2021 7th International Conference on Big Data Computing and Communications (BigCom) | 978-1-6654-4252-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/BigCom53800.2021.00033

The Truman Show: Attack On The Privacy Of Smart Homes Through Traffic Analysis*

Xiaomeng Yu[1], Yanyong Zhang[1], Xiang-Yang Li[1], and Xing Guo[1]

[1]School of Computer Science and Technology, University of Science and Technology of China
Hefei, China
{*yuxm*}@*mail.ustc.edu.cn*, {yanyongz,xiangyangli,guoxustc}@ustc.edu.cn

***Abstract*—The sensor network is widely used in the Internet of Things environment to create a more intelligent and convenient life, sensors closely monitor and get information from the living environment, smart home devices respond to user instructions to provide services. The constant interaction data with the cloud server, however, is unwittingly exposing user privacy to danger. This paper attacks a variety of smart home devices and sensors through traffic analysis, proving that encrypted data has the risk of revealing user privacy in the wireless environment, even if the packet content is not obtained, the state of a single IoT device can be analyzed through the number and shape of packets. Also, considering the user behavior may lead to responses from multiple devices in the environment, so that more elaborate information can be further deduced through the analysis of the combination of multiple equipment states. Based on the attack on single devices, we carried out a joint attack on multiple devices using state sequence diagrams of all devices in the smart home. The experiments prove that the traffic patterns of IoT devices do leak private information of users, we provide the corresponding solution of traffic shaping to defend against such attack.**

***Index Terms*—Internet of Things, sensor network, traffic analysis, traffic shaping**

I. Introduction

In a smart home, users use a variety of feature-rich smart devices and simple sensors to construct a network to provide convenience and safety for daily life, cameras monitor the situation in the house at all times, smart lights guide family members at night, intelligent speakers response to user needs in the first time.

The prerequisite for these devices to complete their functions is that they continuously exchange data to communicate with the outside world. For communication security and privacy, various lightweight encryption algorithms are used to protect data privacy from being leaked. The encrypted data packets are propagated in the network, and the payload in the data packets is hidden. The difficulty for attackers to decipher the content of the data keeps increasing. But even so, the unencrypted meta-information such as the length, direction, and type of the data inevitably reveals the communication information and status information of the device.

Some previous work adopted a similar idea to website fingerprint attacks [2], obtaining upper-layer packets of the device, such as TCP/IP, and analyzing the payload length of TCP and DNS query information. To a certain extent, it is assumed that the device itself is malicious, and information that can be used for attack is obtained inside the device. This assumption does not have practical application value for the widely deployed Smart Internet of Things.

IoT devices are rich in types and simple in status, and they often use wireless networks that do not require cables, are simple to install, and easy to move. Wi-Fi and ZigBee are the most commonly used communication protocols in smart homes. There are identifiers in their data packet headers that can uniquely distinguish devices, such as MAC addresses and ZigBeeIEEE addresses. Therefore, it is not difficult to capture packets in the air and calculate the traffic distribution of a certain device based on this. Also, they often only interact with the server corresponding to the manufacturer, the communication objects and modes are relatively simple, and the equipment itself has limited functions. Therefore, as long as the state division is reasonable, it is completely feasible to select the appropriate feature value to classify the device behavior, even if the data packets are encrypted.

Considering that different devices may produce simultaneous perception and response to the same user activity or environmental changes. For example, the event of a person going out will cause the door and window sensors to react, and his actions will also be captured by the surveillance camera arranged in the room. Therefore, by combining the state information of multiple devices in the environment, we can directly link the state of the device to the user's behavior, and based on this, we can infer the more refined privacy behavior of the user.

In this work, we mainly made the following contributions:

a) traffic analysis attacks on multiple independent devices across protocols and types: We tested 9 different commonly used IoT devices based on Wi-Fi or ZigBee protocols, according to the functional specification, we divided and classified the state of the device. On this basis, the device communication data in the wireless environment is captured and processed, and then the simplest SVM classification model is used to classify and attack the corresponding state.

b) combination attacks on multiple independent devices: Based on the results of a single device attack, we can get the state matrix of all devices in the environment over some time, and combine all the information of these devices to do further attacks. We propose a new joint attack method against multiple devices, which makes it possible to use the state

978-1-6654-4252-7/21/$31.00 ©2021 IEEE
DOI 10.1109/BigCom53800.2021.00033

matrix of all devices in the family to infer family events and their occurrence time.

c) traffic shaping defense for a single device and multiple devices: After the previous attack work, we discussed some traffic shaping strategies that can resist traffic analysis, and proposed different variants in a single device and multiple device scenarios, to protect the security and privacy of smart homes.

