Computer Communications 142–143 (2019) 62–68

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

A solution to detect the existence of a malicious rogue AP

Fu-Hau Hsu [a], Yu-Liang Hsu [a], Chuan-Sheng Wang [a,b,*]

[a] Department of Computer Sciences and information Engineering, National Central University, Taiwan
[b] Information and Communication Security Lab, Chunghwa Telecom Co., Ltd., Taiwan

ARTICLE INFO

Keywords:
Wi-fi
Evil twin
Rogue access point
Wireless security
Network security

ABSTRACT

A *malicious rogue AP* works like an evil twin; however, instead of using a good twin to connect to the Internet, a malicious rogue AP uses a 3G/4G mobile network to connect to the Internet. While administrators have sufficient information to distinguish rogue APs, it is difficult for client users to know whether they are using a wireless network with malicious an AP. To solve evil twin problems at client-side, many solutions make their detection based on some time metrics or evil twin features. However, time metrics may be influenced by pre-fetching, network topology, traffic volume, or network types. And the evil twin features such as packet forwarding cannot distinguish malicious rogue APs because they behave just like a legitimate AP. To solve above problem, this paper proposes an active user-side solution, called Wi-Fi Malicious Rogue AP Finder (RAF). RAF can be installed in any computer or laptop without any special requirement. RAF detect the existence of a malicious rogue AP based on different reverse `traceroute` information collected by a remote server. To the best of our knowledge, RAF is the first one client-side solution which could detect malicious rogue APs based on path information but not time metrics.

1. Introduction

Wireless networks have been widely used in homes, offices, restaurants, coffee-shops, airports, train stations and hotels. Everyone can access the Internet at any place and at any time by using laptops or various mobile devices, such as smartphones, PDAs, and tablets. As a result, IEEE 802.11 wireless networks (WLAN) have become a popular facility for many people's everyday life. There are many public spaces, such as cafés, restaurants, hotels, airports, railway stations, and so on, provide hotspot service in the world. So people can connect to the Internet easily. ABI research [1] shows that there were about 7.8 million hotspots in the end of 2015. The large user pool of Wi-Fi makes their users attractive targets of attackers. Attackers have developed various attacks aiming at wireless networks and their users. Among these attacks, evil twins [2–5] are one of the most notorious attacks.

A *rogue access point* is a wireless access point that has been installed in a network without permissions from related wireless network administrator. Additionally, an *evil twin* is a kind of rogue access points. It disguises as a legal AP (*good twin*) by setting its SSID with the same value as a legal AP. Through some off-the-shelf software [6,7], an attacker can easily transform a laptop into an evil twin. According to [8], it is easy for attackers to launch man-in-the-middle attacks or phishing attacks using an evil twin. Attackers can use an evil twin to steal sensitive information, such as passwords, web sessions, credit card and various information, from users who use the evil twin to connect to the Internet. By this kind of attacks, a malicious user can get a lot of sensitive data.

However, as the cost of 3G/4G telecommunication networks decreases, it is easy to set up an evil twin using a smartphone which can use a 3G/4G mobile network to connect the Internet directly. Hence, instead of using a laptop to create an evil twin, an attacker can use a smartphone to create an evil twin and use a 3G/4G network to connect to the Internet. We call this kind of rogue APs *malicious rogue APs*, shown in Fig. 1. Even though malicious rogue APs are mutants of evil twins, to the best of our knowledge, many proposed solutions to evil twins cannot work properly for malicious rogue APs because of complicated network situation or lack of packet information.

To solve the above problems, this paper proposes an active user-side solution called Malicious Rogue AP Finder (RAF). RAF can be installed in any computer or notebook without any special requirement. As an active user-side solution, RAF must connect to the Internet first. RAF makes its detection based on the *IP packet transmission path*. According to our finding, at the same location, the edge router that a 3G/4G mobile network uses to connect to the Internet is different from the edge router that a Wi-Fi AP of a local wireless network uses to connect to the Internet. Hence, compared with using a Wi-Fi network to connect to the Internet to reach a remote server, if a user uses a 3G/4G mobile network to connect to the Internet to reach the server at the same location as the wireless network, the IP packet transmission path to the server is different. Hence, RAF only needs to know the IP packet

* Corresponding author at: Department of Computer Sciences and information Engineering, National Central University, Taiwan.
E-mail address: luckytft@gmail.com (C.-S. Wang).

https://doi.org/10.1016/j.comcom.2019.03.013
Received 30 June 2018; Received in revised form 14 January 2019; Accepted 28 March 2019
Available online 4 May 2019

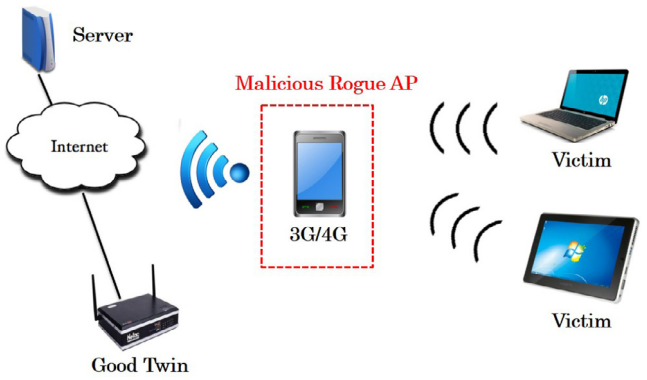

Fig. 1. Setup of a malicious rogue AP.

transmission paths between a specific server and a client host to detect the existence of a malicious rogue AP. During RAF's observation phase, RAF gets IP packet transmission path information from a remote server by HTTPS protocol. If APs with the same SSID using different paths to transmit TCP/IP packets to the same remote server, RAF can accurately detect the existence of a malicious rogue AP by only few network packets.

