1

Function Estimation of Multiple IoT Devices by Communication Traffic Analysis

Yuichi HATTORI* [1], Yutaka ARAKAWA [2], Sozo INOUE [3]
[1 3]Kyushu Institute of Technology,[2]Kyushu University

Abstract

In recent years, IoT devices have become widespread in households, and IoT devices with various functions such as remote control, lighting, door locks, and power outlets are sold and used in various situations. The activity of IoT devices can be likened to a black box, often operating independently of the user's intentions regarding what data the device is sending and where. 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. In order to achieve the IoT activity tracker, in this paper, we collected communication traffic of 16 combinations of device model and executed function from 8 IoT devices with 2 functions each. And we used 28 features derived from the volume of communication that do not contain information that can identify individuals or specific manufacturers to perform 2 types of classification using a random forest algorithm and evaluated their accuracy. As a result, we confirmed that the function could be estimated with an accuracy of 91% when classified into 16 combinations of device model and executed function. When classified by 8 combinations of only executed functions, we confirmed that the function could be estimated with an accuracy of 73%.

[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 such as remote control, lighting, door locks, and power outlets 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 2017 was about 27 billion and predicted to increase to 40 billion by 2020.[12] 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.

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, a vulnerability has been discovered in a camera installed in a smart vacuum cleaner that can be used to listen in on a home, and customer information has been stolen from a casino via a smart thermometer installed in an aquarium.[4] In addition, there are websites that allow users to view and browse a list of video images of network cameras that have problems with the initial setup and configuration, meaning that they can be easily accessed from outside once the IP address is known. There has been a recent increase in attacks targeting IoT devices. For example, Zhang et al., Chakraborty et al., and Mao et al. used sounds that are inaudible to humans to access and remotely control IoT devices.[19, 2, 9] While the proliferation of IoT devices makes our lives more convenient, it is important to consider the security of their use.

Various precautions need to be taken when using IoT devices. In particular, the following three points need to be taken into account.

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 can be likened to 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.[17] 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.[7] 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. Conventional studies have only evaluated the same type of IoT devices.[8] Therefore, it is necessary to verify and improve the features on many types of IoT devices. In this paper, we collected communication traffic of 16 combinations of device model and executed function from 8 IoT devices with 2 functions each. These devices are distributed in Japan, including smart speakers, smart cameras, smart remote controls, and smart plugs. Then we used machine learning to classify the devices and the functions performed by the devices using features extracted from the communication traffic without personally identifiable information to evaluate their accuracy. Additionally, feature selection was performed and an attempt was made to improve accuracy. As a result, we confirmed that the function could be estimated with an accuracy of 91% when classified into 16 combinations of device model and executed function. When classified by 8

combinations of only executed functions, we confirmed that the function could be estimated with an accuracy of 73%.

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 function estimation method of IoT devices by communication traffic analysis, and its evaluation is presented in Section 5. In Section 6, we discuss the our proposal. Finally, we conclude our paper in Section 7.

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.

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.

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.[10] 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.[15] 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.[13] 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.[14]

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.[11] 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.[5] 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[16] In other words, it is necessary to control the resources used in the smart home, just as we do with smartphones today.

3 Function Estimation Method of IoT Devices by Communication Traffic Analysis

In this section, we describe our proposed IoT activity tracker 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 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