The rest of this paper is organized as follows: Section II introduces the attack model and test equipment; Section III provided the attack method and process of independent equipment. The possibility of combined attacks on multiple devices and launches related experiments will be presented in Section IV. Section V briefly discusses our recommendations for defending against traffic analysis attacks.

II. Attack Model

In a wireless network environment, all communication content is transmitted through an open wireless channel, which means that all wireless devices can also obtain information sent by other devices through this open channel, without joining the network itself. These data have been encrypted, we cannot get the specific data content of the transmission, but only through the header information disclosed by these data packets, a lot of device privacy can be obtained.

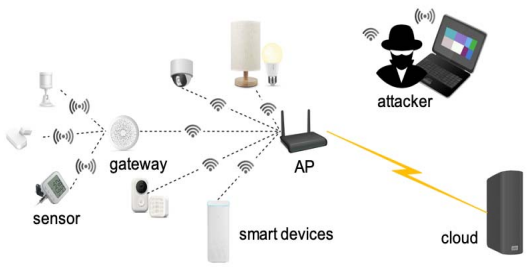


Fig. 1: Network Organization and Attack Model

As shown in Fig. 1, in a smart home scenario, multiple devices using different protocols form a network in this organizational structure, and attackers can obtain message information in the network without being discovered.

To make the attack scenario more realistic and universal, based on the above-mentioned IoT organizational structure, we pretend to be an external attacker who is completely unknown to all kinds of information in the wireless network environment and places the equipment used for sniffing outside the physical boundary of the house to attack each device in the network without prior knowledge.

Besides, for the selection of specific experimental equipment, we also consider three dimensions.

a) communication protocol: In small smart homes, most commercial devices use Wi-Fi, ZigBee, and BLE to communicate, so we try to select devices that can maximize coverage of these common protocols.

b) communication type: Different devices play different communication roles because they are in different positions in the network. The network structure in Figure 1 is the most common smart home networking mode. Since smart home equipment providers often require communication between the device and the cloud to provide complete services, we have classified the devices according to the way they communicate with the cloud: 1) Direct communication, devices work on TCP/IP that directly transmits data to the cloud; 2) Indirect communication, small sensor devices that cannot communicate directly with the cloud, they must access the corresponding gateway to complete further processing and transmission of data; 3) Intermediate communication, gateway or hub-like central devices that connect indirect communication devices to the cloud.

c) status type: Based on the specific model and status distribution of device communication, we divide the device into (1) binary state devices, which only has two states: 0 (sleep) and 1 (active), mainly for monitoring equipment like door and window sensors; (2) uniform state devices, which often continuously send data periodically, and the communication mode is always kept in the same state, such as temperature and humidity sensors; (3) multi-state devices, devices with a variety of different communication state distributions, they have multiple non-dormant states with complex functions just like speakers and cameras.

Under these classification indicators, we selected a representative batch of equipment, which covers these categories to the greatest extent as shown in the table.

III. Traffic Analysis Attack On Single Device

In this section, we analyze the possibility of traffic analysis attacks on encrypted packets in an IoT scenario, and on this basis, we give a complete attack process and conduct experiments to simply and intuitively show the traffic analysis attack result of independent devices in a smart home.

A. Device Identification and Communication Characteristic

The data packets transmitted in the wireless channel may be encrypted one layer after another, but the unencrypted header information of the packet is necessary to be used to complete the basic communication. This easy-to-obtain header information already implicitly includes the device identification. Commonly used wireless communication protocols for IoT devices include Wi-Fi, ZigBee, and Bluetooth. Through the analysis of specific protocols, it can be seen that there is a possibility of acquiring communication characteristics in the corresponding communication process.

1) device identification based on communication address: In a complex network, there may be multiple devices communicating at the same time, and distinguishing the flows of different devices from the mixed communication traffic is the first step in a traffic analysis attack.

a) Wi-Fi based devices: WPA encryption can protect the specific content of Wi-Fi communication. It is difficult for an attacker who has not obtained the key to knowing the actual

TABLE I: Experiment Devices and Corresponding Classification

Devices	Protocol			StatusType			CommType		
	Wi-Fi	ZigBee	BLE	Uniform	Binary	Multi-Status	Direct	Indirect	Relay
DoorWin Sensor		*			*			*	
Movement Sensor		*			*			*	
Humidity Sensor			*	*			*		
HIKVISION Camera	*					*	*		
XIAOMI Camera	*					*	*		
DUER Speaker	*					*	*		
XIAOMI Speaker	*					*	*		
Smart Doorbell	*					*	*		
ZigBee Gateway	*	*			*				*