RAF also has the following properties:

(1) As a user-side solution, RAF does not require any information, lists of legal APs/IPs, training data, or assistance from WLAN administrators. RAF can protect a Wi-Fi user any time at any place.
(2) As an active solution with support of a remote server, a malicious rogue AP cannot hide the IP packet transmission path information when it is under investigation.
(3) RAF can find the difference of IP packet transmission paths between legal APs and malicious rogue APs.

The rest of the paper is organized as follows. Section 2 discusses rogue AP and evil twin related work. Section 3 describes the principle, algorithm, and proof of algorithm of RAF. Section 4 discusses various experimental results to evaluate the effectiveness and efficiency of RAF and some security issues about RAF. Section 5 gives the conclusion.

2. Related work

As attack manipulations against wireless environment appear and evolve rapidly, detection schemes protecting wireless user are also developing accordingly. We can classify these solutions into three categories, administrator side detection, user side detection and physical properties of radio detection.

2.1. Administrator side detection

The protocol which use to transmit network packets is different from wired communication and wireless communication. Base on this property, different protocols has different transmission behaviors and transmit time. [9–21] utilize above properties to deduce whether the related client comes from a wireless network environment or not. By analyze the inter-packet arrival times, Beyah et al. [9] use the property that inter-packet arrival times of wireless traffic is more random than those of wired traffic to detect rogue APs. Shetty et al. [11] proposed an automated classifier which uses the median of the time metric to detect rogue AP. Watkins et al. [13] noticed that the Round Trip Time (RTT) for the packet transmit from the wired link is less than the data transmit in the wireless links. Hence, they take RTT as the time metric to distinguish legal wireless APs and unauthorized wireless APs. To increase the accuracy of the detections, Mano et al. [14] utilize packet payload slicing technique and used local RTT to differentiate wired traffic and wireless traffic.

Wei et al. [12,22] collected the inter-arrival time of a TCP ACK-pair to detect the wireless hosts. Moreover, Wei et al. [10] utilized the inter-arrival time of TCP ACK-pairs, 802.11 protocol and wireless channels, and then used sequential analysis to differentiate wireless and wired traffic, which can use to detected the rogue APs. Venkataraman and Beyah [15] found the jump signature was created by the CSMA/CA of the DCF and the rate adaptation mechanism in the 802.11 MAC to filter out wired traffic and wireless traffic. Ma et al. [21] use a hybrid framework which combined both wireless surveillance and gateway side traffic analyzer to detect rogue APs. They utilized the inter-packet spacing time metric. Unlike the above work to distinguish wired traffic and wireless traffic, Kao et al. [23] utilized client-side bottleneck bandwidth to detect rogue APs. Because the client-side bottleneck bandwidth is related to the client connection bandwidth and can be differentiated the wired traffic and wireless traffic.

Most of the administrator side solutions need to analyze the packets passing through the gateway. These solutions are mainly design for the system administrators, not for the normal users. So when the packet analyze of an organization is usually not provide for the normal users due to security concern. If they provide the network analysis to a unknown third party, it is very perilous to an organization. The trace data may contain private, confidential, or important information. Moreover, most of the solutions need an authorized list of APs or IPs data which is not available for a normal user too. Besides, most of these solution need to distinguish wired traffic and wireless traffic first. However, the rogue AP usually hides behind a legal AP, and most of these solution is not directly to detect a malicious AP. Finally, most of this solutions use time metric to differentiate wired traffic and wireless traffic, and these time metrics may be influenced by various factors such as network topology, network type, network speed and traffic volume, that successively may influence the detection accuracy.

2.2. User side detection

When connecting to an AP, users can actively send exploring packets, measure various time metrics, and use different type of examines that the explore packets are transmitted through one or two APs to detect rogue AP. [8,19,21,24] are this kind of detection method. Nicholson et al. [25] proposed Virgil to discover and select APs automatically. Virgil will associate to each AP and chose the suitable APs based on the bandwidth estimation that connect to a set of reference servers to compute the round-trip-time. Han et al. [19] also utilizes the round trip time information between a DNS server and a client to decide whether an AP is a rogue AP without any assistance from the wireless administrator. When doing the detection, the related APs will receive DNS queries from the same client to nearby DNS servers. The above mechanism may be used by a rogue AP to examine whether someone is inspecting it. Yan et al. [8] proposed ETSniffer which is a user-side rogue AP detection system. It uses the Inter-packet Arrival Time (IAT) as the detection statistic. ETSniffer uses two algorithms Trained Mean Matching (TMM) and Hop Differentiating Technique (HDT) to distinguish one hop wireless channel from two hop wireless channels for different environments. ETSniffer does not need any support form Internet Service Provider (ISP), network administrator or any authorized APs/IPs list; hence, ETSniffer is appropriate for normal users. In order to get the accurate IAT information, ETSniffer needs to send network packets with special format based on the policy which will immediate return ACK. However, the malicious attacker can detect the special format packets and pre-fetching web content to bypass the ETSniffer detection.

