it would need to be more accurate than the results of the this study.

6 Conclusion

In this paper, we presented a function estimation method in IoT devices at intervals of a few seconds by analyzing the communication traffic of IoT devices to realize our proposed control of communication in units of functions performed by IoT devices used in IoT activity tracker. Then we used machine learning to classify devices and functions using features extracted from communication traffic without personally identifiable information to evaluate their accuracy. In 5 of the 8 IoT devices actually distributed in Japan, 2 each of the 4 types of IoT devices, we were able to classify the estimation of 3 types of functions, including static, with an accuracy of 83% or better, using features per second, while three of the devices were not classified well, with an accuracy in the 60% range. In order to actually control communication traffic in an IoT activity tracker, high accuracy is required because normal communication must not be interfered with. Although some IoT devices were identified with an accuracy of 83% or better in this study, further improvement in accuracy is needed to introduce these devices into the actual environment.

In the future, we will further increase the number of types of IoT devices and the number of functions they perform, and improve the accuracy by improving the value of the features. We also plan to prepare a smart home environment in which IoT devices and the IoT activity tracker we are developing are actually installed, and verify whether the IoT activity tracker can control communication of specific functions in a real environment. In addition, the system works in conjunction with existing action recognition technology to identify whether the communication is intended by the user, visualize the results, and control communication, aiming to realize a world in which users can use IoT devices with greater peace of mind.

Acknowledgement

This work was supported by JSPS KAKENHI (JP19KT0020).