Since devices such as gateways use ZigBee/BLE to communicate with sensors and Wi-Fi to communicate with other network devices, we mark both protocols and treat them as cross-protocol devices.

data of the communication, but the unencrypted 802.11 frame header information contains four MAC addresses. The three addresses respectively represent the destination address, the source address, and the address of the wireless workstation for processing and forwarding, which can uniquely identify the communicating device and the communication direction.

b) ZigBee based devices: ZigBee network frames often contain two types of addresses. One is the ZigBee IEEE address that is solidified in the device by the manufacturer once the device is produced. Similar to the MAC address, it can uniquely identify any ZigBee device in the world. The other is the 16-bit network address assigned by the coordinator combined with a certain algorithm when the device enters the network, this network address can uniquely identify any device in the current network. Similar to Wi-Fi communication, this identification information is also easy to obtain and can be used to distinguish device communication information.

2) available meta-information based on the original packet: In addition to the field information related to the device identification, a complete network data packet also contains other information that can be used to calculate traffic characteristics. The most intuitive and convenient statistics are the packet length and data flow direction. Combining time information we can calculate the characteristics like the number of packets per unit time, data transmission rate, and packet length distribution. The timestamp and packet length can be directly obtained in the encapsulated frame header information, and the data flow direction is judged by the relationship between the device address, the source address, and the destination address.

Therefore, in a large number of network data packets, we can process each packet, discarding other less relevant information, and get simple tuples

$$P =< T, S, D, L >$$

T is the timestamp of the captured packet; S is the source address of the packet, and D is the corresponding destination address; L is the length of the packet. In this way, based on the obtained tuple set $S = \{P_1, P_2, ...\}$, the communication information set of a specific device d within a period of time can be obtained through address filtering

$$S(d) = \{P_1(d), P_2(d), \ldots\ldots\}$$

Where $P(d)$ is a tuple of the target device

$$P(d) =< T, L, D >$$

When performing traffic analysis on a specific device, you can capture all data packets related to the device communication, that is, filter out the data packets whose destination address or source address is the communication address of the device. By further judging whether the address is the destination address or the source address, it is possible to distinguish whether the data flow direction for the device is upstream or downstream, and mark it as D; T and L still represent timestamp and data length of the packet.

B. Traffic Analysis Process of Specific Single Device

After the above discussion and definition, we have clarified a complete attack process from distinguishing device eavesdropping data to finally identifying the working status of specific devices. The process is shown in the figure.

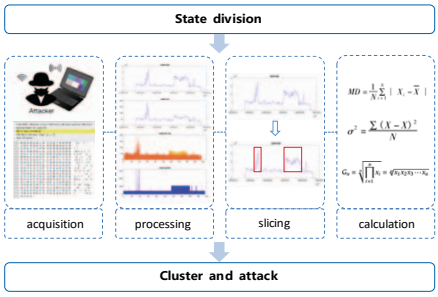


Fig. 2: Traffic Analysis Method and Processing

a) state division: The functions of the Internet of Things devices in the smart home are relatively simple. Each device only completes one or some functions, when the device completes different functions, it is in different states, and the corresponding flow characteristics are different. Therefore, a reasonable division of the device status is an important prerequisite for subsequent steps.

b) data acquisition: As discussed earlier, in a wireless network, the information we need to attack is easy to obtain. There is no need to touch the specific device being attacked, nor access the specific network through the key, but only

some easily accessible hardware devices and software can be used to capture the packet. In this article, we use $sniffer$ under macOS to capture packets in the WiFi network and combine it with $Wireshark$ [18] for preliminary analysis, use the $ebyte\ CC2531\ USB\ dongle$ hardware device to capture the ZigBee packets and combine it with the $PacketSniffer$ software for analysis.

c) data processing: After the original .pcap file is obtained through the previous steps, the data in the file is filtered and simply calculated to obtain basic data such as total data length, packet number, packet length distribution, and original packet sequence can be calculated for subsequent simple identification and feature calculation.

d) sequence slicing: After simple data processing, taking time as the horizontal axis and the corresponding data volume as the vertical axis, we can visually observe the obvious characteristics of the time series. For example, the interactive information sent by the device in the active state is often more abundant than heartbeat messages in the sleep state. To facilitate the automatic processing, avoiding the labor and possible errors caused by the human eye recognition and judgment. Here, the BG algorithm [1] is used to cut the original time sequence, and the sequence pieces in different states are divided so that each sequence piece obtained corresponds to a state piece of equipment working.

e) feature calculation and training: After the source data is divided by the sequence cutting algorithm, the traffic information in each time slice is the specific performance of a specific device activity flow. Therefore, feature extraction of this information can help identify the device activity and further infer user privacy. Due to the difference of device types, the effective characteristics of attacks on different devices may not be the same, the design and selection of the characteristics here cover the requirements of all devices as much as possible, including but not limited to the average value of Top 10%, the average value of Bottom 10%, the mode, the variance, the average, and the standard deviation. The extracted features will be trained to complete the automated flow analysis process. Since there are few features used for judgment, a simple SVM model can complete the learning task. This article will not design and optimize related models in this part, and only use existing models to complete the identification process.