The client side detection solutions does not need any authorized APs/IPs white list or black list, assistance from the network administrator, or network trace information from the gateway; hence, they are very appropriate for normal users who need to connect to a hotspot at

any time. However, the user side detection also faces some challenges which need to be overcome to make them widely adopted. First, active client side detection usually send exploring packets which usually have special forms. If the attackers know this kind of detection, they can use various method to bypass the detection. Second, client side detection usually utilizes various time metrics related to exploring packets, such as round trip time or inter-packet arrival time to distinguish the evil twins and legitimate APs. Nevertheless, different network topology, traffic volume, or device network capability changes, the time metrics may not work appropriately with the same number of exploring packets. In consequence, for a normal user who needs to travel different places at different time, the detection method may not always function well.

One of the possible solutions could be indoor localization [26,27], these solutions could fingerprint a Wi-Fi network and distinguish access points. The information from indoor positioning could be helpful in rogue AP detecting.

2.3. Physical properties of radio detection

Wireless access points use 802.11 protocol to communicate with other clients. Sensor APs [28,29], sensors [30,31] and mobile devices have a wireless interface [32,33] to scan the spectrum between 2.4 GHz and 5 GHz to collect various information from the wireless environment. Then information, such as SSID, BSSID, channel, MAC address, RSS values [34], radio frequency variations [35], and clock skews [36], is extracted as fingerprints of related APs. Last the fingerprints is compared with an authorized list to filter out the malicious rogue APs.

Nevertheless, the solutions which need the time and human power to operate the extra device will increase the maintenance cost. Without continuously monitoring a wireless environment, the above solutions may not provide complete protection for the wireless users. Moreover these solutions may take a legal neighbor AP as a rogue AP. Furthermore, an attacker can install a malicious AP at any time and remove the malicious AP quickly.

In order to overcome these problems, some hybrid solutions [9,16,37] were proposed. For example, Bahl et al. [37] proposed Dense Array of Inexpensive Radios (DAIR) framework. It turns existing desktops into wireless sniffers to decrease deployment cost and increase efficiency instead of sniffing wireless traffic. [9,16] observe wired network traffic to avoid misjudging a legal nearby AP as a rogue AP. If an internal sensor observes the same network packets transmit from the wired traffic and wireless traffic, the system can be sure that the suspect AP is an rogue AP by sending packets to the Internet through the suspect AP.

3. Principle and detection algorithm

In a malicious rogue AP attack scenario, a malicious rogue AP transmits IP packets between it and a remote server through a 3G/4G network. These IP packets belong to a user who is fooled by believe that the malicious rogue AP is a legal AP in his wireless network. Hence, these IP packets transmitted through the 3G/4G network are not visible to traditional IP packet sniffing tools, such as Wireshark. As a result, user-side solutions may not be able to capture the wireless packets for analysis. Thus, to the best of our knowledge, there is no efficient way to detect malicious rogue APs with a limited information of a wireless network. Hence, this paper proposes a malicious rogue AP detection mechanism, called RAF. With the help of a remote server, RAF can detect malicious rogue APs through IP packet transmission paths.

3.1. Thread model

In this paper, the thread model considers the situation that an adversary wants to launch an evil twin attack in a Wi-Fi network created by a hotspot. The adversary uses a smartphone to set up an evil twin. Then the smartphone uses a 3G/4G mobile network to connect to the Internet directly. The adversary has complete information about the Wi-Fi network, such as the APs and SSIDs used in the Wi-Fi network, and even the victims' mobile devices. The adversary could also launch network attacks to increase network load and packet delay. Finally, the adversary knows the full implementation details of the defense methods used by the victims.

3.2. IP Packet transmission path

In the Internet, an IP packet is delivered from its source host to its destination host through a series of routers. The serious of routers consist of the IP packet transmission path of the IP packet. 3G/4G mobile networks and Wi-Fi networks use different edge routers to connect to the Internet. Hence, if a host uses a 3G/4G network to access a remote server, the IP transmission path of its IP packets should be different from the IP transmission path utilized by the IP packets handling by a Wi-Fi network. `Traceroute` is a tool to find the route path from a source host to a destination host. It sends a series of probe packets to the destination host. Each time when a new probe packet is created, the time-to-live (TTL) field of its IP header is increased by one. The TTL values starts from one to thirty in Windows operation system. When a probe packet is transmitted in the Internet, its TTL value is decreased by 1 each time when a router receives it. If the TTL value becomes zero, the router drops the packet and sends an ICMP Time Exceeded error message with the IP of the router to the client. Hence from the series of ICMP Time Exceeded error packets, a source host can create the IP packet transmission path of its IP packets to the destination host.

