Platform Utilizing Others' Behavior Data to Detect Anomalous Operation Hiding Private Information

Masaaki YAMAUCHI, *Graduate Student Member, IEEE,* Yuichi OHSITA, *Member, IEEE,*
Masayuki MURATA, *Member, IEEE,*
Graduate School of Information Science and Technology, Osaka University, Suita, Osaka, Japan
{m-yamauchi, y-ohsita, murata}@ist.osaka-u.ac.jp

***Abstract*—As the number of IoT consumer electronics is increasing, cyberattacks to IoT devices are increasing. In particular, operating IoT devices by attackers make users feeling unsafe and may harm users physically. Therefore, we have proposed a method to detect anomalous operations by learning users' behavior. However, this method misdetects many legitimate operations if a sufficient amount of data on the users' behavior. One approach to avoid misdetections even if a sufficient amount of data cannot be obtained from each user is to use the data collected from the others. But users do not want to share their private information with others. In this paper, we proposed an anomaly detection platform that utilizes the dataset of similar users without sharing their private information.**

I. Introduction

Recently, consumer electronics such as refrigerators and electric fans have been connecting to the Internet and called as IoT (Internet of Things) devices. Users can operate these IoT devices by using smartphones and AI speakers via the Internet. As a number of the connected IoT devices increases, a number of cyberattacks targeting them increases. Attacking IoT devices has a risk to affect the real-life of users. In particular, operating IoT devices by attackers make users feeling unsafe and may harm users physically, through actions such as changing the temperature of an air conditioner or the settings of a refrigerator. In addition, simultaneous attacks on high-power IoT devices can suddenly increase energy demands and lead to major power outages [1].

We have proposed a method to detect anomalous operations on IoT devices [2]. This method models users' behaviors as sequences of events which includes operations of IoT devices and other behavior monitored in the home environment. This method learns sequences of events for each condition. Then, it detects anomalous operations by comparing the current sequences with the sequences learned for a similar condition.

This method requires a sufficient amount of data on legitimate users' behavior to avoid misdetection; it misdetects users' legitimate operations if similar behavior is not monitored before. But only a limited amount of data can be obtained at each home. One approach to avoiding misdetections even if a sufficient amount of data cannot be obtained from each user is to use the data collected from the others. If the current behavior matches the behavior of similar users, the behavior can be regarded as legitimate. But users do not want to share their private information such as their behaviors with others.

In this paper, we proposed an anomaly detection platform utilizing similar users' data without sharing their private information. In this platform, an agent is deployed for each home to learn and detect anomalous operations in the home. The agent avoids a lack of data on legitimate operations by cooperating with other agents storing similar behavior.

II. Anomaly Detection Utilizing Others' Behavior Data Hiding Private Information

A. Overview

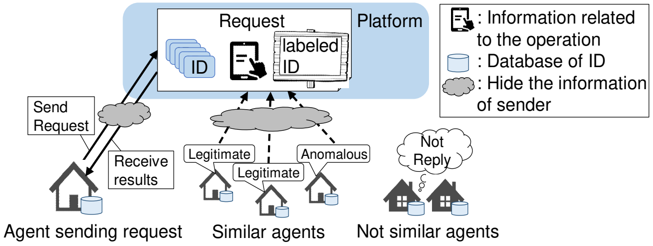

Fig. 1: Overview of our platform

Fig. 1 shows an overview of our platform. In our platform, an agent is deployed for users in a home to learn the users' behaviors and detect anomalous operations. When an agent cannot decide whether current operations are legitimate or anomalous, it sends requests to the other agents via the platform to cooperate with other agents for deciding the operations are legitimate or anomalous. Each agent first checks whether the sender of the request has learned similar users' behaviors to the agent. If the sender has learned similar behavior, the agent checks whether the behavior included in the request is legitimate or not based on its learned behavior. Then, the agent votes based on its decision. By these steps, the platform collects the votes from similar agents. As a result, the agent that sent the request decides whether the current operation is legitimate or not by checking the results of the votes.

Our platform performs the above steps without identifying any agents. In our platform, the identifiers are set only to the requests. Thus, the other agents cannot identify who sends the request. The similarities between agents are calculated based on the IDs of the requests; The IDs of the past requests that are regarded as legitimate by the sender are attached to the request and are used by the other agents to identify if the sender of the request learned similar behaviors.