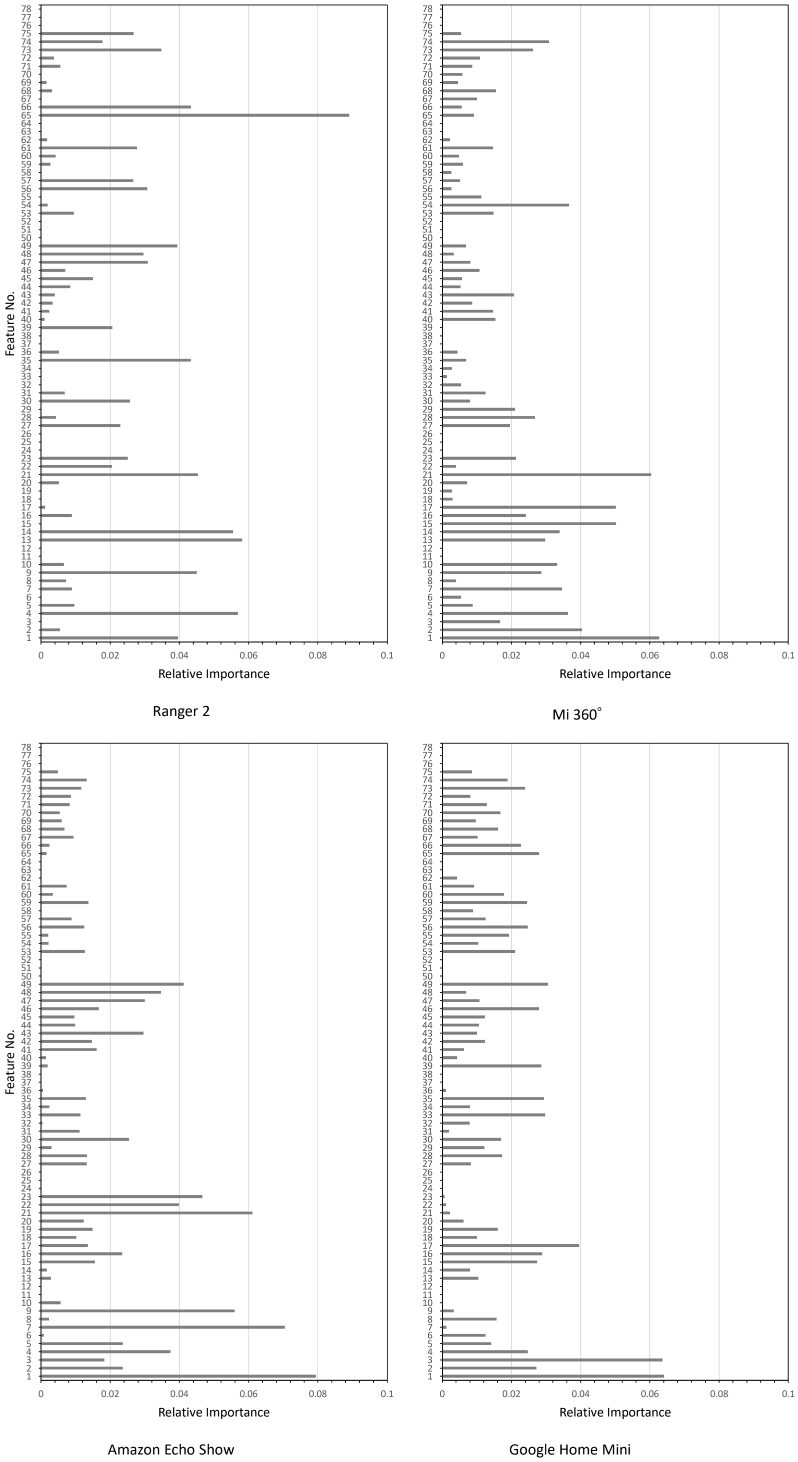
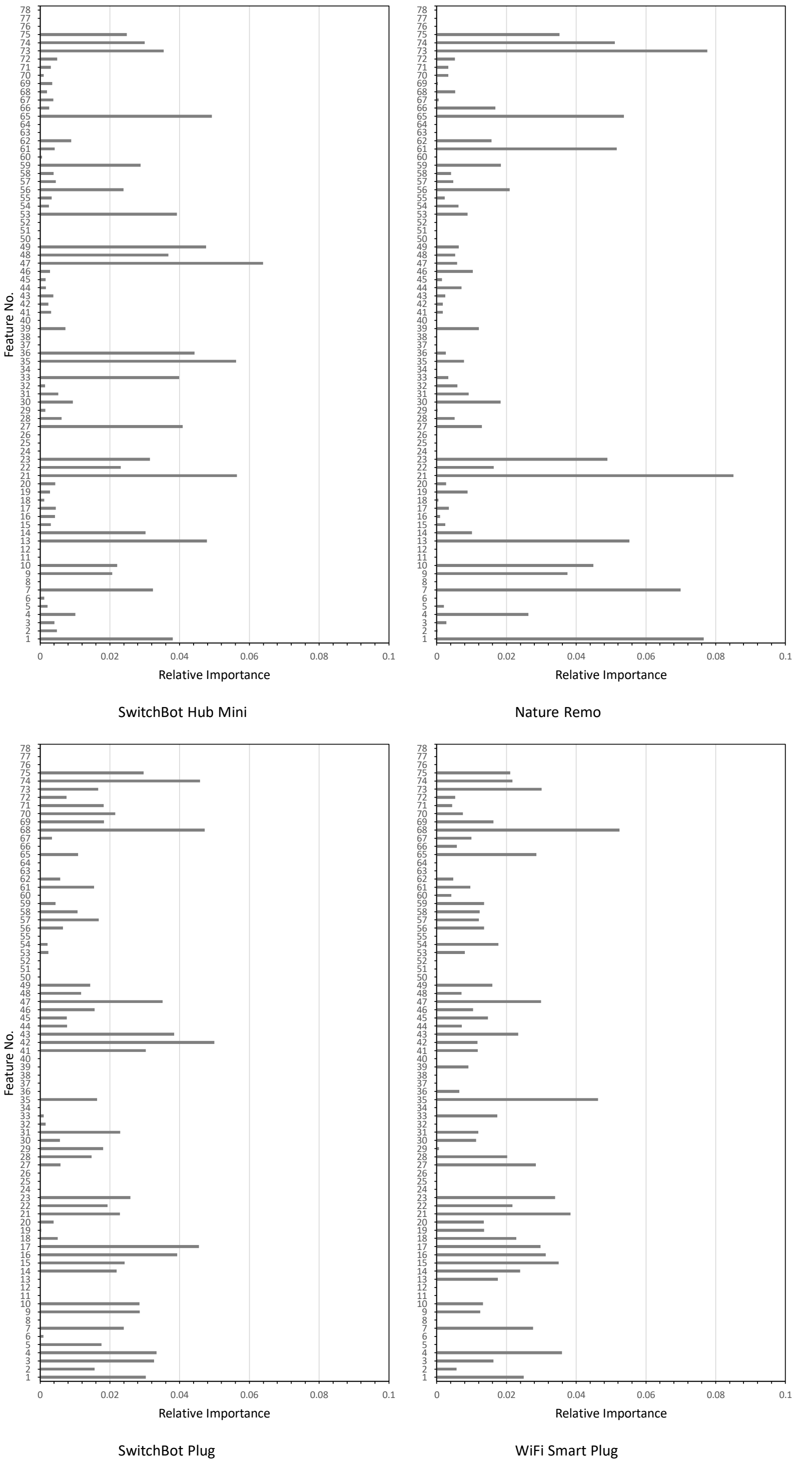