3.3. Design principle and RAF algorithm

RAF detects the existence of malicious rogue APs based on the IP packet transmission path information. As mentioned in the above subsection, in a wireless network, a 3G/4G device, such as a smartphone, and a Wi-Fi access point uses different edge routers to connect to the Internet. Therefore, RAF chooses different devices to connect to the Internet and observing related IP packet transmission paths. Then RAF compares the paths related to different wireless devices to see whether they are the same to determine whether there exists a malicious rogue AP. If the paths are different, for example one connects to the Internet via a Wi-Fi network but another one connects via a 3G/4G mobile network, it means there exists a malicious rogue AP in the wireless network. To identify the malicious rogue AP in the wireless network, currently we have to examine the paths manually.

Our preliminary survey shows that ISPs tend to use fixed routers as the edge routers of 3G/4G mobile networks. Utilize the database from [38], which collected edge router IP addresses and mobile network IP addresses to detect fake GPS, it is possible to identify paths that belong to 3G/4G mobile networks or Wi-Fi networks. Note that this step is programmable and could be automatic, however we leave this as our future work.

There is still a challenge that IP packet transmission path information cannot be collected by RAF. If the information is collected by RAF and RAF connects to the Internet through a malicious rogue AP, then every exploration packet will pass through the malicious rogue AP which can modify the result and let RAF receive a forge path. Finally we use reverse `traceroute` mechanism which is proposed by Ethan et al. [39] to solve this problem. RAF connects a remote server which provides reverse `traceroute` to get IP packet transmission path information. Currently, we use HTTPS to transmit the path information to RAF. Fig. 2 shows RAF detection mechanism.

What follows is the detection algorithm of RAF.

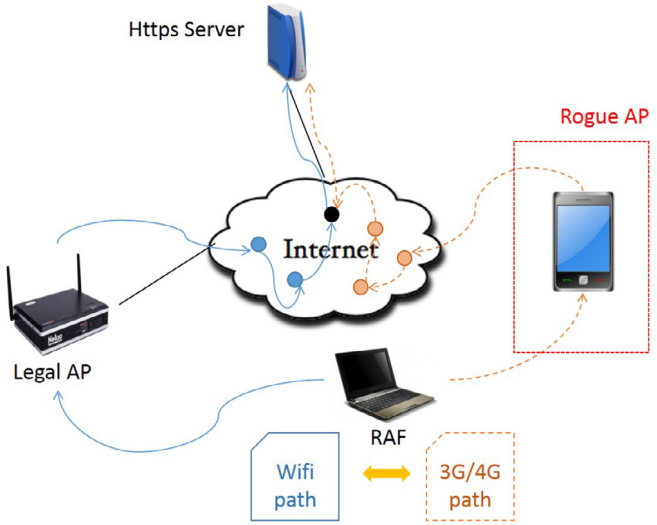

Fig. 2. The RAF detection mechanism.

(1) RAF checks whether there exist two APs with the same SSID. If not, there is no malicious rogue AP. The detection finishes. Otherwise, The WLAN may contain a rogue AP. Go to step 2 and assume, AP_1 with MAC address MAC_{AP_1} and AP_2 with MAC address MAC_{AP_2} have the same SSID.

(2) RAF connects to a specific web server which provides reverse `traceroute` service by using AP_1 and AP_2 respectively, then RAF sends a HTTPs connection request to the server. The server returns two IP packet transmission paths to RAF, then go to step 3.

(3) RAF compares the two paths obtained in Step 2. If the paths are different, one of the AP is rogue AP. Otherwise both APs are not rogue APs. The detection finishes.

3.4. System structure and components

Fig. 3 shows the system structure and components of RAF which is implemented as an application; hence, RAF can be easily installed in any computer. RAF has two major components, *path access component* and *path comparison component*. The path access component searches for Wi-Fi APs in a wireless network that have the same SSID first. Then it associates with each of these APs to access the reverse `traceroute` service provided by a remote server and obtain the IP packet transmission path related to each of the APs. If there are more than two APs with the same SSID, the IP packet transmission paths obtained by the path access component are compared with each other to see whether they are all the same. If these paths are not all the same; then it shows that there exists a malicious rogue AP in the wireless network; otherwise, there is no malicious rogue AP in the wireless network.

4. Evaluation

In this section, we utilize various experiments to evaluate the detection accuracy and efficiency of RAF. We deploy a web server at a university to provide reverse `traceroute` service that can find the IP packet transmission path from the server to a host. The reverse `traceroute` server had a 2.4 GHz Intel Core 2 Duo CPU and 4GB memory, and running Microsoft Windows 7 32-bit operating system. The server uses HTTPS protocol to transmit path information to its clients to avoid the path information being modified by a malicious rogue AP. The HTTPS connection is a common services on the Internet, and the attacker is difficult to decrypt HTTPS packets.