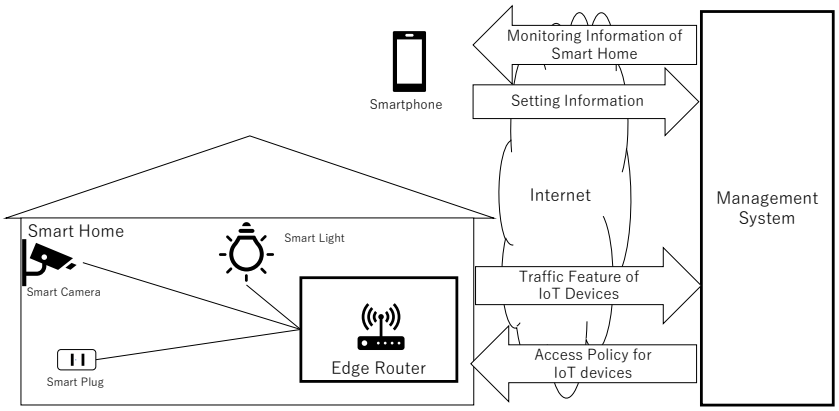

FIGURE 1: Outline of IoT activity tracker

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 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 tracker described in Section 3.1. The proposed method estimates the functions of IoT devices by learning their communication traffic patterns through machine learning. To construct an estimation model for use in an IoT activity tracker, we collected communication traffic of 16 combinations of device model and executed function from 8 IoT devices with 2 functions each. These devices distributed in Japan, including smart speakers, smart cameras, smart remote controls, smart plugs. Then we used machine learning to classify the devices and the functions using features extracted from the communication traffic without personally identifiable information to evaluate their accuracy. From communication traffic, features can be calculated from volume of communication, such as packet size and number of destination IPs, or from information related to the content of communication, such as country of destination IP and management information of destination IP. In this paper, we used features derived from the volume of communication that do not contain information that can identify individuals or specific manufacturers. 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 fo-

TABLE 1: List of feature values

	Feature Value
1	Maximum packet size sent in 1.5 sec
2	Maximum packet size received in 1.5 sec
3	Mean of TCP packet size of in 1.5 sec
4	Mean of packet size sent in 1.5 sec
5	Mean of packet size received in 1 sec
6	Maximum packet size received in 1 sec
7	Maximum packet size sent in 0.5 sec
8	Maximum TCP packet size of in 1.5 sec
9	Mean of number of TCP packets in 1 sec
10	Maximum TCP packet size in 1 sec
11	Mean of packet size sent in 1 sec
12	Max of number of packet received in 1.5 sec
13	Mean of UDP packet size of in 1 sec
14	Mean of TCP packet size of in 1 sec
15	Mean of UDP packet size of in 0.5 sec
16	Mean of packet size received in 1.5 sec
17	Maximum packet size sent in 1 sec
18	Max of number of UDP packets in 1 sec
19	Maximum UDP packet size in 1 sec
20	Max of number of packet received in 1 sec
21	Maximum TCP packet size in 0.5 sec
22	Variance of packet size sent in 0.5 sec
23	Max of number of TCP packets in 1.5 sec
24	Variance of packet size sent in 1 sec
25	Max of number of TCP packets in 1 sec
26	Mean of number of UDP packets in 1 sec
27	SD of packet size sent in 0.5 sec
28	Maximum UDP packet size in 1.5 sec

cused on features derived from the volume of communication. Calculated the mean, maximum, variance and standard deviation of the number of packets sent, the size of the packets sent, the number of packets received, the size of the packets received, the number of TCP packets, the size of TCP packets, the number of UDP packets, the size of UDP packets, the number of source IPs and the number of destination IPs in time windows of 0.5, 1, and 1.5 seconds; and a total of 120 features were extracted. From them, a random forest algorithm was used to calculate the importance of the features, and features of low importance were excluded. As a result, the features used are shown in Table 1. The machine learning algorithm used was random forest algorithm, which is supervised machine learning, and was evaluated by 10-fold cross-validation.

