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

Rogue AP (rAP) detection methods are mainly classified into two categories: fingerprint-based schemes and transmission-based schemes. Fingerprint-based schemes focus on the features of a predefined authorized AP itself such as MAC address, channel, RSSI, and clock skew. The collected features are then compared with previously known features of legitimate APs to determine the legitimacy of a given AP with the equipment setup in each Wi-Fi network. For example, in [1], [2], [3], the MAC address of an AP is compared against addresses of legitimate APs for detection. An unknown MAC address indicates that an AP is rogue. Also, other factors like RSSI [4], [5], clock skew [6], [7], or channel [8] are used to fingerprint rAPs. However, these schemes are easily enable an attacker to avoid because the features, including MAC address, are well known that they can be spoofed.

In order not to be avoided by attackers, transmission-based schemes focus on the fact that the route in the wireless local area network (WLAN) while being attacked has an extra hop to the rAP instead of the fingerprints of AP which can be easily spoofed. Nikbakhsh et al. [9] compares the routes that a packet travels in the LAN to determine whether an AP is legitimate or not. If the traceroute indicates an extra hop, which is proof of the evil twin attack. Although this scheme can work in the network topology which has no legitimate wireless range extender (RE) , the LANs have RE especially in the large area where a lot of users are such as airports. In such LANs, the scheme cause false alarms because it is not able to distinguish RE and rAP. Similarly, [10], [11] utilize the packet delay caused by the extra hop instead of the hop count in [9]. Han. et al. [10] utilize round trip time (RTT) between the user and the DNS server to determine whether an AP is legitimite or not. Similarly, Yang et al. propose the detection method that uses a discriminative feature of inter-packet arrival time. These two techniques use packet delay of traffic caused by the extra hop to the rAP as a feature for detection. However, Jang et al. [12] reveal the fact that the computational power of the software bridging mainly accounted for the packet delay. Thus, these schemes which utilize the packet delay cannot detect hardware-based rAPs having little bridging delay unlike software-based rAPs. In fact, their experiments show that the shemes is not able to distinguish the legitimate AP and the hardware-based rAP. In order to detect both types of rAPs, software-based and hardware-based, [12] focus on the channel between the legitimate AP and the rAP, which is different from that used between the user device and the rAP so as not to interfere channel each other. This scheme detect rAP finding out these two channel with the throughput of the transmission from the user device to the gateway. Although these two channels are always shown up because of the extra hop regardless of the rAP device, the throughput used for finding them out is largely dependent on the network connection. Thus, following these transmission-based schemes, it is necessary to design the scheme which enable to detect rAP regardless on each network environment such as a topology and a transmission quality.

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

II. PREVIOUS SCHEME

A. Previous Scheme

Keep your text and graphic files separate until after the text has been formatted and styled. Do not number text heads—LaTeX will do that for you.

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 Conference 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.