C. Practical Cases of Attacks on Single Device

According to the device classification in Section II, we carried out traffic analysis attacks as described in the above process on several IoT devices with representative characteristics.

1) multi-state devices using Wi-Fi to communicate: Here, the HIKVISION surveillance camera is used as a typical representative to experiment. According to the description of the manual, the camera has a monitoring function. When the motion detection function is turned on, if the camera detects a change in the monitoring screen or human movement within the monitoring range, an alarm message will be sent to the client APP. Users can choose to view the monitoring screen

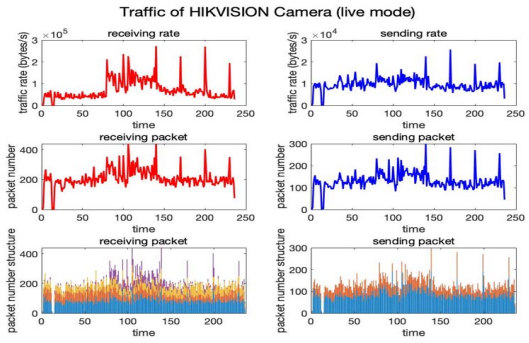


Fig. 3: Traffic of HIKVISION Camera (live mode)

on the APP and then the camera will transmit data to the APP and turn on the live broadcast mode. Otherwise, the camera will be in monitoring mode, and will not maintain the state of transmitting at all times, but will only trigger data transmission when the user-defined rules are met.

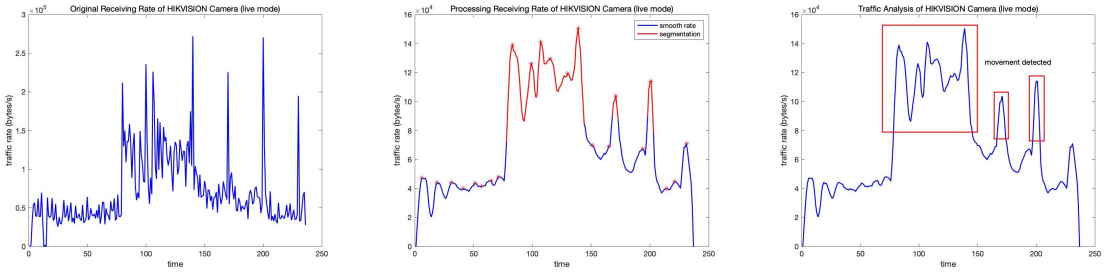
Take the surveillance mode as an example. When the camera and the APP transmit information, a large amount of interactive information will be generated, which will continuously generate upstream and downstream traffic. By deliberately arranging the behavioral changes of the participants in the experiment, we obtained the results in Fig. 3.

The 3*2 sub-pictures in the figure visually describe the characteristics of the camera's (rate, data packet quantity, data packet quantity structure) * (upstream direction, downstream direction), where the structure of the number of data packets is to further disassemble the number of data packets according to the size of the data packet, for example, packages are classified according to their size into four categories: small, medium, large, and extra-large. It can be seen that the data rate (that is, the number of bytes sent in one second) is positively related to the number of data packets, and the peak traffic in the receiving direction is usually directly related to the number of extra-large packets.

Subsequently, we conducted further data processing on the receiving rate, because the characteristic amount of receiving rate is the most obvious on the camera device.

In all following experiments, we used different features and parameters with the best effects to conduct specific attacks on different devices. As shown below, Fig. 4b smoothes the receiving rate and cuts the sequence. Three non-stationary states are cut out in the continuous steady-state (no action detected). According to experimental records, these three non-stationary sequences correspond to the information transmission after the camera recognizes the action.

In addition to the obvious difference in traffic characteristics between the calm state and the motion detection state in the live mode, we also analyzed the traffic in the live mode and the monitor mode, as well as the traffic with/without movement in the monitor mode. To describe this difference more accurately, we calculated the average value of the time slices after the



(a) origin traffic (b) slicing (c) analysis

Fig. 4: Attack Process of HIKVISION Camera (live mode)

sequence was cut, and clustered the results with SVM.

