Rogue Access Point Detection using ARP Failure due to the Intentional MAC Address Duplication

1st Kosuke Igarashi
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

2nd Hiroya Kato
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

3rd Iwao Sasase
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

Abstract—Detecting a rogue AP (RAP) in Wi-Fi network is imperative. Among various scheme, a user side detection scheme focusing on two channels used by a RAP is promising. That scheme can detect a RAP in a stable traffic environment by disclosing the presence of tow channel with channel interference. However, the detection performance is degraded in the real environment where traffic is more unstable. Thus, it is necessary to design the scheme which is independent of such factors. In this paper, we propose . Our main idea is that there exists a RAP and a LAP on the same path under the attack. This is because the RAP is established between a user device and a LAP for the attack. On the basis of this idea, the proposed scheme reveals that the AP with which a user device connects is a RAP by discovering the MAC address of a LAP on the same path. In order to find the MAC address, we leverage the phenomenon that a user device cannot receive Address Resolution Protocol (ARP) reply packets in the situation where its MAC address and that of a AP are duplicated on the same path. By doing this, the presence of a LAP is revealed, which can judge that the connected AP is a RAP. As aresult, the proposed scheme achieves accuracy of 96.5%. True positive rate and false positive rate are 31.0% higher and 9.0% lower than the previous scheme even in unstable traffic environment. Furthermore, the proposed scheme can detect RAPs accurately even in a real environment where the previous scheme cannot.

Index Terms—component, formatting, style, styling, insert

I. INTRODUCTION

With the rapid development of wireless communication techniques, Wi-Fi as the most commonly used Internet access technology is deployed and keeps spreading all over the world [1] . It is located in everywhere of our daily life, such as shopping malls, restaurants, public transit systems and so on. While the free access to Wi-Fi network attarcts a large number of users, it also allows adversaries to launch attacks to the users just by setting up a rogue AP (RAP) on their laptop in the network, which is called "Evil Twin Attack (ETA) " [2]. The RAP clones the Service Set IDentifier (SSID) and or even MAC address of a legitimate AP (LAP) provided by a public facility, which is the reason why it is called ETA. In the ETA, a RAP is established between a user device

and the Internet as Man-In-The-Middle (MITM) attacks [3]. Thus, adversaries can 'eavesdrop on the exchange of sensitive information such as identity credentials, passwords, and bank accounts by observing relayed packets through their laptop between a user device and a LAP. In addition, adversaries can also carry out an active attack by leading a user to phishing websites or infecting a user device with malicious softwares [4]. Since, wireless devices connect automatically to an AP which has the strongest Received Signal Strength Indication (RSSI) among all APs which have same SSID. Moreover, by exploiting the characteristic that users freely connect free Wi-Fi network, an adversary can succed in the attacks without being noticed by a user. Thus, the detection of the RAPs is urgent demand.

The attack model is divided into two models based on how a RAP provides the Internet service to user device. The one is a model where a RAP use mobile communication, and it can be detected easily with Internet Services Provider (ISP) names or Global IP addresses [5]. Thus, we focus on the other model where a RAP uses same gateway with LAPs in the network by connecting with one of them since it cannot be easily detected by existing schemes. Exisiting RAP detection schemes supposing this attack model are divided into network administrator side detections and user side detections. The network administrator side detections mainly use whitelist-based mechanisms based on physical features of APs [6] [7]. However, those solutions are inapplicable to Wi-Fi hotspots since they make netowork addministrators set additional devices in their infrastructures. On the other hand, the user side detections focus on communication features. In particular, most of the exisiting schemes utilize network latency, such as Round-Trip Time or Inter-packet Arrival Time [5] [8]. However, since such delay is caused by the software-based RAP on a laptop, latency based schemes can be easily evaded by using a hardware-based RAP. Thus, in order to cope with both software-based RAPs and hardware-based ones, the user side detection scheme which focuses on two communication channels used by a RAP is proposed [9]. That scheme can detect the RAP by finding out these two channels on the

basis of the decline in the throughput. That scheme is the most useful detection since it can detect a hardware-based RAP which does not cause delay. Hence, we focus on that scheme [9] as the previous scheme. Although the previous scheme is successful in the experimental environment, its detection performance is degraded by ubstable traffic in a real environment. Therefore, it is necessary to realize the user side detection which is independent of the network traffic.

