A Technical Survey on Approaches for Detecting Rogue Access Points

Jianwei Hu, Yetao Li, Yanpeng Cui, and Le Bu

Abstract With the popularity of wireless local area networks (WLANs) and access points (APs) which play an integral part in the wireless infrastructure coordinating wireless users and connecting them to the wired side of networks to the Internet become increasingly vulnerable and are exposed to malicious attacks. This paper focuses on rogue access points (RAPs) common attacks. The attack principle of different types of RAPs and corresponding RAPs detection methods are presented. Besides, the disadvantage and strength of these RAPs detection methods are also compared in this survey. Finally, some possible issues and future research trends are introduced.

1 Introduction

Wireless networks are rapidly spreading due to their advantages such as convenience, flexibility, mobility, scalability, and easy installation. However, the universalization of this technology also increases the security risk. RAPs are one of the most dangerous security risks.

RAP usually has the same service set identifier (SSID) with the legitimating one to cheat users. As a wireless network attack reported in 2015, attackers successfully tricked users into accessing their APs and obtain sensitive information such as bank account numbers, passwords, and photos. As the RAPs set by the attacker usually provides the network services normally, users will not feel a significant difference when accessing the RAP. In enterprise networks, attackers can also use RAPs to invade internal networks. Therefore, both wireless networks in public environments and the internal wireless networks of enterprises need security detection.

J. Hu · Y. Li (✉) · Y. Cui
Xidian University, No. 2 South Taibai Road, 710071 Xi'an, China
e-mail: liyetao2012@outlook.com

L. Bu
Imperial College, London, UK

R. Kountchev et al. (eds.), *Advances in Wireless Communications and Applications*,
Smart Innovation, Systems and Technologies 190,
https://doi.org/10.1007/978-981-15-5697-5_20

2 Taxonomy of RAPs

In the literature, RAPs are classified into three categories: twin APs, incorrectly configured APs, and unauthenticated APs.

2.1 *Twin APs*

Twin APs are RAPs that highly mimic legitimate APs [1], which is usually carried out by portable devices, small in size, and difficult to detect [2]. They exist in two types: substitution and coexistence. Substitution means that RAPs take place to legitimate APs by disconnecting users or someway else [3], and trick users into accessing them. Coexistence represents that a RAP and a legitimate AP coexist in a certain space and compete providing services at the same time.

2.2 *Incorrectly Configured APs*

APs in enterprises configured incorrectly by network employees could cause security problems [4, 5]. For example, attackers could steal network certificates by attacking mobile devices used by users to gain access to the enterprise internal network [6, 7]. Moreover, some personal APs in small shops or restaurants usually post the passwords in public or do not have a password [8].

2.3 *Unauthenticated AP*

An unauthenticated AP refers to an AP built privately on the network. Such APs are a part of the network but neither uniformly deployed nor controlled by the administrator. For example, if employees share the network privately, unauthorized users will access the network through these unauthenticated APs or sniff the network traffic [9]. Attackers can also set up unauthenticated APs deliberately, harming the network and stealing sensitive information.

3 Existing RAP Detection Approaches

Several novel approaches have been proposed by researchers. The perspective of the administrator and client detection are summarized below.

3.1 Detection from Client-Side

Use special length frame arrival time (SLFAT) to detect RAPs. It provides that the same gateway is used, as the legitimated APs [10]. SLFAT monitors the traffic sent by the target APs at the detection node and extracts the arrival time of special frames of the same length to determine whether there is a RAP forwarding data packet.

Detection of routing options based on IP headers [11]. The IP header has a record routing option function. When this function is turned on, the router address passed between the source address and the destination address will be recorded in the IP packet header of the data packet. After receiving the data packet, you can view all the passed IP addresses. If an abnormal path is found, a RAP exists. However, due to security and other considerations, many firewalls will disable or ignore packets that record routes [12], and the average number of routes on the Internet is 19–21, which is much higher than the number of 9 addresses that can be recorded [13].

Detection based on TCP connection [14]. The client connects to a nearby AP and establishes a TCP connection with the public server. When switching to a different AP with the same wireless SSID, the client sends a heartbeat request to the former public server. Only the gateway keeping, switches AP will not affect the previous TCP connection. Then, the public server can respond to heartbeat requests from the client. Conversely, a RAP exists. Meanwhile, if an attacker impersonates a public server to perform a man-in-the-middle attack, this detection will not work.

Detect duplicate association [15]. During the authentication stage, the retry bits, sequence number, and association ID (AID) of the two association responses are analyzed to verify whether a RAP exists. However, for some open-mode RAPs, this detection approach fails.