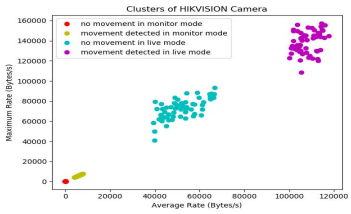


Fig. 5: Cluster of Door and Window Sensor

2) binary-state devices using ZigBee to communicate: We use XIAOMI door and window sensors as a representative of this type, such small sensors usually only take on simple functions due to their limited resources. When the sensor detects the action of the door and window, it will send a message to the gateway through the ZigBee protocol, and then the gateway will perform further calculation or scheduling, and the sensor often does not transmit a message when nothing is detected.

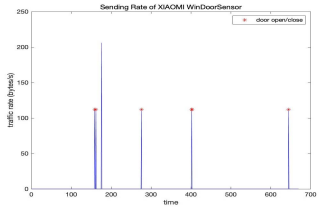


Fig. 6: Traffic of Door and Window Sensor

Fig. 6 shows the traffic analysis attack on door and window sensors. It can be seen that when no opening and closing event occurs, the sensor hardly sends traffic, while once closing/open event is generated, a data packet with a length of 112 bytes will be sent. Compared with the event record in the user APP, there is no missed judgment or wrong judgment.

3) other devices: The above two devices are more representative devices, which respectively show WiFi-based and ZigBee-based devices, and also reflect changes in the communication characteristics of devices in dual and multiple states.

In addition to the above two devices, we conducted traffic analysis attacks and clustering on doorbells, speakers, and gateways. The results are shown in the following figure.

IV. Traffic Analysis Attack On Multiple Devices

According to the traffic analysis of a single device, we can get the status information of each device at every moment. They reveal some key user privacy, such as which IoT devices the user is using at the moment, the activities of the people in the house, and the user's attention to the security information inside the house, etc. However, isolated single-device information has certain drawbacks in stealing user privacy. For example, the information they disclose is limited, the features are not obvious, or the devices that are affected by noise may have a certain possibility of misjudgment, and are easily affected by traffic shaping strategies. Therefore, based on single-device traffic analysis, we carried out a joint attack on multiple devices.

A. Background Knowledge of Multi-Device Joint Attack

The main basis for a multi-device joint attack is as follows

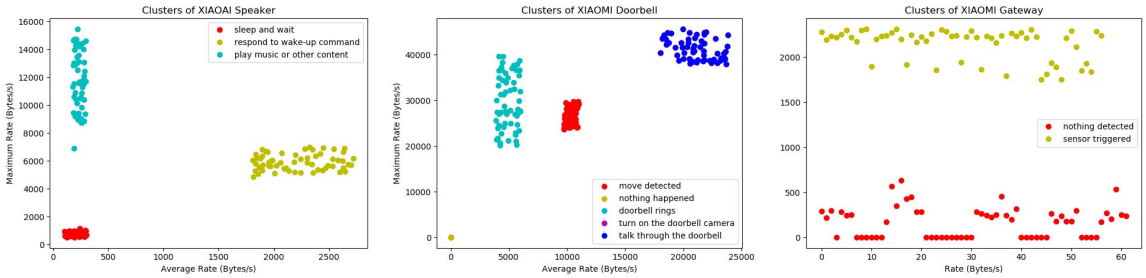
a) The occurrence of the same physical event may cause multiple devices to respond: for example, actions such as getting up and sitting down will be sensed by the movement sensor pasted on the seat, and the camera will also capture human movement information;

b) order of responses of different devices contains more detailed and specific information: the response order of the door and window sensors on the door and the camera in the house reflects the opening/closing action corresponding to the getting-in event or the getting-out event;

c) Indirect communication sensor devices and corresponding central devices have relatively consistent flow distribution: because these sensors need to use the central device for further calculation and communication, they tend to respond almost simultaneously.

B. Cases of Multi-Devices Joint Attack

For the example mentioned above, a confirmatory experiment was carried out here. The process of multi-device joint attack is relatively simple. Based on a single device attack, a state sequence within a period can be obtained, and subsequent



(a) Cluster of XIAOAI Speaker (b) Cluster of XIAOMI Doorbell (c) Cluster of XIAOMI ZigBee Gateway

Fig. 7: Attack Process of HIKVISION Camera (live mode)

calculations and analysis can be performed based on this sequence.