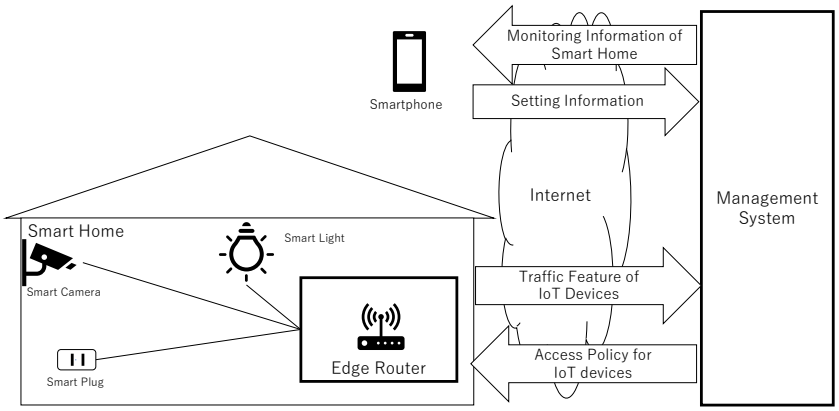

FIGURE 2: Diagram of data collection environment

4 Data Collection

In this section, we describe data collection environment and data collection method.

4.1 Data collection environment

Figure 2 shows the diagram of data collection environment. This means that all IoT device communications will go through the edge router. The data collection environment was built on a virtual machine with an edge router, which is part of the IoT activity tracker described in Section 3.1. Eight IoT devices were connected to the edge router through access points. The list of IoT devices used for data collection is shown in Table 2.

4.2 Data collection method

Using the collection environment described in Section 4.1, we collected communication traffic of 16 combinations of device model and function executed from 8 IoT devices with two functions each. In addition, each of the 16 patterns collected was collected 10 times. The list of functions of IoT devices for collected data is shown in Table 3. For functions that require time to complete, such as "Play music" the number of seconds was limited by stopping playback in the middle of the function. In selecting the functions to be collected this time, we focused on those with similar behavior for the same device type. For

TABLE 2: List of IoT devices used for data collection

	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

TABLE 3: List of functions of IoT devices for collected data

	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

example, the "Ask for today's news" function of the smart speakers Google Home Mini and Amazon Echo Show was excluded from the selection because the Amazon Echo Show plays today's news from the beginning every time, whereas the Google Home Mini plays the today's news from the middle of the news when it is played for the second time, which is a different behavior.

For data collection, communication packets were collected by using the tcpdump[6] command for the network interface on the side to which the IoT device was connected to the edge router. The data collection procedure is as follows:

1. Starts collecting communication packets.
2. Wait about 10 seconds.
3. Execute the target function.
4. Confirm the execution of the target function.
5. Wait about 10 seconds.
6. Ends collecting communication packets.

4.3 Data processing method

In the data collection environment used, all IoT devices are connected to the same network environment, so the communication of other IoT devices is also mixed when collecting packets. It is necessary to extract only the packets of the target IoT devices for use in this evaluation. Therefore, only packets from IoT devices for which the destination and source IPs are the target IPs were extracted and used for evaluation.

5 Evaluation

To test the validity of the functional estimation method, a random forest algorithm was used and evaluated by cross-validation of 10 segments. 2 types of evaluations were conducted: 16 combinations of IoT device models and executed functions, and 8 combinations of functions only. As a result, we confirmed that the function could be estimated with an accuracy of 91% when classified into 16 combinations of device model and executed function. Its confusion matrix is shown in Table 4 and a list of its class labels is shown in Table 5. Both IoT devices were able to classify "play music (10 sec)" and "Ask for today's weather" which involve a lot of communication. Less communicative functions, such as SwitchBot Plug's "turn on power" and Nature Remo's "turn off the TV," are misclassified as similar functions with less accuracy than other functions. Since only a few communications to execute the function occurred in the first place, the accuracy is expected to drop further when IoT devices and functions are added and evaluated in the future. When classified by 8 combinations of only executed functions, we confirmed that the function could be estimated with an accuracy of 73%. Its confusion matrix is shown in Table 6 and a list of its class labels is shown in Table 7. In this case, too, "Play music(10 sec)" and "Ask for today's weather", which generate a lot of communication, are correctly classified. The accuracy of "mute the TV" and "turn on the TV", which do not generate much communication, is low. In particular, "mute the TV" and "turn on the TV" are performed using a smart remote control, and the smart remote control that receives the instructions sends an infrared signal for the function in question. Therefore, it is considered difficult to classify only by the information of the communication traffic because the actual communication is almost the same and the communication occurs only a few times.