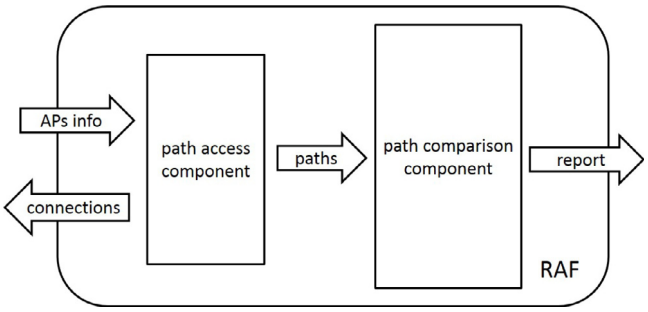

Fig. 3. System structure and components of RAF.

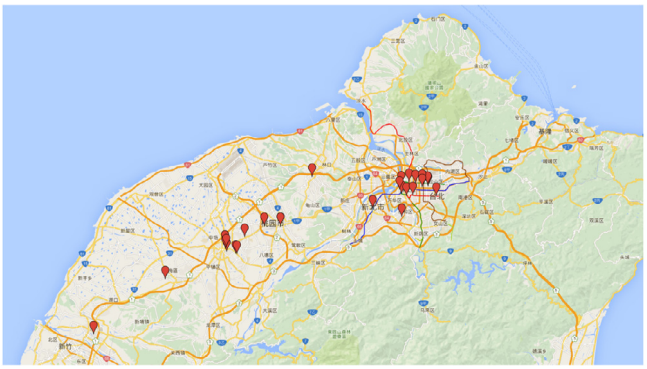

Fig. 4. The locations of 30 hotspots used in our experiments.

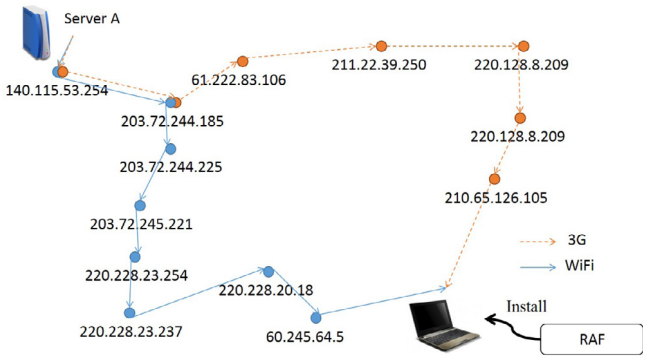

Fig. 5. A IP packet transmission path between a reverse `traceroute` server and a host installed RAF.

4.1. Reverse `traceroute` services

`Traceroute` is a widely used diagnostic tool to find the path information. By default, it sends a sequence of UDP packets in Linux operation system. ICMP or TCP packets also can be used in Linux. Windows operation system sends ICMP echo requests. As mentioned in the previous subsection, RAF use reverse `traceroute` service and HTTPs to correctly get the IP packet transmission path information. In fact, some ISPs or governmental research centers provide reverse `traceroute` service to the public. The reverse `traceroute` server list are posted on Stanford Linear Accelerator Center website.

4.2. Accuracy of RAF

We selected 30 places which provide free wireless hotspots to evaluate the detection time and detection accuracy of RAF. Fig. 4 shows the geography locations of these 30 hotspots. These places are located in some train stations, Mass Rapid Transit stations (MRT), libraries,

Table 1
Detection time (seconds) that three different reverse `traceroute` servers spend to find the IP packet transmission paths between them and our test RAF client when the RAF client was associated with a local Wi-Fi AP or local 3G AP at 30 different places.

Location	Server A (Wi-Fi)	Server A (3G)	Server B (Wi-Fi)	Server B (3G)	Server C (Wi-Fi)	Server C (3G)
1	342	342	11	2	35	25
2	6	330	4	2	26	26
3	6	342	2	2	1	25
4	6	342	5	4	26	28
5	342	342	6	4	28	26
6	20	342	14	7	26	26
7	305	342	9	4	32	26
8	6	341	3	2	28	27
9	342	342	6	3	2	25
10	342	342	6	2	30	26
11	342	342	6	2	30	25
12	342	342	6	3	30	25
13	6	342	3	3	1	26
14	6	342	5	6	27	28
15	6	342	5	4	27	26
16	7	342	9	2	27	29
17	342	342	6	9	34	25
18	342	342	2	2	25	25
19	342	342	6	3	36	25
20	342	342	6	4	28	25
21	342	342	8	3	44	25
22	342	342	9	4	32	25
23	342	342	17	2	30	26
24	342	342	4	2	25	25
25	342	342	3	4	26	25
26	8	342	4	2	28	29
27	342	342	6	2	52	25
28	342	342	3	3	30	25
29	342	342	3	3	26	26
30	342	342	9	3	34	25
Average	229.3333333	341.5666667	6.2	3.266666667	27.53333333	25.83333333

coffee shops, restaurants, and department stores. The maximum length of paths used to connect to our test reverse `traceroute` servers is 30 hops. At each hotspot, our RAF client was associated with a local Wi-Fi AP or a local 3G AP to connect to the Internet and then three reverse servers were used in our experiments. Server A is deployed at a university which uses HTTPS service, server B and Server C are selected from the reverse `traceroute` server list located in Taiwan. Fig. 5 shows an IP packet transmission path between a reverse `traceroute` server and a host that has installed RAF.