1) Multiple devices respond to the same event: In the experiment, we arranged a sensor to detect movement on the seat. The working mode of the sensor is similar to that of the door and window sensors. After detecting movement, the corresponding data will be transmitted. The camera in the live mode is also turned on in the room. By repeating the actions of standing up/sit down several times, the state sequence diagram shown in 8 is obtained. It can be seen that when the motion sensor and the camera capture the movement of a person on the seat, two devices with similar sensitivity will respond to the event at the same time and generate corresponding flow characteristics.

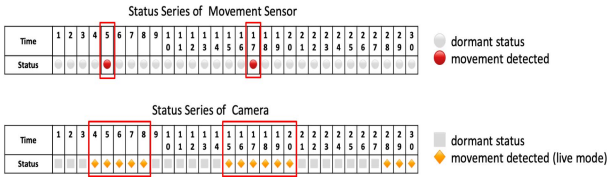


Fig. 8: Multiple Devices Respond to Same Event

2) Different events lead different response sequences of devices: We set up a smart home scene, that is, the entrance door is equipped with door and window sensors, and the camera is turned on in the room. Door and window sensors can only detect whether the event is opened or closed, but cannot determine whether the event is opened or closed and whether the door opening or closing action occurred in the event of going out or entering the door. When combined with the camera information inside the room, the more detailed determination can be updated.

In the experimental scenario without human intervention (that is, the user will not intentionally do unreasonable things to defend against attacks), it can be considered that the two sequences of "door opening, the camera captures movement, door closing" and "camera captures movement, door opening, door closing" represent entry and exit events respectively. Through experiments, we found that it is indeed possible to judge door opening and closing events and door entry and exit events through the information of these two devices.

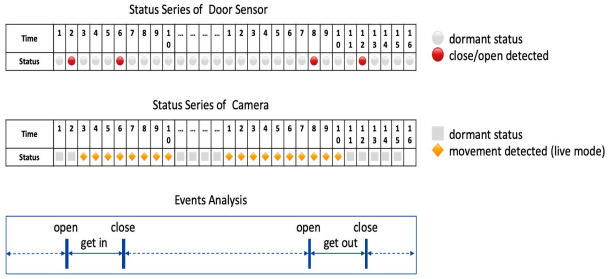


Fig. 9: Response Order and Event Determination

3) Cooperative response of combined communication devices: Small sensors focus on capturing changes in the environment, and timely send this information to a central device with strong computing capabilities such as a gateway through a short-distance transmission protocol. The gateway will further calculate and process the data, and then pass them to the cloud or perform other operations. The two cooperate to complete the basic functions, and neither is indispensable. As shown in 10, each data collection requires two devices to respond in sequence, and a single-device-based traffic masquerading defense for such a combination has little effect.

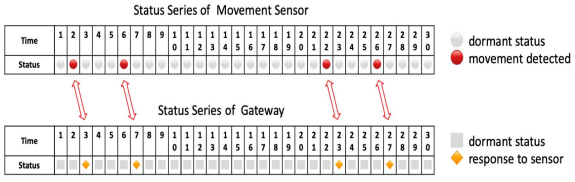


Fig. 10: Responses of Combined Communication Devices

Through the above three cases, we found that in a relatively complex smart home environment, devices usually have a certain degree of relevance. The household traffic information obtained by combining all the device information may expose more privacy, and it will also invalidate some traffic disguise, which brings more risks to user information leakage.

V. Discussion On Traffic Shaping

In order to protect the privacy information behind the traffic generated by the device, the currently widely discussed solution is traffic shaping, which reduces the accuracy of the attacker's traffic analysis by changing the external characteristics of the traffic. This article also briefly gives some protection methods using traffic masquerading strategies.

A. Traffic Shaping of Single Device

According to the equipment classification in Section II, different types of equipment should adopt different traffic shaping methods. Since the single state equipment is not vulnerable to attacks, it will not be mentioned here.

1) Binary state device: Binary state devices often have only two states of 0-1. The device in the 0-state is in the dormant state because it is not triggered, there is no need for data transmission. The 1-state is transferred from the 0-state after reaching a certain trigger condition. It is an "excited state" of the device. Therefore, corresponding data transmission is also required to complete the basic functions of the IoT device.

The conversion from a 1-state to a 0-state is difficult to achieve because it means that the device traffic cannot be transmitted normally or may be discarded, which violates the original intention of the device to complete the core functions of the Internet of Things. But the transition from the 0-state to the 1-state is achievable. The main realization idea is to properly replay the 1-state traffic to generate false event traffic. In this way, the real 1-state and the fake 1-state are mixed together, and it is difficult for the attacker to judge the real one. The time and number of occurrences of the 1-state increase the false positive rate. In addition, in the feature learning and discovery phase, since the difference between the two states is not grasped, it may be difficult for the attack based on traffic analysis to proceed.