TABLE 4: Confusion matrix of function estimation results(Combination of IoT device models and functions)

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	9	0	0	0	0	1	0	0	0	0	0
6	0	0	0	0	0	1	8	1	0	0	0	1	0	0	0	0
7	0	0	0	0	0	1	0	9	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	7	3	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	2	8	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	9	0	1	0	0	0
11	0	0	0	0	0	0	0	0	0	0	2	8	0	0	0	0
12	0	0	0	0	0	0	1	0	0	0	0	0	9	0	0	0
13	0	0	0	0	0	0	0	1	0	0	0	0	1	8	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10

TABLE 5: Class labels of Table 4

Class Label	**Detail**
0	Play music(10sec)(Amazon Echo Show)
1	Ask for today's weather(Amazon Echo Show)
2	Play music(10sec)(Google Home Mini)
3	Ask for today's weather(Google Home Mini)
4	Change camera direction(Rotate left, 3sec)(Ranger 2)
5	Talk to smart camera(Ranger 2)
6	Change camera direction(Rotate left, 3sec)(Mi 360°)
7	Talk to smart camera(Mi 360°)
8	Mute the TV(Nature Remo)
9	Turn on the TV(Nature Remo)
10	Turn off power(SwitchBot Plug)
11	Turn on power(SwitchBot Plug)
12	Mute the TV(SwitchBot Hub Mini)
13	Turn on the TV(SwitchBot Hub Mini)
14	Turn off power(WiFi Smart Plug)
15	Turn on power(WiFi Smart Plug)

TABLE 6: Confusion matrix of function estimation results(Only functions)

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	15	3	1	0	0	1	0	0
1	5	15	0	0	0	0	0	0
2	0	0	15	0	4	1	0	0
3	0	0	0	20	0	0	0	0
4	0	0	2	0	18	0	0	0
5	0	0	1	0	0	7	12	0
6	0	0	1	0	0	13	6	0
7	0	0	0	0	0	0	0	20

TABLE 7: Class labels of Table 6

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

6 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.

6.1 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.

6.2 Impact of IoT device updates

IoT devices undergo periodic software updates. This may cause changes in communication destinations, communication volume, and so on. Furthermore, for IoT devices that allow additional third-party applications to be installed, such as smart speakers, it is necessary to consider not only firmware updates but also application updates.

6.3 Similarity of communication traffic for different device models with the same functionality

Even with the same functionality, different device models may have different communication traffic features. For example, different manufacturers of IoT devices have different connection points and implementation methods, resulting in different communication traffic features. Therefore, in order to classify them, it is considered effective to classify devices first and then functions. However, "play music" on a smart speaker, for example, would have similar communication traffic features if the application running on the IoT device has the same connection destination, even if the device model is different.

6.4 Different function but similar communication traffic

Many IoT devices communicate using HTTPS to receive and send data in formats such as JSON. For example, in the case of a smart remote control, even if commands are sent in JSON, they are communicated only a few times, and the contents are not very different. Therefore, it would be difficult to classify them based solely on the communication traffic. Therefore, in order to detect these functions, it is necessary to link them with existing behavior

recognition technique and to detect them in conjunction with room occupancy status and other factors.

6.5 Impact of an increase in the number of devices or functions

In this study, we validated 16 device and function combinations. We will continue to add more combinations for further validation. Based on the results of this verification, identification is good except for the IoT device functions mentioned in Section 6.4. Therefore, if a smart remote control or other device with similar communication for each function is added, the accuracy is expected to be reduced. Smart speakers and other devices with different communication for each function are expected to be well identified even if the number of functions or devices increases.

