Conference Paper Title*

*Note: Sub-titles are not captured in Xplore and should not be used

1st Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

2nd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

3rd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

***Abstract*—This document is a model and instructions for LaTeX. This and the .cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

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

攻撃モデル先に言いたい感ある.

I. INTRODUCTION

IP 見ればすぐわかるから攻撃者は MITM パターンできますよっていう説明

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. [**?**] 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, that scheme is hard to detect RAP which is located near the LAP because RSSI is not as exact as it can indicate a small difference of the nearby location.

In order to detect in more detail, Lanze et al. [**?**] focus on clock skew as a device fingerprinting based purely on physical properties. Clock skew is an unvoidable physical phenomenon that causes crystal oscillator based clocks to run with minuscule yet measurable deviations in speed. However, these network administrator side detections are inapplicable to Wi-Fi hotspots because they have to setup additional sensors or install detection software in their infrastructure to prevent attacks besides providing free Internet service. 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. [10] 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. [12] 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, [12] focuses on two communication channels utilized by a RAP between a user device and LAP. 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 it is the countermeasure against a reasonable attack model where hardware-based RAP is used. Thus, we select [12] as the previous scheme. In the next section, we elaborate the previous scheme.

identify applicable funding agency here. If none, delete this.

III. ATTACK MODEL AND PREVIOUS SCHEME

A. Attack Model

In an evil twin attack, 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. As a result, although a user device receives SSID broadcast from both LAP and the RAP, it cannot differentiate between these APs. Thus, the user device simply connects with the AP that has a higher RSSI value. We assume that a RAP relays WLAN traffic between a LAP and a user device, which act as a "man-in-the-middle-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 [10]. In addition to that, we assume that the adversary exploits hardware-based APs which cannot be detected accurately by existing schemes since they do not cause a computational delay due to a software bridging.

B. Previous Scheme

1) Overview of the Previous Scheme: The main idea of the previous scheme [12] 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. Since the traffic in real environment is unsteady, the previous scheme is subject to environmental changes, which can lead to degrade the accuracy. 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 firstly explain the idea of the proposed scheme. In the next subsection, the algorithm is described 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 the RAP, a LAP exists inevitably on the other side of the RAP due to a man-in-the-middle-attack. 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 that a LAP is on the other side of the connected RAP 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, a LAP receives ARP reply packets whose original destination is a user device before a 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 the 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 AP connected by a user device. 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 A_{target} denote a AP which connects with a user's device. The set of MAC addresses of APs whose SSIDs are identical to that of $M_{A_{target}}$ in the communication range of a user's device is created through beacon frames of them. Let the set denote $M_{all} = \{M_{input} | 0 \leq input \leq n_{all}\}$, where n_{all} is the number of collected MAC addresses.

2) ARP Reply based Detection: Fig. **??** shows the flowchart of this phase. As shown in Fig. **??**, this phase consists of four procedures which are 1) Comparison with $M_{A_{target}}$, 2)Setting M_{user_device} to $M_{A_{input}}$, 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, the $M_{A_{input}}$ and the $M_{A_{target}}$ 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, M_{user_device} which denotes the MAC address of a user' s device is set to $M_{A_{input}}$.

After M_{user_device} is set to $M_{A_{input}}$, the connection between the user device and A_{target} 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 A_{target} automatically due to the stronger RSSI than any other M_{all}.

Finally, in the third procedure, the ARP reply packets whose destination is set as $M_{A_{input}}$ are observed to investigate whether the A_{input} is on the same path with the user's device. If the packets do not reach the user's device, the A_{target} can be revealed as the MAC address of the RAP which exists between the user device and the LAP with A_{input}, and the detection phase is finished. Otherwise, the A_{target} is judged that it is on the distinct path from the A_{input}. In this case, the same procedures in the flowchart are repeatedly conducted for another A_{input} in $M_{A_{all}}$ until the RAP is detected. If the detection phase is carried out for all A_{input} without the detection of RAP, the A_{target} is declared as a LAP.

V. EVALUATION

In order to demonstrate the effectiveness of our scheme, we compare it with the scheme [12] 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

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$TPR = \frac{TP}{TP + FN} \tag{2}$$

$$FPR = \frac{FP}{FP + TN} \tag{3}$$

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

We implemented the detectors in a laptop, which is a MacBook Pro with an Intel Core i5 CPU and 16GB RAM. In order to configure [12] for comparison, we use a TP-Link Archer C6 as an interference device.

Simiraly, the same AP devices are used for both LAP and RAP. In additon, in order to set a RAP up for distinct channel from LAP, TP-Link Archer C50 is introduced as a repeater between the RAP and LAP. These two APs, where one is in the station mode and the other is in AP mode, are interconnected using a LAN cable. 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.

B. 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. Fig. **??** shows one of the traffic examples used in the experiments.

C. Time of Detection

The experiments are conducted for 100 times in each case, namely attack scenario and non attack scenario, respectively. The average time required per detection is represented as T. It is affected by the observation time of ARP procedure per AP, which is represented as Δt , and also the number of LAPs before a RAP is detected in an attack scenario. We conduct each evaluation by changing Δt set to 5s through 10s at every second. In addition, during the time, if ARP reply packets are observed on the occasion of the time, our scheme judges the AP is not on the same path with a targeted AP and proceed to the next AP. Conversaly, if ARP reply packets cannot be observed during the observation time, our scheme regards the AP as a RAP and quit continuing the entire detection.

D. Evaluation of the Proposed Scheme

First, in order to show the effectiveness of our scheme, we compare it with [12] with ACC. Fig. **??** shows the result of our evaluation for each scheme. The both schemes are conducted in the random traffic scenario. As shown in Fig. **??**, [12] cannot detect the attack accurately and the ACC is about 69%. As regards the proposal scheme, however the ACC is lower than that of [12] when each ARP observation time is shorter than 5s, it is getting higher with the observation time. In particular, in the case where the time is longer than 7s, ACC is improved up to 96.5%.

TABLE I
EVALUATION OF THE DETECTION

Δt (s)	ACC (%)	TPR (%)	FPR (%)
5.0	59.7	100.0	19.4
6.0	74.0	100.0	48.1
7.0	94.4	100.0	88.8
8.0	96.5	100.0	92.9
9.0	96.4	100.0	92.7
10.0	96.5	100.0	93.1

As a result, shown in TABLE **??**, the longer each observation time is, the higher FPR is. Moreover, the higher FPR results in the higher ACC, directly since the TPR is always 100.0%. In order to reveal the reason, 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 lower FPR, LAPs are detected as RAPs incorrectly since it is not enough for a user device to get ARP reply packets. Given the fact, we conduct the further experiment to realize more precise detection by setting enough time to auquire ARP reply packets. As a result, we enable the detection without any error when the Δt is set to 15s.

E. Evaluation in a Real Environment

In order to demonstrate the effectiveness of our scheme in a real enrionment, we conduct it in a cafe and evaluate ACC and the total time required for the detection. There exists three APs arranged, whose SSID are all same. In the attack scenario, one of them is replaced by a RAP, which has a same SSID. In the same way with the last experiment above, we conduct our scheme in the both cases where a user device connects with a RAP or LAP. The experiments are conducted around 2:00pm on a weekday at an cafe. The observation time of ARP procedure is set to 15s enough to get ARP reply packets. TABLE **??** shows the results in the real environment. Our scheme realize 100% accuracy even in a real environment if the time for observation of ARP procedure is enough. At that time, the avg. total time per detection is 32.1s.

Through this result, it can be said that our proposal can detect the attack accurately in a real environment whose traffic is unstable. However, as with other existing schemes, our schemes also assumes Wi-Fi network models where legitimate repeaters are not installed. It may be not unusual to introduce a legitimate repeater in their network to relay traffic farther at the expense of transmission speed in a large area. In this case, our proposal can not distinguish a RAP and legitimate repeater since both of them relay packets between a user device and LAP in the same way as man-in-the-middle. However, in order to detect the attack even in such Wi-Fi networks, we are focusing on their RSSI values. Since a legitimate repeater has a function to rely packets from a LAP to where it cannot do due to 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. On the basis of this idea, we work on the additional procedure as a future work to distinguish legitimate repeater with RSSI value, which can tell their general distance each other [**?**]. For example, it can judge a AP as a legitimate repeater if their difference of RSSI values are larger than a threshold of the value.

TABLE II
EVALUATION RESULT IN REAL ENVIRONMENT

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

REFERENCES

[1] A. Adya, P. Bahl, R. Chandra, and L. Qiu, "Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks," n Proc. of ACM Annual International Co.nference on Mobile Computing and Networking, MOBICOM, 2004, pp. 30-44.

[2] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "Enhancing the security of corporate Wi-Fi etworks using DAIR," in Proc. of ACM International Conference on Mobile Systems, Applications, and Services, MobiSys, 2006, pp. 1–14.

[3] R. Chandra, J. Padhye, A. Wolman, and B. Zill, "A location-based management system for enterprise wireless LANs," in Proc. of USENIX Symposium on Networked Systems Design and Implementation NSDI, 2007.

[4] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in Proc. of ACM Workshop on Wireless Security, 2006, pp. 43–52.

[5] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in Proc. of the 27th Conference on Computer Communications, INFOCOM, 2008.

[6] 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 Proc. of ACM Symposium on Information, Computer and Communications Security, ASIACCS, 2014, pp. 3–14.

[7] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," IEEE Trans. Mob. Comput., vol. 9, no. 3, pp. 449–462, 2010.

[8] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in Proc. ofACM Annual International Conference on Mobile Computing and Networking, MOBICOM, 2008.

[9] S. Nikbakhsh, A. B. A. Manaf, M. Zamani, and M. Janbeglou, "A novel approach for rogue access point detection on the client-side," 27th International Conference on Advanced Information Networking and Applications Workshops, 2012.

[10] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue AP detection," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 11, pp. 1912–1925, 2011

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

[12] R. Jang, J. Kang, A. Mohaisen and D. Nyang, "Catch Me If You Can: Rogue Access Point Detection Using Intentional Channel Interference," in IEEE Transactions on Mobile Computing.