B. Procedure of an agent sending a request

Each time an agent detects an operation of devices, the agent checks whether the operation is legitimate or not. If the agent cannot determine whether the operation is legitimate or not due to a lack of data learned by the agent, it sends a request to the platform. The request includes the information on the current operation that is used to identify the operation is legitimate or not. The request also includes the IDs of the past requests that were identified as legitimate by the agent. This information is used to check whether the sender learned similar behavior to agents receiving the request. When sending the request to the platform, the sender can also hide who sent the request even to the platform by using tools such as Tor [3].

After other agents vote, the agent receives the result of votes from the platform. If the number of votes to "Legitimate" is larger than a predefined threshold T, the agent regards the current operation as legitimate.

C. Procedure of agents receiving a request

When an agent receives a request, the agent first checks past requests' IDs identified as legitimate by the sender. The agent compares the IDs with past requests' IDs identified as legitimate by the agent and stored. If a number of matched IDs is smaller than a threshold N, the agent does not vote, because the home of the sender has different behavior. By doing so, we avoid the degradation of anomaly detection by using the information of users whose behaviors are different.

If the number of matched IDs is larger than the threshold N, the agent checks the behavior included in the request is legitimate or not by using its learned model. Then, it votes by returning its decision to the platform. The decision is "Legitimate", "Anomalous", or "Unknown", where "Unknown" is a case that an agent does not have a sufficient amount of data to determine whether the behavior included in the request is legitimate or not.

If the agent identified the behavior of the request as legitimate, the agent stores its ID. The stored ID is used to identify the senders of future requests have similar behaviors or not.

III. Evaluation

We implemented and evaluated our platform by simulation.

A. Evaluation environment

In this evaluation, each agent uses the anomaly detection method we have proposed in our previous work [2].

We used the dataset collected in our previous work [2], collected in our laboratory where several home IoT devices were deployed. We selected four students as subjects in each month and let them use the devices as they like. In this evaluation, we divided the collected data set into 28 datasets so that each divided dataset includes the operations by one user at a month.

Moreover, to evaluate our platform by the cross-validation method, we divided each data set into two parts. Firstly, one of the parts is used to train the behaviors, and the other part is used for a test. Then, we changed the role of the two parts and evaluate our platform. Finally, we added up the two results as one result. In our evaluation, we regard the operations by the users in the dataset is regarded as a legitimate. We also inserted 100 anomalous operations per day into the test dataset at the randomly selected time.

B. Result

TABLE I: Detection results on electric fans

	Misdetect	Misdetected	False negative	False negative
	ratio	/Total	ratio	/Total
Single	0.236	30/127	0.00493	224/45176
Similar	0.197	25/127	0.00645	293/45176
All	0.165	21/127	0.00819	372/45176

Table I shows the results for three cases. The "Single" is a case that each agent detected anomalous operations without cooperating with other agents. The "Similar" is a case that used our platform with $(T, N) = (1, 1)$, i.e., detection by cooperating with only similar agents. The "All" is a case that used our platform with $(T, N) = (1, 0)$, i.e., detection by cooperating with all agents. The results are the sum of the results for 16 users.

The results indicate that our platform reduced the number of misdetections because methods using our platform could efficiently use information from other agents. The results also indicate that cooperating with all agents caused false negatives while it reduced misdetections. On the other hand, cooperating with only similar agents reduced the number of misdetections compared with the detection by a single agent, while it avoided the increase of the number of false negatives compared with the case of cooperating with all agents.

IV. Conclusion and Future Work

We proposed an anomaly detection platform that utilizes the dataset of similar users without sharing their private information. We implemented our platform and evaluated it through simulation. The result demonstrates that our platform is useful to reduce the misdetection of legitimate operations. In this paper, we evaluated our method using a small amount of dataset. But the advantages of our platform becomes large as the number of homes using our platform increases. Considering such a point, we will evaluate our method in the case that more homes use our platform. Also, we will investigate how to set the parameter T and N. Moreover, though this paper assumes that all agents perform correct operations, the attacks targeting our platform may also be an important problem, which is also one of our future research topics.

References

[1] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. of 27th USENIX Secur. Symp.* Baltimore, MD: USENIX Assoc., Aug. 2018, pp. 15–32.

[2] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, "Anomaly detection in smart home operation from user behaviors and home conditions," *IEEE Trans. on Consum. Electronics*, vol. 66, no. 2, pp. 183–192, May 2020.

[3] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proc. of 13th USENIX Secur. Symp.* San Diego, CA: USENIX Assoc., Aug. 2004, pp. 303–320.