In order to realize the user side detection which is independent of a network environment, in this paper, we propose . The main idea of our scheme is that there exist two APs, namely the RAP and a LAP, on the same path from a user device to a gateway. Therefore, in an attack scenario, besides the connected RAP, a LAP exists inevitably on the other side of the RAP because of the MITM attack. On the basis of this idea, the proposed scheme reveals the connected AP as RAP by finding MAC address of such LAP from obtainable beacon frames by a user device [10]. In order to find the MAC address, we leverage the phenomenon that a user device cannot receive Address Resolution Protocol (ARP) reply packets from a gateway in the situation where its MAC address and that of a AP are duplicated on the same path. The proposed scheme intentionally creates such situation by setting the MAC address of a user device to the one on the same path has. By doing this, the proposed scheme can reveal the connected AP as a RAP in an attack scenario. The contributions of our scheme are as follows:

1). To the best of our knowledge, the proposed scheme is the first one which is independent of features of a RAP. By focusing only on the characteristic of attack and a MAC address of a LAP, the proposed scheme does not allow an adversary to avoid detection by manipulating features of the RAP.

2). The proposed scheme achieves accurate detection performance without any error even in a real environment. It can guarantee beneficial effects on every available hotspot.

The rest of this paper is constructed as follows: Related works are described in Section II. The attack model, previous scheme and its shortcoming are intriduced in Section III. The proposed scheme is explained in Section IV. Various evaluation results are shown in Section V. Finally, the conclusions of this paper are presented in Section VI.

II. RELATED WORKS

Rogue AP (RAP) detection methods are mainly classified into two categories: network administrator side detections and user side detections. Network administrator side detections focus on the physical features such as Received Signal Strength Indication (RSSI) and clock skew which cannot be spoofed by an adversary. RAP can be detected by comparing with the physical features of it with those in the predefined whitelist with equipments such as traffic sensors in each Wi-Fi network.

Wu et al. [6] pay attention to the RSSI which is hard to be forged arbitrarily and highly correlated to the transmitter's location and power. For each LAP in a network, RSSI, which

is measured by additional costly devices, is registered as the information in whitelist beforehand. By using RSSI, even if the MAC address of an AP is identical to that in the whitelist, that scheme can disclose that it is a RAP with spoofed MAC address set by an adversary at different location. However, those solutions are inapplicable to Wi-Fi hotspots since administrators have little motivation to guarantee no attacks by setting up additional devices in their infrastructures. Although it is useful as a supplementary feature, using only RSSI is insufficient to detect a RAP with high accuracy.

In order to detect in more detail, Lanze et al. [7] focus on clock skew as a device fingerprinting based purely on physical properties. Clock skew is the time gap of clock signals caused by the crystal oscillator, which is one of the components equipped in each AP. Since the clock skew is a precise feature which is unique to each AP, that scheme can be useful. However, that scheme is inapplicable to Wi-Fi hotspots because it requires additional costly sensors for obsering the feature. Administrators have little motivation to guarantee their free network by setting up additional devices in their infrastructures. Thus, the detection schemes that require no equipment of additional devices by a network administrator are desired.

Meanwhile, user side detections do not need to introduce additional devices to a Wi-Fi hotspot. They focus on differences in the transmission characteristics caused by the extra hop to a RAP on the path between a LAP and user device. Compared with legitimate networks, extra hop results in several measurable changes in transmission characteristics such as Round Trip Time (RTT) and channel used between a user device and DNS server.