2) Multiple states device: This type of device may have many complex non-zero states. Two processes are involved here, one is the ambiguity and confusion between non-zero states, and the other is the transition from 0 states to non-zero states.

As shown before, various information such as the length distribution of data packets, the number of data packets, and the rate at each moment are consistent, and the differences between different states are complex and significant. Therefore, the transition between non-zero states is relatively complicated. Equipment manufacturers or traffic protectors who subsequently intervene can consider processing all non-zero states into the same pattern so that all functional implementations are wrapped in the same pattern. For example, when the speaker responds to wake-up and when playing content, the traffic is the same. The attacker can only understand that the speaker is working, but cannot guess what function it is performing. Proper replay on this basis can achieve better results.

For devices that do not perform normalization processing for non-zero states, the attack accuracy can also be reduced through replay, but traffic selection needs to be taken into consideration when performing replay actions. In order to protect each state, each state needs to be replayed at a certain frequency. The former method only needs to replay the traffic of the same pattern at a relatively low frequency. In comparison, the latter method will generate more useless traffic.

B. Traffic Shaping of Multiple Devices

It is very inefficient to only implement isolated random traffic shaping strategies on different devices. Taking replay as an example, if the probability of device d_1 being replayed at a certain moment is P_1, and the probability of device d_2 being associated with it being replaying If it is P_2, the probability that both devices replay at the same time at this moment is P_1P_2, so that the probability of effective replay is greatly reduced, that is to say, in an isolated state, two devices have to replay multiple times before they can encounter one. Effective replay, which generates a lot of useless traffic.

To solve this problem, the shaper can introduce a relatively fixed replay protocol, such as replaying the flow after a fixed duration after real traffic, the fixed duration can form an agreement between related devices so that the replays of the related devices follow the same distribution. This protocol can be provided to the device when the shaper intervenes, or periodic protocol synchronization can be performed through other intermediate devices.

As the Internet of Things is still developing, the public's attention is still focused on functional expansion, and few manufacturers consider privacy and security in actual production. Most of the work is still at the stage of conception and simulation. Whether it is a single device or multiple devices, the injection of additional traffic will not affect the normal transmission of real traffic, because in practical engineering applications the latter has a higher priority in message queues. Besides, the additional power consumption introduced by flow injection is related to the frequency and timing of injection, and there are some other complexes and specific issues that are not illustrated in this section due to space constraints, the related strategies will be solved in detail in the future work.

VI. Related Work

A. Traffic Analysis

In the traditional Internet, attackers infer which website the victim is visiting through Website Fingerprinting (WF) [2]. Even if the text is encrypted, the URL length of the HTTP GET request cannot be concealed. The object number and size are of HTTP are used to identify encrypted network traffic, these two characteristics are sufficient to identify most websites in the world [3]. Using HTTP packet length and direction as attributes to infer the source of encrypted HTTP connections can identify sources with an accuracy of up to 90% [4].Using encrypted proxy [5] and anonymization methods [6] are not effective against attacks. In addition to the HTTP protocol, the SSH protocol is not secure. Even very simple statistics are sufficient to reveal sensitive information such as login passwords [7].

Traffic analysis of IoT devices has a long history, as well as traffic analysis of mobile devices [8] [9] [10]. As early as 2008, FATS attacks on Internet of Things devices were able to observe the private activities of household users [11]. By analyzing the flow of smart home products [12], we can understand the potentially sensitive information of the smart home status. The accuracy of attacks under different protocols to identify smart home devices and user activity status and behavior is as high as 90% or more [13]. However, as discussed earlier, most of these attacks assume that the device or ISP is malicious, and do not consider the actual attack scenario. When certain protection methods are adopted, the efficiency of attacks on a single device may be greatly reduced, which is not considered in current works either. Besides, the joint analysis of multiple device information is not considered in the previous work. Based on the state sequence matrix of the single device attack, we conduct a joint privacy inference attack on the state of multiple devices in the smart home environment.