Table 1 shows the experimental results that at each of these 30 locations, the IP packet transmission path between a RAF host and a reverse `traceroute` server through a Wi-Fi AP is different from the path through a 3G AP. It is worth noting that detecting a 3G AP could be faster than a Wi-Fi AP, because of the reverse `traceroute` is launched by a server. As a result, RAF can accurately detect whether a wireless network has a malicious rogue AP.

4.3. Comparisons with other work

Traditional time metrics-based solutions can detect classic rouge APs; however, an attacker may change the response time to interfere with the detection accuracy of a time metrics-based solution. The network traffic also influences the detection accuracy of time metrics-based solutions. Han et al. [40] using time metrics algorithm to detect rouge AP. They found that under heavy traffic conditions, the detection rate is reduced from 100% to 60%. Hence, attackers can use heavy traffic to reduce the detection accuracy of this solution. Kuo et al. [41] also show that time-based methods could be affected by several factors, such as the RSSI, data traffic load, Internet speed, DNS response time, and so on. In our threat model, we assume that an attacker can launch attacks to interfere with the network environment, thus bypass time metric-based solutions.

Unlike time metric-based solutions, RAF does not send probe packets. RAF collects IP packet transmission path information through a remote HTTPs server. An attacker on a local network cannot interfere with the detection result of RAF. Therefore, RAF is not affected by the above network traffic and time delay issues. We compare RAF with a traditional time metrics-based method [41]. Table 2 shows the result.

Table 2
Comparisons between RAF and a time metrics-based solution.

	RAF	Kuo et al. [41]
Detection time	A few seconds to a few minutes	About one minute
Affected by network traffic	Little	Great
Difficulty to bypass detection	Hard	Easy

4.4. Discussion

In this section, we discuss various problems that RAF may encounter. First, RAF detects a malicious rogue AP based on the IP packet transmission path information. Hence, at a location, if a 3G/4G mobile network and a wireless network use the same edge router to connect to the Internet, RAF cannot detect the existence of a malicious rogue AP. Second, if an attacker blocks the reverse `traceroute` server connection, RAF cannot detect malicious rogue APs. However this behavior can be detected by RAF users.

4.5. Future work

Currently RAF could detect the existence of a malicious rogue AP. However, to identify the malicious rogue AP in a wireless network, currently we need to examine the IP packet transmission path information manually.

According to our survey, we found that 3G/4G mobile networks always use the same edge routers to connect to the Internet. Therefore, we can compare the edge router of a suspicious trace path with these IP addresses used by the edge routers of 3G/4G mobile networks to

confirm whether a TCP/IP connection is connected to the Internet through a legal Wi-Fi AP or a malicious rouge AP. We plan to create a database that contains information about mobile network IP address information, including the IP addresses of 3G/4G ISP edge routers. By utilizing the database, RAF would be able to confirm whether an AP is a malicious rogue AP.

After the RAF confirms the presence of a rouge AP, we currently need to manually perform the above operations to identify it. The rouge AP can also be located using the existing method [42,43]. In fact, users only need to report suspicious APs to the network administrator.

5. Conclusion

In this paper, we propose an active user-side malicious rogue AP finder, RAF, which can prevent a wireless user from using malicious rogue APs to connect to the Internet, which in turn reduces a lot of security threats. RAF is a light weight solution; hence, a user can use it whenever he needs at any place without the assistance from the administrators of a WLAN, network trace of the related network, or a legal AP/IP list. Besides, RAF utilize remote servers to make its detection; hence, malicious rogue APs cannot detect its existence, let alone taking any step to bypass its detection. Experimental results show that RAF can accurately detect malicious rogue APs through using only few wireless packets.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] ABI Research, Growing Demand for Mobility will Boost Global Wi-Fi Hotspots to Reach 6.3 Million in 2013, available from: http://blog.yam.com/urlawyer/article/73520365.

[2] CNN, Evil twin threat to Wi-Fi users, available from: http://edition.cnn.com/2005/TECH/internet/01/20/evil.twins/.

[3] Erin Biba, Does Your Wi-Fi Hotspot Have an Evil Twin, available from: http://www.pcworld.com/article/120054/article.html.

[4] Chris Hails, Smartphones and Public Wi-Fi Evil Twin Attacks, available from: http://blog.netsafe.org.nz/2011/04/28/smartphones-and-public-wi-fi-evil-twin-attacks/.

[5] Scams Inc, Evil Twin Attacks: Scamming Wireless Network Users, available from: http://scamsinc.com/2012/02/13/evil-twin-attacks-scamming-wireless-network-users/.

[6] Shmoo, Airsnarf - A rogue AP setup utility, available from: http://airsnarf.shmoo.com/.

[7] Hack WiFi, Rogue AP Dangers – Wireless Evil Twin Attack Techniques, available from: http://www.freehowtohackwifi.com/advanced-wifi-hacks/rogue-ap/.

[8] C. Yang, Y. Song, G. Gu, Active user-side evil twin access point detection using statistical techniques, IEEE Trans. Inf. Forensics Secur. 7 (5) (2012) 1638–1651, [Online]. Available: http://ieeexplore.ieee.org/document/6236067/.