Mustafa et al. [5] differentiate RAPs from LAPs by measuring the RTT between the user device and the DNS server through different target APs (RAPs or LAPs). Because there exists the extra hop caused by the RAP on the path, RTT is longer in comparison to the case where a user directly connects to the LAP. Although that scheme which leverages the packet delay are useful only for the case where the adversary sets RAP up on the laptop, Jang et al. [9] reveal the fact that the computational power of the software bridging mainly accounts for the packet delay. Thus, the adversary can evade the packet delay based detection by utilizing hardware-based RAPs having little bridging delay unlike software-based RAPs.

In order to detect both types of RAPs, namely, software-based and hardware-based ones, Jang et al. focus on two communication channels utilized by a RAP between a user device and LAP [9]. Whereas a RAP intervene between a user device and LAP, two distinct channels are used to reduce communication delay caused by channel interference each other. For example, it is assumed that channel 1 is used as the channel between a user device and a RAP, and channel 6 is that between a RAP and a LAP. That scheme detects RAP by finding out the presence of these two channels with the throughput of the transmission from the user device to the DNS server. That scheme is the most robust user side detection which is independent of the performance of the RAP because
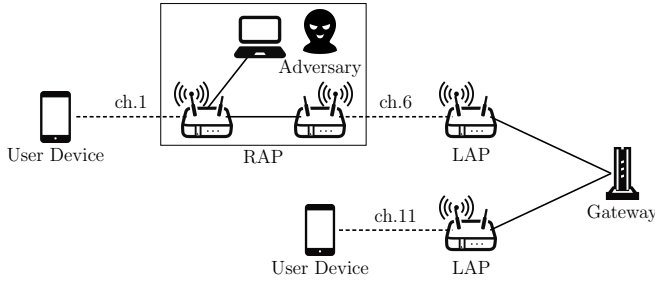
Fig. 1. The Attack Model

Fig. 2. Throughput in a Cafe

it is the countermeasure against a reasonable attack model where hardware-based RAP is used. Thus, we select [9] as the previous scheme. In the next section, we elaborate the previous scheme.

III. ATTACK MODEL AND PREVIOUS SCHEME

A. Attack Model

In an ETA, the adversary sets up a RAP which uses a SSID of a LAP in the targeted Wi-Fi network. Besides, the MAC address of the RAP is cloned from one of the LAPs in the network [3]. As a result, although a user device receives SSID broadcast from the RAP and LAPs, it cannot differentiate between these APs. Thus, since the user device simply connects with the AP that has a higher RSSI value, the RAP sends beacon frames with stronger signals. Fig. 1 shows the attack model. We assume that a RAP relays WLAN traffic between a LAP and a user device, which act as a MITM attack to steal private information of a user. By avoiding using mobile Internet access, e.g., 3G/4G, the adversary can evade simple detections with Internet Services Provider (ISP) names or Global IP addresses [5]. Furthermore, in addition to that, we assume that the adversary exploits hardware-based APs in order not to cause a computational delay [9]. In order to use distinct channels on the both sides, a RAP is composed of two routers which are interconnected with a LAN cable. One of these routers is connected to a LAP in station mode and the other disguise user device as a LAP in service mode. Because a high-end router which can relay packets with distinct channels appears nowadays, it can replace a RAP in our model.

B. Previous Scheme

1) Overview of the Previous Scheme: The main idea of the previous scheme [9] is that the adversary needs to use two distinct communication channels on the path from a user device to the LAP to avoid channel interference each other. The one is the channel for the path between a LAP and a RAP, and the other is that for the path between a RAP and the user device. Thus, from the perspective of the user device, there exists another channel on the route that is different from the channel with the connected AP. The extra channel cannot be observed directly from the user device. The previous scheme detects the RAP by finding out these two channels on the basis of the decline in the throughput. In order to decrease the
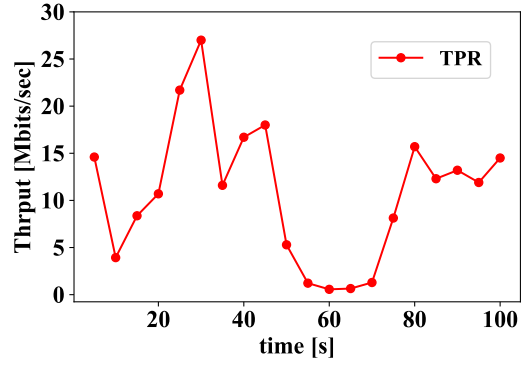
throughput, the previous scheme saturates the channel used between a LAP and the RAP by intentionally interfering a channel with an additional equipment in a user device. For example, when a user device is using channel 1 with the targeted AP which cannot be judged to be legitimacy, the equipment in a user device transmits a large number of packets to all the channel except channel 1 to saturate traffic on the path. If there exists the other channel on the route, the decline in the throughput can be observed by the user device, and the presence of RAP is revealed.

2) Shortcoming of the Previous Scheme: Although the previous scheme is successful in the detection for hardware-based RAP in the experimental environment, it cannot detect accurately in the real world. This is because throughput is considerably dependent on various factors of the network environment such as mobility of the traffic, collisions, network topology changes, and unintentional interference. Fig. 2 shows the graph regarding the change of throughput in a cafe on a weekday. Since the traffic in real environment is unsteady as shown in Fig. 2 in fact, the previous scheme is subject to environmental changes, which can lead to degrade the detection performance. Thus, the requirement that we must satisfy is to leverage factors which are independent of the network environment for the detection.

IV. PROPOSED SCHEME

In order to meet the requirements mentioned in Section III-B2, in this paper, we propose . In the following subsections, we explain the idea of the proposed scheme and the algorithm in detail.

A. Idea

The main idea of the proposed scheme is that there exist two APs, namely, the RAP and a LAP, on the same path from a user device to a gateway. In general, a LAP is the only device which exists on the path. Therefore, in this case, the LAP is identical to the AP directly connected with a user device. In an attack scenario, besides the connected RAP, a LAP exists inevitably on the other side of the RAP. Therefore, a connected AP can be revealed as the RAP when the presence of a LAP is detected on the same path.

On the basis of this idea, the proposed scheme reveals a LAP is on the other side of the connected AP by finding out the MAC address of a LAP. In order to discover the MAC address of a LAP on the same path, we leverage the phenomenon that a user device cannot receive Address Resolution Protocol (ARP) reply packets in the situation where there exist duplicate MAC addresses on the same path. The proposed scheme intentionally creates such situation by setting the MAC address of a user device to the MAC addresses obtained from beacon frames of APs in the communication range of a user device. Note that the MAC address of the AP with which a user device connects is excluded from targets for setting MAC addresses. If the MAC address of a user device is set to that of a LAP on the same path, the LAP receives ARP reply packets whose original destination is a user device before the user device receives them. Thus, since a user device cannot receive ARP reply packets, it continues to resend ARP requests, which results in disabling internet connectivity. By observing the continuance of resending ARP request packets within a definite period of time without ARP reply packets, the proposed scheme can reveal that there exists the RAP and a LAP on the path, which detects the attack.

When a user device connects with the RAP, there exists a MAC address of a LAP in the communication range of a user device. This is because the RAP are located relatively near a LAP to avoid communication delay. Hence, we can inevitably obtain the MAC address of a LAP in the case where there exists the RAP in a network. In the real situation, it is possible that there exist several LAPs in a communication range of a user device. Thus, we collect the only MAC addresses of APs which have the identical SSID to that of APs in the network. This is because RAP must utilize an SSID of a LAP for pretending to be LAP. A user device can receive ARP reply packets even if its MAC address is set to that of each LAP on distinct paths. This is because the MAC addresses can be duplicated except those on the same path.

Since the proposed scheme is independent of the real network environment, it is useful for overcoming the shortcoming of the previous scheme. In addition to that, the proposed scheme is not affected by a spoofed MAC address because it focuses on the only legitimate MAC address never spoofed.

B. Algorithm

In this subsection, the algorithm for detection based on searching the MAC address of a LAP on the same path is explained. The proposed algorithm mainly consists of 1) MAC address collection phase and 2) ARP reply based detection phase.

1) MAC Address Collection: Let $AP_{connect}$, $SSID_{connect}$ and $m_{connect}$ denote a AP which connects with a user's device, its SSID and its MAC address, respectively. The set of MAC addresses of APs whose SSIDs are identical to $SSID_{connect}$ is created through beacon frames of them. Let the set is denoted by $M_{all} = \{m_{input} | 0 \leq input \leq n_{all}\}$, where n_{all} is the number of collected MAC addresses.
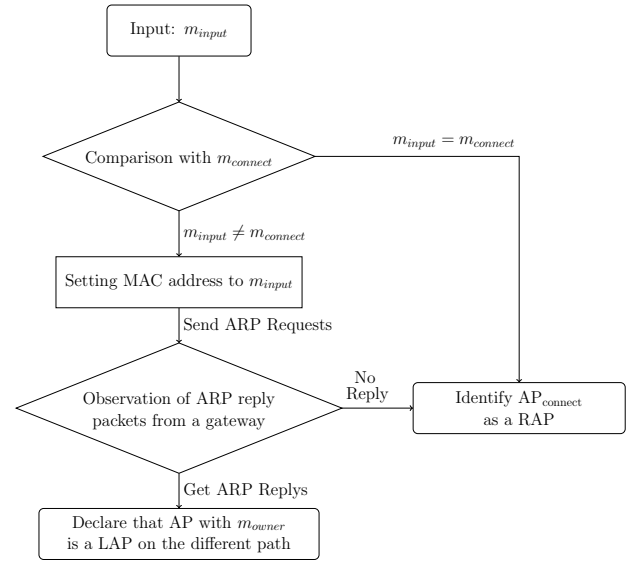

Fig. 3. The Flowchart of the Proposed Scheme

2) ARP Reply based Detection: Fig. 3 shows the flowchart of this phase. As shown in Fig. 3, this phase consists of three procedures which are 1) Comparison with $m_{connect}$, 2)Setting MAC address, and 3) Observation of ARP reply from the gateway to the user device. These procedures are repeatedly conducted for every m_{input} in M_{all} unless the RAP is detected.

In the first phase, m_{input} and $m_{connect}$ are compared. If they are the same MAC address, it easily judges the either of them is the RAP due to the cloned address. In this case, since RAP is detected, the detection phase is finished. However, in the case where the RAP clones a MAC address of a LAP beyond the communication range of a user's device or it does not clone, the accordance of MAC addresses cannot be detected only by this MAC address checking. Thus, the detection process goes to the second phase.

In the second phase, the MAC address of user device is set to m_{input}. After the MAC address is set to m_{input}, the connection between the user device and $AP_{connect}$ is once lost since the gateway become unable to use the original MAC address as a destination for the packets. Thus, the user device sends ARP request in order to reconnect with it through the $AP_{connect}$ automatically due to the stronger RSSI than any other APs.

Finally, in the third procedure, the ARP reply packets whose destination is set as m_{input} are observed to investigate whether the AP with m_{input}, is on the same path with the user's device. If the packets do not reach the user's device, the $AP_{connect}$ can be revealed as the RAP which exists between the user device and the LAP with m_{input}, and the detection phase is finished. Otherwise, the $AP_{connect}$ is judged that it is on the distinct path from the AP with m_{input}. In this case, the same procedures in the flowchart are repeatedly conducted for another m_{input} in $M_{A_{all}}$ until the RAP is detected. If

the detection phase is carried out for all m_{input} without the detection of RAP, the $\mathrm{AP_{connect}}$ is declared as a LAP.