B. Traffic Shaping

In order to resist various traffic analysis attacks, researchers have carried out a series of defenses. From the introduction of various encryption algorithms to encrypt data and text to the use of various anonymous networks, facts have proved that these are not very good against traffic analysis attacks. So some work began to use traffic masquerading methods to disguise the external characteristics of data traffic to achieve the purpose of deceiving attackers to prevent traffic analysis. Researchers [14] add noise traffic into the original traffic, thereby changing the traffic fingerprint, and use some transparent pictures to establish additional fake links to resist fingerprint attacks. Using packet filling and packet segmentation, the fingerprint of the target website is converted to the fingerprint of the closest web page, and then the anonymity of communication is protected at the least cost. This is the earliest concept of traffic shaping. By adopting a predictive packet filling strategy [15], further delay and bandwidth can be reduced. The privacy protection of smart homes has not attracted widespread attention. The relevant strategies currently available for investigation include the ILP [16] and STP method [17] proposed by Noah. Similar to the attack work, none of these protections work takes into account the factors associated with multiple devices.

VII. Conclusion

This article discusses the security vulnerabilities in the existing IoT scenarios. The traffic information in the environment may expose the user's private information. We verified this through experiments and built a real experimental scenario to reproduce a reasonable cross-protocol and cross-device joint attack process based on wireless channels. After analyzing the flow of a single device, we have obtained the characteristics of the flow distribution of the device in different working states, so that the real-time flow of a device can be attacked, and the working status and possible environmental information of the device can be judged. Based on the attack on a single device, we conducted a joint attack on all devices in the environment. By analyzing the state sequence diagrams of the devices, we obtained more detailed private information on the device groups that may have associated characteristics.

In terms of the discoveries of attack work, we proposed a traffic shaping strategy to protect device privacy. We evaluated the solutions in single-device and multi-device scenarios and verified the feasibility through theoretical derivation.

Acknowledgment

The work is partially supported by the National Key RD Program of China 2018YFB0803400China National Funds for Distinguished Young Scientists with No. 61625205, NSFC with No. 61751211, No. 61520106007, Key Research Program of Frontier Sciences, CAS, No. QYZDY-SSW-JSC002, and NSF CNS 1526638.

References

[1] Bernaola-Galván, Pedro, et al. "Scale invariance in the nonstationarity of human heart rate." Physical review letters 87.16 (2001): 168105.
[2] Hintz, Andrew. "Fingerprinting websites using traffic analysis." International workshop on privacy-enhancing technologies. Springer, Berlin, Heidelberg, 2002.
[3] Sun, Qixiang, et al. "Statistical identification of encrypted web browsing traffic." Proceedings 2002 IEEE Symposium on Security and Privacy. IEEE, 2002.
[4] Liberatore, Marc, and Brian Neil Levine. "Inferring the source of encrypted HTTP connections." Proceedings of the 13th ACM conference on Computer and communications security. 2006.
[5] Tor project: Anonymity online, august 2011.http://torproject.lu
[6] Coull, Scott E., et al. "On Web Browsing Privacy in Anonymized NetFlows." USENIX Security Symposium. 2007.
[7] Song, Dawn Xiaodong, David A. Wagner, and Xuqing Tian. "Timing analysis of keystrokes and timing attacks on ssh." USENIX Security Symposium. Vol. 2001. 2001.
[8] Stöber, Tim, et al. "Who do you sync you are? smartphone fingerprinting via application behaviour." Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks. 2013.
[9] Dai, Shuaifu, et al. "Networkprofiler: Towards automatic fingerprinting of android apps." 2013 Proceedings IEEE INFOCOM. IEEE, 2013.
[10] Conti, Mauro, et al. "Analyzing android encrypted network traffic to identify user actions." IEEE Transactions on Information Forensics and Security 11.1 (2015): 114-125.
[11] Srinivasan, Vijay, John Stankovic, and Kamin Whitehouse. "Protecting your daily in-home activity information from a wireless snooping attack." Proceedings of the 10th international conference on Ubiquitous computing. 2008.
[12] Copos, Bogdan, et al. "Is anybody home? Inferring activity from smart home network traffic." 2016 IEEE Security and Privacy Workshops (SPW). IEEE, 2016.
[13] Acar, Abbas, et al. "Peek-a-Boo: I see your smart home activities, even encrypted!." Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2020.
[14] Wright, Charles V., Scott E. Coull, and Fabian Monrose. "Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis." NDSS. Vol. 9. 2009.
[15] Yu, Shui, et al. "Predicted packet padding for anonymous web browsing against traffic analysis attacks." IEEE Transactions on Information Forensics and Security 7.4 (2012): 1381-1393.
[16] Apthorpe, Noah, et al. "Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic." arXiv preprint arXiv:1708.05044 (2017).
[17] Apthorpe, Noah, et al. "Keeping the smart home private with smart (er) iot traffic shaping." Proceedings on Privacy Enhancing Technologies 2019.3 (2019): 128-148.
[18] wireshark https://www.wireshark.org