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 device's features such as Received Signal Strength Indication (RSSI) and clock skew which cannot be spoofed by an adversary unlike MAC address. 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. [**?**] utilize the RSSI as the feature for whitelist which is a measurement hard to forge arbitrarily and highly correlated to the transmitter's location and power. An AP which has different RSSI but same MAC address from that in the whitelist shows it is a rAP with spoofed MAC address set by an adversary at different location. However, it is hard to detect rAP which has no big difference in location because RSSI is not as microscopic as it can tell 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 Wi-Fi hotspot to be setup costly devices. 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, such evil 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 the evil hop introduced by the rAP is added on the path, RTT in this case is longer compared with the case where a user directly connects to the lAP. Although those schemes which utilize the packet delay are useful to the attack which the adversary set rAP up on the laptop for, Jang et al. [12] reveal the fact that the computational power of the software bridging mainly accounted 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 currently because it is reasonable attack model to be setup hardware-based rAP by adversary. Thus, in this paper, we select [12] as a previous scheme and aim at proposing the user side detection which enable to detect rAP regardless on each network environment and performance of the rAP.

III. ATTACK MODEL AND PREVIOUS SCHEME

A. Attack Model

In an evil twin attack, the adversary sets up rAP using the SSID of the targeted Wi-Fi network and MAC address cloned from one of the APs in the network. As a result, a user's device receives SSID broadcast from both lAP and the rAP, but it cannot differentiate between these APs. The user's device simply assumes that both the APs are legitimate and connects with the one 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, and may 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]. Also, we assume the adversary launched hardware-based APs which cannot be detected accurately by existing schemes because 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 router to avoid channel interference each other: one for the path between lAP and rAP and the other for that betweeen rAP and user's device. Thus, from the perspective of the user's device, there exists another channel on the route different from the channel with the connected AP. Since the throughput value is dependent on the traffic on the path, the channel which is used between a lAP and rAP and not able to be seen directly from the user's device can be detected as a decline in the throughput by saturating that channel. 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 several 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.

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 because the throughput used for finding two channels out is largely dependent on various factors of the network environment such as mobility of the traffic, collisions, network topology changes, unintentional interference and so on. Since the traffic in real environment is unsteady, the previous scheme is subject to environmental changes which can lead to degrade the accuracy. Thus, it is necessary to propose the scheme which is independent of the traffic environment. Also, the previous scheme can consider incorrectly a legitimate repeater which uses distinct channels on the both sides as a rAP because of the decline in the throughput as with a rAP.

IV. PROPOSED SCHEME

In order to meet the requirements mentioned in the last section, in this paper, we propose a rAP detection scheme searching MAC address lAP has which are on the same route from a user's device to a router with Address Resolve Protocol (ARP). Our goal of our scheme is to realize the user side detection which are independent of the features which are affected by a network environment and able to tell whether it is a legitimate repeater or rAP accurately.

A. Idea

The main idea of our scheme is that there exists MAC addresses of 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 router. This is because several APs are already set to cover whole area in an appropriate arragement with several communication channel so that every user in the LAN can use Internet without overlapping each other's channel. Therefore, the more lAPs overlapping communication range with the rAP, the more likely a rAP unnecessary in theory diployed by an adversary results in channel interference. Also, an rAP needs to be set nearby the lAP so as not to cause packet delay due to a large spatial distance which can make a user quit using the Wi-Fi. Thus, it should be deployed nearby a lAP directly connected in order to avoid overlapping communication ranges and packet delay as much as possible. Meanwhile, in non attack scenario, a legitimate repeater, which looks like an rAP at first glance, is deployed at completely different location from it. A legitimate repeater has a functional role to transmit packets from a lAP associated with ISP to the area where they cannot be sent due to the spatial distance at the expense of transmission rate to some extent. As a result to introduce a repeater in the network, it is a common case that the transmission rate decline significantly because of some effects caused by it such as its distance, collisions, or the rapid increase of users saturating the traffic even if it uses two distinct channels on the both side. Thus, a rAP is detected by searching a MAC address which a rAP has on the same path which can be received by a user's device. In our detection scheme, unlike existing schemes, it does not matter whether a rAP clones MAC address of one of APs in the network because our detection scheme is based on the MAC address of the lAP on the other side of the evil twin. Thus, our scheme can detect if it tells spoofed MAC address to a user's device. We mentioned the detection schemes based on the phyisical features including MAC address with sensors introduced in a LAN by an administrator but they have shortage that they cannot distinguish which path an evil twin is set in addition to the cost issue. Thus, we realize the user side detection based on the rule of transmission that the same MAC address never exist on the same path. In order to search the MAC address of the lAP on the same path with a rAP, we focus on address resolution procedure based on ARP which is carried out when a user's device connects to a Wi-Fi network between router.

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.