V. EVALUATION

In order to demonstrate the effectiveness of the proposed scheme, we compare it with the scheme [9] which interferes the channel between a LAP and RAP explained above as a previous scheme.

The metric of the evaluations are ACCuracy (ACC), TPR (True Positive Rate), and FPR (False Positive Rate) defined as

$$\mathrm{ACC} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}} \quad (1)$$

$$\mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \quad (2)$$

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \quad (3)$$

where TP, TN, FP, and FN denote the number of True Positive (RAPs is reregarded as RAPs), True Negative (LAPs are regarded as LAPs), False Positive (LAPs are regarded as RAPs), and False Negative (RAPs are regarded as LAPs), respectively. We evaluate our scheme with these metrics by two scenarios which are the case of attack where a user device connects with a RAP and that of non-attack where a user device connects with a LAP.

A. Experimental Setup

1) Detector: We implemented the detectors in a laptop, which is a MacBook Pro with an Intel Core i5 CPU and 16GB RAM. We observe ARP packets with T-shark, which is a tool for capturing packets [11]. In order to configure [9] for comparison, we use a TP-Link Archer C6 as an interference device.

2) LAP and RAP: TP-Link Archer C6 is also used to setup the LAP. As regards the RAP, in order to use distinct channels on both sides as the model in the previous scheme, it is composed of two APs (TP-Link Archer C6 and TP-Link Archer C50). These two APs, where one is in the station mode ($\mathrm{AP_{sm}}$) and the other is in AP mode ($\mathrm{AP_{am}}$), are interconnected using a LAN cable. The $\mathrm{AP_{sm}}$ is responsible for repeating packets to and from the LAP and $\mathrm{AP_{am}}$ has a spoofed SSID and MAC address. All devices are operated in the IEEE 802.11n mode with MIMO. We arrange a LAP, RAP, and user device at equal intervals and it is about 5 feet.

3) Traffic Scenario: In order to demonstrate the robustness against unstable traffic in real environment, we intentionally generate random traffic to the LAP at random time in each experiment.

4) Time of Detection: The experiments are conducted for each case, namely attack scenario and non attack scenario 100 times. The average time required per detection is represented as T. It is affected by the observation time of ARP procedure per a AP, which is represented as Δt , and also the number of LAPs before a RAP is detected in an attack scenario. We conducted each evaluation by changing Δt from 5 seconds to 10 seconds at every second.

B. Evaluation of the Proposed Scheme

In order to show the effectiveness of the proposed scheme (Prop.), we compare it with the previous scheme [9] (Prev.). Fig. 4 shows the results of the ACC of each scheme. As shown in Fig. 4, the previous scheme cannot accurately detect the attack in random traffic scenario, and the ACC is about 69%. However the ACC of the proposed scheme is lower than that of the previous scheme when each ARP observation time is not greater than 6s. The ACC is getting higher as the observation time increases. In particular, in the case where the time is longer than 7s, ACC is improved up to 96.5% in the propsed scheme. Fig. 5 shows the FPR of each scheme. As shown in Fig. 5, the longer each observation time is, the lower FPR is in the proposal scheme. It decreases up to 74% in the result of the last three time settings compared with that of the beginning. In additon, Fig. 6 shows the TPR of each scheme. As shown in Fig. 6, TPR of the proposed scheme is 100.0% regardless of the observation time, which means it never pass a RAP over in an attack scenario.

In order to reveal the reason of these results, we analyze the ARP packets in detail. Through the packet analysis, we disclose the reason is that the time for finishing ARP procedure tends to be longer than 6s and it is not always fixed. Thus, in the case of less than 7.0 seconds, several LAPs are detected as RAPs incorrectly since it is not enough for a user device to get ARP reply packets while a RAP is never overlooked. Given the fact, we conducted the further experiment to realize more precise detection by setting enough time to auquire ARP reply packets. As a result, we conclude that the proposed scheme enables the detection without any error when the Δt is set to 15 seconds.

C. Evaluation in a Real Environment

In order to demonstrate the robustness and the average time per detection time T of the proposed scheme in a real environment, we conducted an experiment in a cafe and evaluate ACC and the total time required for the detection. Fig. 7 shows the Wi-Fi network model in the cafe. As shown in Fig. 7, there exist two LAPs, which are LAP(a) and LAP(b), and the both have same SSID and two different MAC addersses for two frequency bands which can be used in IEEE 802.2n. The MAC addresses of LAP(a) are represented as m_A and m_a , and similarly, those of LAP(b) are represented as m_B and m_b. Through the evaluations, the user device is always connected to m_A. In non attack scenario, we use m_B and m_b as MAC address in the set of M_{all} defined in Section IV-B. In contrast, we construct the attack scenario experimentally by assuming m_A and m_a as the MAC address of a RAP and that of a LAP which is on the same path with RAP since an acutual RAP cannot be installed in a real world. In order to match the number of the MAC addesses which need to be input to our scheme, we only use m_a and m_B in the attack scenario. Our experimental situation can be regarded as the same situation with the attack model shown in 1. The experiments are conducted 100 times in each situation around 2:00pm on a weekday at an cafe. The observation time of
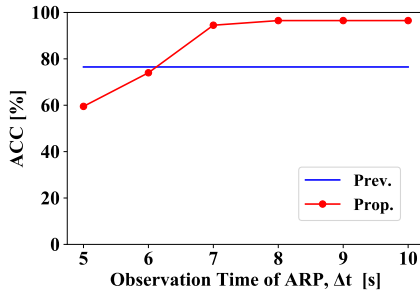
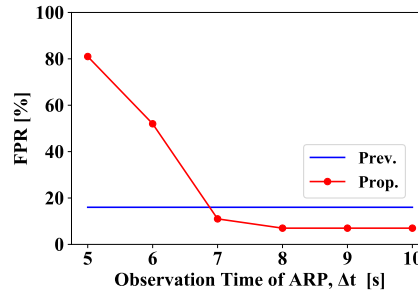Fig. 4. The ACC of the Prop. and Prev.

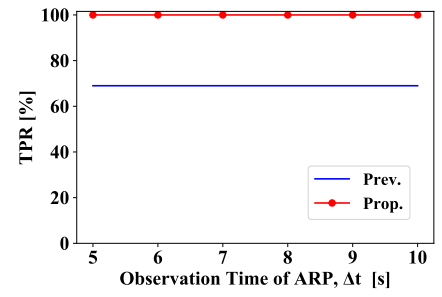
Fig. 5. The FPR of the Prop. and Prev.

Fig. 6. The TPR of the Prop. and Prev.

Fig. 7. The Network Model in the Cafe
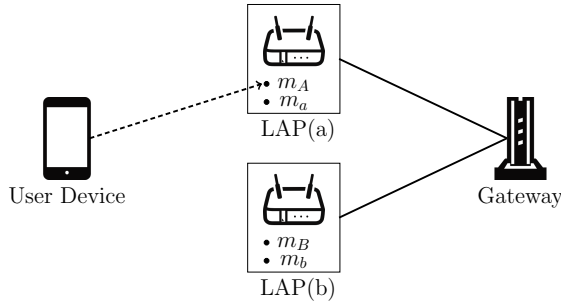
TABLE I
EVALUATION RESULT IN REAL ENVIRONMENT

ACC (%)	Avg. Total Time (s)
100.0	32.1

ARP procedure is set to 15 seconds enough to get ARP reply packets.

TABLE I shows the results in the real environment. The proposed scheme realizes 100% accuracy even in a real environment if Δt is enough. At that time, T is 32.1 seconds. It is much shorter than the time that the most of recent security softwares take to scan their disk. Thus, it guarantees the device's safety for users without being annoyed. Through this result, we conclude that the proposed scheme can accurately detect the attack with relatively short time in a real environment whose traffic is unstable.

However, as with other existing schemes, the proposed scheme also assumes Wi-Fi network models where legitimate repeaters are not installed. It may be usual to introduce a legitimate repeater in network to relay traffic farther at the expense of transmission speed in a large area. In this case, the proposed scheme cannot distinguish a RAP and legitimate repeater since both of them relay packets between a user device and a LAP in the same way as MITM attack. In order to detect the attack even in such Wi-Fi networks, we focus on their RSSI values, which can tell their general distance each other [12]. Since a legitimate repeater has a function to relay packets from a LAP to devices which cannot connect

with the LAP because of the long distance, it should be located far from a LAP in general. In contrast, a RAP is basically introduced near a connecting LAP not to cause traffic delay due to their long distance. Thus, we assume that a AP can be judged whether it is a legitimate repeater or not on the basis of this idea. In the future, we plan to devise the additional countermeasures and conduct some experiments so as to distinguish legitimate repeater with RSSI value.

VI. CONCLUSION

In this paper, we have proposed . We collect MAC addresses from user side and set the MAC address of user device to them. By observing ARP packets in the situation, we can reveal the legitimacy of connected AP. The detection performance of the scheme is better than the previous scheme. The results show it can detect a RAP without any error even in unstable traffic environment. In addition, the simulation in a small cafe shows the availability in a real network. In the future, we will conduct a large-scaled examination of the proposed scheme. Furhermore, we need to expand the scheme for the network where a legitimate repeater is arranged.

REFERENCES

[1] A. Burns, L. Wu, X. Du, and L. Zhu, "A novel traceroute-based detection scheme for wi-fi evil twin attacks," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.

[2] Q. Lu, R. Jiang, Y. Ouyang, H. Qu, and J. Zhang, "Bire: A client-side bi-directional syn reflection mechanism against multi-model evil twin attacks," *Computers & Security*, vol. 88, p. 101618, 2020.

[3] M. Agarwal, S. Biswas, and S. Nandi, "An efficient scheme to detect evil twin rogue access point attack in 802.11 wi-fi networks," *International Journal of Wireless Information Networks*, vol. 25, no. 2, pp. 130–145, 2018.

[4] A. Kumar and P. Paul, "Security analysis and implementation of a simple method for prevention and detection against evil twin attack in ieee 802.11 wireless lan," in *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, 2016, pp. 176–181.

[5] H. Mustafa and W. Xu, "Cetad: Detecting evil twin access point attacks in wireless hotspots," in *2014 IEEE Conference on Communications and Network Security*. IEEE, 2014, pp. 238–246.

[6] W. Wu, X. Gu, K. Dong, X. Shi, and M. Yang, "Prapd: A novel received signal strength–based approach for practical rogue access point detection," *International Journal of Distributed Sensor Networks*, vol. 14, no. 8, p. 1550147718795838, 2018.

[7] F. Lanze, A. Panchenko, B. Braatz, and T. Engel, "Letting the puss in boots sweat: Detecting fake access points using dependency of clock skews on temperature," in *Proceedings of the 9th ACM symposium on Information, computer and communications security*, 2014, pp. 3–14.

[8] C. Yang, Y. Song, and G. Gu, "Active user-side evil twin access point detection using statistical techniques," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1638–1651, 2012.

[9] R. Jang, J. Kang, A. Mohaisen, and D. Nyang, "Catch me if you can: Rogue access point detection using intentional channel interference," *IEEE Transactions on Mobile Computing*, vol. 19, no. 5, pp. 1056–1071, 2020.

[10] O. Nakhila and C. Zou, "User-side wi-fi evil twin attack detection using random wireless channel monitoring," in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, 2016, pp. 1243–1248.

[11] "Tshark-the wireshark network analyser," http://www.wireshark.org.

[12] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 mac layer spoofing using received signal strength," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*. IEEE, 2008, pp. 1768–1776.