FIGURE 2: The importance of the features for each model(Smart cameras and smart speakers)



SwitchBot Hub Mini

Nature Remo

SwitchBot Plug

WiFi Smart Plug

FIGURE 3: The importance of the features for each model(Smart remote controllers and Smart plugs)

Bibliography

[1] Apthorpe, N., Reisman, D., Feamster, N.: A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. arXiv preprint arXiv:1705.06805 (2017). URL https://arxiv.org/abs/1705.06805

[2] Bendiab, G., Shiaeles, S., Alruban, A., Kolokotronis, N.: Iot malware network traffic classification using visual representation and deep learning. In: 2020 6th IEEE Conference on Network Softwarization (NetSoft), pp. 444–449. Ghent, Belgium (2020). DOI 10.1109/NetSoft48620.2020.9165381

[3] Dong, S., Li, Z., Tang, D., Chen, J., Sun, M., Zhang, K.: Your smart home can't keep a secret: Towards automated fingerprinting of iot traffic. In: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, ASIA CCS '20, p. 47–59. Association for Computing Machinery, New York, NY, USA (2020). DOI 10.1145/3320269.3384732. URL https://doi.org/10.1145/3320269.3384732

[4] Google: Change app permissions on your android phone - android help. https://support.google.com/android/answer/9431959 (2022)

[5] Hattori, Y., Arakawa, Y., Koike, D., Ishida, S., Inoue, S.: Function-level access control system for home iot devices. In: Sensors and Materials, Volume 34, Number 6(2), pp. 2125–2139. MYU K.K. Sensors and Materials, Tokyo, Japan (2022). URL https://doi.org/10.18494/SAM3901

[6] Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J.D., Ochoa, M., Tippenhauer, N.O., Elovici, Y.: Profiliot: a machine learning approach for iot device identification based on network traffic analysis. Proceedings of the symposium on applied computing pp. 506–509 (2017). URL https://dl.acm.org/doi/10.1145/3019612.3019878

[7] MIC: Data collection-information and communications in japan. https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2022/data_chapter3.pdf (2023)

[8] Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A.R., Tarkoma, S.: Iot sentinel: Automated device-type identification for security enforcement in iot. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), pp. 2177–2184. IEEE, Atlanta, GA, USA (2017)

[9] NICT: Nicter report 2022. https://csl.nict.go.jp/en/nicter-report.htmlnicter-report2022 (2023)

[10] NICT: Nicterweb - dark net observation — national institute of information and communications technology cybersecurity laboratory. https://www.nicter.jp/en (2023)

[11] Nobakht, M., Javidan, R., Pourebrahimi, A.: Demd-iot: a deep ensemble model for iot malware detection using cnns and network traffic. Evolving Systems **14**, 1–17 (2022). DOI 10.1007/s12530-022-09471-z

[12] Sivanathan, A., Gharakheili, H.H., Sivaraman, V.: Inferring iot device types from network behavior using unsupervised clustering. In: 2019 IEEE 44th Conference on Local Computer Networks (LCN), pp. 230–233. IEEE, Osnabrueck, Germany (2019)

[13] Sivanathan, A., Gharakheili, H.H., Sivaraman, V.: Detecting behavioral change of iot devices using clustering-based network traffic modeling. IEEE Internet of Things Journal **7**(8), 7295–7309 (2020)

[14] Sivanathan, A., Sherratt, D., Gharakheili, H.H., Radford, A., Wijenayake, C., Vishwanath, A., Sivaraman, V.: Characterizing and classifying iot traffic in smart cities and campuses. 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) pp. 559–564 (2017). URL `https://ieeexplore.ieee.org/abstract/document/8116438`

[15] XDA: Tp-link deco x68 review: A good mesh router ruined by bizarre software. https://www.xda-developers.com/tp-link-deco-x68-review (2022)

[16] Yahoo: Zoom admits some calls were routed through china by mistake (2020). Https://techcrunch.com/2020/04/03/zoom-calls-routed-china/

[17] Yuichi Hattori Yutaka Arakawa, S.I.: Function estimation of multiple iot devices by communication traffic analysis. In: The 4th International Conference on Activity and Behavior Computing (ABC2022). London, UK (2022)

[18] Zeng, E., Mare, S., Roesner, F.: End user security and privacy concerns with smart homes. Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017) pp. 65–80 (2017). URL `https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng`