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 IEEEtran.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 features in the predefined whitelist with equipment setup such as a traffic sensor 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. RSSI, which is measured by additional coslty devices, is registered as the information in whitelist. By using RSSI, even if an AP has the same MAC address as 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 additional devices are desired.

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

Meanwhile, user side detections do not need to introduce costly 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's 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 and 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 attack for which 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, [12] focuses on two communication channels utilized by a RAP between a user's device and LAP, respectively. Whereas a RAP intervene between a user's device and LAP, two distinct channels are used to reduce communication delay caused by channel interference each other. For example, it is assume that channel 1 is used as the channel between a user's device and a RAP, and channel 6 is that between a RAP and a LAP. That scheme detect RAP by finding out these two channels with the throughput of the transmission from the user's 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 which hardware-based RAP is used. Thus, we select [12] as the previous scheme. In the next section, we elaborate the previous scheme.

III. ATTACK MODEL AND PREVIOUS SCHEME

A. Attack Model

In an evil twin attack, the adversary sets up RAP using a SSID of a LAP in the targeted Wi-Fi network and MAC address cloned from one of the APs in the network. As a result, although a user's device receives SSID broadcast from both LAP and the RAP, it cannot differentiate between these APs. Thus, the user's device simply connects with the AP that has a higher RSSI value. We assume the model that a RAP relays WLAN traffic between a legitimate AP providing Internet connectivity and a user's device, which act as a man-in-the-middle-attack. By avoiding to use mobile Internet access, e.g., 3G/4G, the adversary can evade detection 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 user's device to the LAP to avoid channel interference each other. The one is the channel for the path between LAP and RAP, and the other is that for the path betweeen RAP and user's device. Thus, from the perspective of the user's 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's device. Since the throughput value is dependent on the traffic on the path, the channel which is used between a LAP and RAP can be detected by a decline in the throughput. In order to decrease the throughput, the previous scheme saturates the channel used between LAP and RAP by intentional channel interference. For example, when a user's device is using channel 1 with the targeted AP which cannot be judged to be legitimacy, the user-side device introduced for intentional channel interference transmit a large number of packets with all the channel except channel 1 to saturate the path. If there exists the other channel on the route, the decline in the throughput can be observed by the user's 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.

IV. PROPOSED SCHEME

In order to meet the requirements mentioned in Section ここでコンパイルエラーが起こっているので一旦コメントアウト 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 our scheme is that there exist two APs, namely, RAP and LAP, in the communication range of a user's device which are both on the same path from it to a LAP. In general, a LAP is the only device which exists on the same path from a user's device to a gateway. In contrast, since a RAP act as a man-in-the-middle, there exists another AP, which is legitimate, on the other side of a connected AP in an attack scenario. Therefore, a connected AP can be revealed as a RAP when a LAP is detected on the other side of it.

Based on this idea, our scheme reveal a LAP on the other side of a connected RAP by finding out its MAC address from beacon frames in the communication range of a user's device. Although, it is assumed that there exist LAPs on the other path in a communication range of a user's device since several APs which have same SSID canbe deployed in a network. In order to solve this problem, our scheme observe ARP reply packets from a gateway whose original destination is a user's device, setting MAC address of a user's device to their MAC addresses on purpose. In a non attack scenario, a user's device can acquire evev if its MAC address is set to that of LAPs on the distnct paths. In contrast, in attack scenario, there exists a case that the ARP reply packets cannot be sent to a user's device when user's MAC address is set to that of the RAP. In other words, the same MAC address of the RAP is included as a destination of them in the packets. Since the ARP reply packets destinated originally to the user's device are go through the RAP on the same path at first, they result in being acquired by the RAP before being done by the user's device.

By doing so, our scheme can reveal that there exists two APs on the path, detecting the attack. In addition to the independence of a real environment, our scheme is not affected by a spoofed MAC address because it focuses on a legitimate MAC address never spoofed.

B. Algorithm

In this subsection, the algorithm for detection based on searching the MAC address of LAP on the same path is explained. The algorithm consists of three procedures, 1) AP information collection, 2) setting MAC address on user's device, and 3) ARP observation. The second and last procedures are repeatedly conducted for every MAC address acquired in the first phase which is presented as 試行回数の数式.

1) AP Information Collection: In this procedure, MAC address of APs, including an AP directly connected, which exist in the communication range of a user's device and have SSID of the network a user is trying to use are collected by the user's device from beacon frame they are transmitting. ここで収集した MAC アドレスをこう表す，直接接続はこう表す. It does not matter whether the RAP is spoofying its MAC address or not. At this stage, if same MAC addresses are acquired, it means either of them clone another MAC address.

Thus, using the network should be avoided whether it is on the same path or not because the risk of being attacked is extremely high. In contrast, in the case an RAP clones the MAC address which the LAP far from the user's device has, the user's device cannot receive both of the MAC addesses. Since it cannot detect only by collecting MAC addresses at this procedure, the further research is needed.

2) Setting MAC Address on User's Device: In order to detect an RAP which cannot be done only by searching the overlapping of MAC addresses at collection phase above, our scheme research whether there exists another AP on the other side of the connected AP using the collected MAC address. In this procedure, the MAC address of the user's device is changed to one of the collected MAC addresses in preparation for the ARP observation at next phase.

3) ARP Observation: In this procedure, ARP is observed to search MAC address the LAP on the other side of the connected AP has if the user's device is attacked. ARP is a procedure always done at the beginning of the Wi-Fi communication for mapping IP address to MAC address in a LAN to establish communication to the Internet and composed of two phases: ARP request, and ARP reply. ARP request is a packet sent by a user's device to a gateway i.e. router of the LAN at the beginning of the network communication. Since MAC address is used for a destination address of a packet in LAN communication, the device cannnot communicate with the Internet, or even gateway, without the MAC address of the gateway. In order to acquire a MAC address of a gateway, ARP request packets, which includes source MAC address information, are sent to the gateway's IP address. After the gateway get the packet from the device, ARP reply packets are sent by the gateway to the source device on the basis of the source MAC address included in ARP request packets, which can tell the gateway's MAC address by including it as a source MAC address. Thus, if the user's device has same MAC address with that of the LAP on the same path to the gateway, it cannnot acquire the ARP reply because the LAP on the way back to the source of request, i.e. the user's device, can receive both packets which are sent to the two devices which have same MAC addresses. Although, in non attack scenario, a user's device can receive ARP replys no matter which MAC address it has acquired at the first procedure because there exists no several APs on the same path in the communication range. On the other hand, in attack scenario, since one of the MAC addresses acquired at the collection phase is same address with LAP on the path, it cannot acquire ARP replys in the case it is set to the MAC address at the last phase. By searching that MAC address in the communication range, our scheme can detect a RAP in the LAN.

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.