Authentication using a dedicated public server and watermark packets [16, 17]. The server continuously replies to the watermark data packet which the client sends to it before to the client. At the same time, the client detects whether other channels are transmitting the watermark. If the data packet exists, the initial AP is a RAP, and the others are legitimate. This applies when an attacker uses a legitimate access point to provide network services. However, the attacker can avoid detection by storing the watermarked data packet and disconnecting with the legitimate AP at their replay arrival time and the round-trip time.

Detect base on RAP and rogue wireless client (RWC) [14]. When the wireless client (WC) sends/receives data via RAP, the attacker's RWC and legitimate AP will also send/receive the same data, which means WC data will appear twice on the wireless channel. However, this detection method is not valid in the mode of the man-in-the-middle attack.

Detection based on the confirmation number and serial number [18]. The confirmation number and serial number in the IP packet are used as the basis for judging whether there is forwarding in the wireless network. However, this detection method requires a lot of details of the IP packet header. Encrypted wireless network services cannot be supported.

3.2 Detection from Administrator Side

Using authorization lists to detect RAPs [19]. Administrators usually form authorization lists (white lists) that contain the identity information of legitimate APs by scanning APs neighboring of their identity information and then comparing them with lists to detect RAPs' existence. Therefore, focusing on significant information and ignoring unnecessary data can do much help for reducing detection time, while the information in the data packet is not hard to alter.

Clock deviation detection approach [20]. It is a passive detection method that uses information extracted from the beacon frame to combine a clock offset with the device's inherent temperature to detect a RAP. However, this method is limited to detecting RAPs released by software.

Honeypot-based wireless intrusion detection scheme [16]. First is distinguished whether the packet comes from an authorized host, to detect the man-in-the-middle attack by the packet flow rate decreases with the increase of the packet spacing, Snort detects DoS, DNS spoofing, and then redirects malicious traffic from Snort to the KFSensor honeypot for deepening analysis. The scope of this system is a small network, and it remains to be determined whether it can be extended to a larger network.

Use dedicated hardware to interfere with channels for detection [21]. The AP2 throughput of non-adjacent channels is detected by interfering AP1 channels. If a drop occurs, AP2 may be a RAP because the wireless connection is provided by replaying the signal from AP1. However, this approach interferes with the normal user's online experience. And deploying wireless sensors across different wireless networks or gathering traffic at a centralized site is expensive and complex.

Detection based on protocol modification [22]. It mainly uses received signal strength (RSS) which changes on the wireless channel between the client and the AP. The client and the AP need to exchange challenge and response packets to complete the detection. This detection method is efficient, but modifying the protocol involves driver and firmware upgrades, which make it difficult to be popularized.

Group-aware approach [13]. It uses the spatial correlation of RSS for detection. RSS measurements collected from the population helps to provide a robust profile and minimize the impact for the inaccuracies on individual RSS values. The measurement can also dynamically match the configuration file to filter out the abnormal samples detected in real-time. The efficiency of this method depends on the number of users in the detection area.

Physical layer channel state information (CSI) [23]. A position model which is based on the edge of the landmark area, combining a large amount of crowdsensing data, is used to determine whether the detected AP is a RAP. This method uses a crowdsourcing strategy which is also depends on the number of users.

Table 1 Strengths and weaknesses of current techniques

Method	Technical requirements	Strengths	Weaknesses
Time-based detection	None	Passive detection based on the frame information	Only applicable to software release attacks
Authorization list	None	Fast detection speed	AP fingerprint spoofing can bypass the detection
Honeypot	Honeypot system	Semi-defense detection	Suitable for small network environment
Active interference	Dedicated sensor hardware	Low false positives	Affects normal network communication, high hardware deployment costs
Protocol-based	Modify agreement	High efficiency	Difficult to popularity
Automated detection	Sensor device	Passive, little infrastructure	Takes time and energy a lot

4 Conclusion

Because the simplicity of RAP creation takes a security threat to the wireless network, several detection approaches proposed by researchers. The current techniques have several weaknesses, as listed in Table 1.

Early RAP detection mainly used the authorization list to identify APs and RAPs by media access control address (MAC) and SSID. Later, multi-parameter detection was developed, and more fingerprint information of AP devices was involved in the detection work. The detection range was limited based on the time method. Later interference technology affects network user. Meanwhile, other testing methods are introduced with their strength and limitations. With the development of intelligent technology, the research of detection technology is gradually developing toward automation. Wireless intrusion detection system (WIDS) technology is the trend of future wireless security research.