7 Conclusion

In this paper, we presented a function estimation method in IoT devices 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. We collected communication traffic of 16 combinations of the device model and the executed function from 8 IoT devices with 2 functions each. These devices are distributed in Japan, including smart speakers, smart cameras, smart remote controls, and smart plugs. Then we used machine learning to classify devices and functions using features extracted from communication traffic without personally identifiable information to evaluate their accuracy. As a result, we confirmed that the function could be estimated with an accuracy of 91% when classified into 16 combinations of device model and executed function. When classified by 8 combinations of only executed functions, we confirmed that the function could be estimated with an accuracy of 73%. 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. 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).

Bibliography

[1] Noah Apthorpe, Dillon Reisman, and Nick Feamster. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805*, 2017.

[2] Anirban Chakraborty, Manaar Alam, Vishal Dey, Anupam Chattopadhyay, and Debdeep Mukhopadhyay. Adversarial attacks and defences: A survey. *arXiv preprint arXiv:1810.00069*, 2018.

[3] Shuaike Dong, Zhou Li, Di Tang, Jiongyi Chen, Menghan Sun, and Kehuan Zhang. 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, page 47–59, New York, NY, USA, 2020. Association for Computing Machinery.

[4] Forbes. Time to update your vacuum cleaner – hack turns lg robot hoover into a spy, 2017. https://www.forbes.com/sites/thomasbrewster/2017/10/26/lg-hombot-robot-hoover-hacked-into-surveillance-device/.

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

[6] The Tcpdump Group. the-tcpdump-group/tcpdump: the tcpdump network dissector, 2022. https://github.com/the-tcpdump-group/tcpdump.

[7] Yuichi Hattori, Yutaka Arakawa, Daichi Koike, Shigemi Ishida, and Sozo Inoue. Function-level access control system for home iot devices. In *Sensors and Materials, Volume 34, Number 6(2)*, pages 2125–2139. Sensors and Materials, 2022.

[8] Daichi Koike, Shigemi Ishida, and Yutaka Arakawa. Called function identification of iot devices by network traffic analysis. In *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, SAC '21, page 737–743, New York, NY, USA, 2021. Association for Computing Machinery.

[9] Jian Mao, Shishi Zhu, Dai Xuan, Qixiao Lin, and Jianwei Liu. Watchdog: Detecting ultrasonic-based inaudible voice attacks to smart home systems. *IEEE Internet of Things Journal*, 2020.

[10] Yair Meidan, Michael Bohadana, Asaf Shabtai, Juan David Guarnizo, Martín Ochoa, Nils Ole Tippenhauer, and Yuval Elovici. Profiliot: a machine learning approach for iot device identification based on network traffic analysis. *Proceedings of the symposium on applied computing*, pages 506–509, 2017.

[11] Markus Miettinen, Samuel Marchal, Ibbad Hafeez, N Asokan, Ahmad-Reza Sadeghi, and Sasu Tarkoma. Iot sentinel: Automated device-type identification for security enforcement in iot. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 2177–2184. IEEE, 2017.

[12] MinistryofInternalAffairsandCommunications. Ict in japan and the world, 2018. https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2018/chapter-1.pdf.

[13] Arunan Sivanathan, Hassan Habibi Gharakheili, and Vijay Sivaraman. Inferring iot device types from network behavior using unsupervised clustering. In *2019 IEEE 44th Conference on Local Computer Networks (LCN)*, pages 230–233. IEEE, 2019.

[14] Arunan Sivanathan, Hassan Habibi Gharakheili, and Vijay Sivaraman. Detecting behavioral change of iot devices using clustering-based network traffic modeling. *IEEE Internet of Things Journal*, 7(8):7295–7309, 2020.

[15] Arunan Sivanathan, Daniel Sherratt, Hassan Habibi Gharakheili, Adam Radford, Chamith Wijenayake, Arun Vishwanath, and Vijay Sivaraman. Characterizing and classifying iot traffic in smart cities and campuses. *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 559–564, 2017.

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

[17] Yahoo. Zoom admits some calls were routed through china by mistake, 2020. https://techcrunch.com/2020/04/03/zoom-calls-routed-china/.

[18] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 65–80, 2017.

[19] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. Dolphinattack: Inaudible voice commands. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017.