[9] R.A. Beyah, S. Kangude, G. Yu, B. Strickland, J.A. Copeland, Rogue access point detection using temporal traffic characteristics, in: GLOBECOM, IEEE, 2004, pp. 2271–2275, [Online]. Available: http://ieeexplore.ieee.org/document/1378413/.

[10] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, D. Towsley, Passive online rogue access point detection using sequential hypothesis testing with tcp ack-pairs, in: Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement, IMC '07, ACM, New York, NY, USA, 2007, pp. 365–378, [Online]. Available: http://doi.acm.org/10.1145/1298306.1298357.

[11] S. Shetty, M. Song, L. Ma, Rogue access point detection by analyzing network traffic characteristics, in: Military Communications Conference, 2007 MILCOM 2007, IEEE, 2007, pp. 1–7.

[12] W. Wei, S. Jaiswal, J. Kurose, D. Towsley, Identifying 802.11 traffic from passive measurements using iterative bayesian inference, in: Proc. IEEE INFOCOM, 2006.

[13] L. Watkins, R.A. Beyah, C.L. Corbett, A passive approach to rogue access point detection, in: GLOBECOM, IEEE, 2007, pp. 355–360, [Online]. Available: http://ieeexplore.ieee.org/document/4410983/.

[14] C.D. Mano, A. Blaich, Q. Liao, Y. Jiang, D.A. Cieslak, D. Salyers, A. Striegel, Ripps: Rogue identifying packet payload slicer detecting unauthorized wireless hosts through network traffic conditioning, ACM Trans. Inf. Syst. Secur. 11 (2) (2008) [Online]. Available: http://www.cs.odu.edu/~nadeem/classes/cs795-WNS-S13/papers/enter-016.pdf.

[15] A. Venkataraman, R. Beyah, Rogue access point detection using innate characteristics of the 802.11 mac, in: Y. Chen, T. Dimitriou, J. Zhou (Eds.), SecureComm, in: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 19, Springer, 2009, pp. 394–416, [Online]. Available: http://cap.ece.gatech.edu/papers/securecomm2009.pdf.

[16] H. Yin, G. Chen, J. Wang, Detecting protected layer-3 rogue aps, in: BROADNETS, IEEE, 2007, pp. 449–458, [Online]. Available: http://ieeexplore.ieee.org/document/4550468/.

[17] W. Wei, B. Wang, C. Zhang, J. Kurose, D. Towsley, Classification of access network types: Ethernet, wireless lan, adsl, cable modem or dialup, Comput. Netw. (2008) 3205–3217.

[18] V. Baiamonte, K. Papagiannaki, G. Iannaccone, Detecting, Detecting 802.11 wireless hosts from remote passive observations, in: I.F. Akyildiz, R. Sivakumar, E. Ekici, J.C. de Oliveira, J. McNair (Eds.), Networking, in: Lecture Notes in Computer Science, vol. 4479, Springer, 2007, pp. 356–367, [Online]. Available: https://link.springer.com/content/pdf/10.1007/978-3-540-72606-7_31.pdf.

[19] H. Han, B. Sheng, C.C. Tan, Q. Li, S. Lu, A timing-based scheme for rogue ap detection, IEEE Trans. Parallel Distrib. Syst. 22 (11) (2011) 1912–1925, [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6007016.

[20] C. Corbett, R. Beyah, J. Copeland, A passive approach to wireless nic identification, in: ICC, IEEE, 2006, pp. 2329–2334, [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4024512.

[21] L. Ma, A.Y. Teymorian, X. Cheng, A hybrid rogue access point protection framework for commodity wi-fi networks, in: Proc. IEEE INFOCOM, 2008.

[22] W. Wei, S. Jaiswal, J. Kurose, D. Towsley, K. Suh, B. Wang, Identifying 802.11 traffic from passive measurements using iterative bayesian inference, IEEE/ACM Trans. Netw. 20 (2) (2012) 325–338, [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5942183.

[23] K.-F. Kao, I.-E. Liao, Y.-C. Li, Detecting rogue access points using client-side bottleneck bandwidth analysis, Comput. Secur. 28 (3–4) (2009) 144–152, [Online]. Available: https://dl.acm.org/citation.cfm?id=2639897.

[24] F.-H. Hsu, C.-S. Wang, Y.-L. Hsu, Y.-P. Cheng, Y.-H. Hsneh, A client-side detection mechanism for evil twins, Comput. Electr. Eng. (2015) [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0045790615003559.

[25] A.J. Nicholson, Y. Chawathe, M.Y. Chen, B.D. Noble, D. Wetherall, Improved access point selection, in: Proceedings of the 4th International Conference on Mobile Systems, Applications and Services, MobiSys '06, ACM, New York, NY, USA, 2006, pp. 233–245, [Online]. Available: http://doi.acm.org/10.1145/1134680.1134705.

[26] S. Jeon, J.-P. Jeong, Y.-J. Suh, C. Yu, D. Han, Selective ap probing for indoor positioning in a large and ap-dense environment, J. Netw. Comput. Appl. 99 (2017) 47–57, [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517303119.

[27] T. Kulshrestha, D. Saxena, R. Niyogi, V. Raychoudhury, M. Misra, Smartits: Smartphone-based identification and tracking using seamless indoor-outdoor localization, J. Netw. Comput. Appl. 98 (2017) 97–113, [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517302965.

[28] Motorola Solutions, TIRED OF ROGUES? Solutions for Detecting and Eliminating Rogue Wireless Networks White paper, available from: http://www.motorolasolutions.com/web/Business/Products/Software%20and%20Applications/Network%20Design%20Software/AirDefense_Security_Compliance/_documents/Static_files/Tired_of_Rogues.pdf.

[29] Airwave, The Airwave Project, available from: http://www.airwave.com.

[30] Cisco, Cisco wireless lan solution engine (wlse) white paper, available from: http://www.cisco.com/c/en/us/products/cloud-systems-management/ciscoworks-wireless-lan-solution-engine-wlse/index.html.

[31] Proxim, Rogue access point detection: Automatically detect and manage wireless threats to your network white paper, available from: http://www.proxim.com.

[32] Netstumbler, The Netstumbler Project, available from: http://www.netstumbler.com.

[33] AirMagnet, The AirMagnet Project, available from: http://www.airmagnet.com/.

[34] Y. Sheng, K. Tan, G. Chen, D. Kotz, A. Campbell, Detecting 802.11 mac layer spoofing using received signal strength, in: INFOCOM, IEEE, 2008, pp. 1768–1776, [Online]. Available: http://ieeexplore.ieee.org/abstract/document/4509834/.

[35] V. Brik, S. Banerjee, M. Gruteser, S. Oh, Wireless device identification with radiometric signatures, in: J.J. Garcia-Luna-Aceves, R. Sivakumar, P. Steenkiste (Eds.), MOBICOM, ACM, 2008, pp. 116–127, [Online]. Available: https://dl.acm.org/citation.cfm?id=1409959.

[36] S. Jana, S.K. Kasera, On fast and accurate detection of unauthorized wireless access points using clock skews, IEEE Trans. Mob. Comput. 9 (3) (2010) 449–462, [Online]. Available: http://ieeexplore.ieee.org/abstract/document/5210105/.

[37] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, B. Zill, Enhancing the security of corporate wi-fi networks using dair, in: Proceedings of the 4th International Conference on Mobile Systems, Applications and Services, MobiSys '06, ACM, New York, NY, USA, 2006, pp. 1–14, [Online]. Available: http://doi.acm.org/10.1145/1134680.1134682.

[38] Y.-H. Chang, Y.-L. Hwang, C.-W. Ou, C.-L. Hu, F.-H. Hsu, Fake gps defender: A server-side solution to detect fake gps, in: The Third International Conference on Advances in Computation, Communications and Services, 2018.

[39] E. Katz-Bassett, H.V. Madhyastha, V.K. Adhikari, C. Scott, J. Sherry, P. Van Wesep, T.E. Anderson, A. Krishnamurthy, Reverse traceroute, in: NSDI, vol. 10, 2010, pp. 219–234.
[40] H. Han, B. Sheng, C.C. Tan, Q. Li, S. Lu, A timing-based scheme for rogue ap detection, IEEE Trans. Parallel Distrib. Syst. 22 (11) (2011) 1912–1925.
[41] E. Kuo, M. Chang, D. Kao, User-side evil twin attack detection using time-delay statistics of tcp connection termination, in: 2018 20th International Conference on Advanced Communication Technology, ICACT, 2018, pp. 1–1.
[42] Z. Zhang, X. Zhou, W. Zhang, Y. Zhang, G. Wang, B.Y. Zhao, H. Zheng, I am the antenna: Accurate outdoor ap location using smartphones, in: Proceedings of the 17th Annual International Conference on Mobile Computing and Networking, MobiCom '11, ACM, New York, NY, USA, 2011, pp. 109–120, [Online]. Available: http://doi.acm.org/10.1145/2030613.2030626.
[43] C. Wang, X. Zheng, Y. Chen, J. Yang, Locating rogue access point using fine-grained channel information, IEEE Trans. Mob. Comput. 16 (9) (2017) 2560–2573.

Fu-Hau Hsu received his Ph.D. degree in the department of computer science from Stony Brook University, New York, USA in 2004. He is a professor at the Department of Computer Science and Information Engineering of National Central University. His research focuses on system security, web security, network security, and cellular phone security. He is affiliated with the Advanced Defense Lab and the Wireless Network and Multimedia Lab.

Yu-Liangu Hsu is a Ph.D. student in the Department of Computer Science and Information Engineering of National Central University. He received the M.S. degree in computer information science from Soochow University, Taipei, Taiwan, in 2007, and the B.S. degree in computer information science from Soochow University, in 2001. His research interests include network security, wireless security, and system security.

Chuan-Sheng Wang is a Ph.D. student in the Department of Computer Science and Information Engineering of National Central University. He received his M.S. degree in computer science and information engineering from National Central University in 2010. His research areas include network security, web security, and malware analysis.