References

1. Breński, K., Chołuj, M., Luckner, M.: Evil-AP-mobile man-in-the-middle threat. In: IFIP International Conference on Computer Information Systems and Industrial Management, Springer, Cham. pp. 617–627. (2017)
2. Lanze, F., Panchenko, A., Ponce-Alcaide, I., Engel, T.: Undesired relatives: protection mechanisms against the Evil Twin attack in IEEE 802.11. In: Proceedings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks, pp. 87–94 (2014)
3. Khan, W.Z., Aalsalem, M.Y., Saad, M.N.B.M., Xiang, Y.: Detection and mitigation of node replication attacks in wireless sensor networks: a survey. Int. J. Distrib. Sens. Netw. **9**(5), 149023 (2013)

4. Bartoli, A., Medvet, E., Onesti, F.: Evil Twins and WPA2 enterprise: a coming security disaster? Comput. Secur. **74**, 1–11 (2018)
5. Vanhoef, M., Piessens, F.: Key reinstallation attacks: forcing nonce reuse in WPA2. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1313–1328 (2017)
6. Bartoli, A., Medvet, E., De Lorenzo, A., Tarlao, F.: In: Secure Configuration Practices of WPA2 Enterprise Supplicants. arXiv: Cryptography and Security (2018)
7. Brenza, S., Pawlowski, A., Pöpper, C.: A practical investigation of identity theft vulnerabilities in eduroam. In: Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 1–11. (2015)
8. Ma, L., Teymorian, A. Y., Cheng, X., Song, M.: RAP: Protecting commodity Wi-Fi networks from rogue access points. In: The 4th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness and Workshops, pp. 1–7 (2007)
9. Alotaibi, B., Elleithy, K.: Rogue access point detection: taxonomy, challenges, and future directions. Wire. Pers. Commun. **90**(3), 1261–1290 (2016)
10. Lu, Q., Qu, H., Ouyang, Y., Zhang, J.: SLFAT: client-side Evil Twin detection approach based on arrival time of special length frames. Secur. Commun. Netw. **2019** (2019)
11. Nikbakhsh, S., Manaf, A. B. A., Zamani, M., Janbeglou, M.: A novel approach for rogue access point detection on the client-side. In: 2012 26th International Conference on Advanced Information Networking and Applications Workshops, pp. 684–687. IEEE. (2012)
12. Sherwood, R.: Discovering and securing shared resources on the internet (Doctoral dissertation). (2008)
13. Zhou, T., Cai, Z., Xiao, B., Chen, Y., Xu, M.: Detecting rogue AP with the crowd wisdom. In: International Conference on Distributed Computing Systems. (2017)
14. Nakhila, O., Amjad, M. F., Dondyk, E., Zou, C.C.: Gateway independent user-side Wi-Fi Evil Twin attack detection using virtual wireless clients. Comput. Secur. 41–54. (2017)
15. Agarwal, M., Biswas, S., Nandi, S.: An efficient scheme to detect Evil Twin rogue access point attack in 802.11 Wi-Fi networks. Int. J. Wire. Inf. Net. **25**(2), 130–145. (2018)
16. Agrawal, N., Tapaswi, S.: The performance analysis of honeypot based intrusion detection system for wireless network. Int. J. Wire. Inf. Netw. **24**(1), 14–26 (2017)
17. Mónica D., Ribeiro, C.: Wi-Fi Hop—mitigating the Evil Twin attack through multi-hop detection. In: Atluri, V., Diaz, C. (eds.) Computer Security—ESORICS 2011. Lecture Notes in Computer Science, vol 6879. Springer, Berlin, Heidelberg. (2011)
18. Hsu, F.H., Wang, C.S., Hsu, Y.L., Cheng, Y.P., Hsneh, Y.H.: A client-side detection mechanism for Evil Twins. Comput. Elect. Eng. **59**, 76–85 (2017)
19. Vanjale, S.B., Mane, P.B.: Multi parameter based robust and efficient rogue AP detection approach. Wire. Pers. Commun. **98**(1), 139–156 (2018)
20. Lanze, F., Panchenko, A., Braatz, B., & Engel, T.: 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, pp. 3–14 (2014)
21. Jang, R., Kang, J., Mohaisen, A., Nyang, D.: Highly-accurate rogue access point detection using intentional channel interference: poster. In: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 277–278. (2017)
22. Altaweel, A., Stoleru, R., Gu, G.: EvilDirect: a new Wi-Fi direct hijacking attack and countermeasures. In: 2017 26th International Conference on Computer Communication and Networks (ICCCN) (pp. 1–11). IEEE. (2017)
23. Wang, C., Zhu, L., Gong, L., Liu, Z., Mo, X., Yang, W., … Li, Z.: Detecting Evil-Twin attack with the crowd sensing of landmark in physical layer. In: International Conference on Algorithms and Architectures for Parallel Processing, pp. 234–248. Springer, Cham. (2018)