PAPER

Client-Side Evil Twin Attacks Detection Using Statistical Characteristics of 802.11 Data Frames*

Qian LU[†], **Haipeng QU**[†a)], ***Members***, **Yuan ZHUANG**[†], **Xi-Jun LIN**[†], ***and*** **Yuzhan OUYANG**[†], ***Nonmembers***

SUMMARY With the development of wireless network technology and popularization of mobile devices, the Wireless Local Area Network (WLAN) has become an indispensable part of our daily life. Although the 802.11-based WLAN provides enormous convenience for users to access the Internet, it also gives rise to a number of security issues. One of the most severe threat encountered by Wi-Fi users is the evil twin attacks. The evil twin, a kind of rogue access points (RAPs), masquerades as a legitimate access point (AP) to lure users to connect it. Due to the characteristics of strong concealment, high confusion, great harmfulness and easy implementation, the evil twin has led to significant loss of sensitive information and become one of the most prominent security threats in recent years. In this paper, we propose a passive client-based detection solution that enables users to independently identify and locate evil twins without any assistance from a wireless network administrator. Because of the forwarding behavior of evil twins, proposed method compares 802.11 data frames sent by target APs to users to determine evil twin attacks. We implemented our detection technique in a Python tool named ET-spotter. Through implementation and evaluation in our study, our algorithm achieves 96% accuracy in distinguishing evil twins from legitimate APs.

key words: *evil twins detection, rogue access point, man-in-the-middle attack, WLAN security*

1. Introduction

Compared with wired networks, the Wireless Local Area Network (WLAN) has become extremely prevalent in the past few years due to a series of advantages: flexibility, mobility, scalability and easy installation. WLANs utilize radio waves to provide communication between APs and users' devices (such as smart phones, laptops) in wireless networks. Hence, users can conveniently use the Wi-Fi APs in WLAN to access the Internet in many places, such as hotels, offices, airports terminals, emporiums.

Although it is convenient to access the Internet, WLANs bring a lot of security issues. The rogue access point (RAP) is one of the most widely used means for adversaries to attack wireless networks. RAP is a kind of wireless access point that is installed on a reliable network without explicit authorization from the network administrator. In general, RAP can be divided into four categories: improperly configured AP, unauthorized AP, compromised AP and evil twin [1]. The evil twin, sometimes called as phishing access point, has the same Service Set Identification (SSID) with legitimate AP, deployed by adversaries targeting to intercept sensitive information from victim users. Users who lack professional knowledge and security awareness are prone to be attacked by a malicious adversary, causing a series of grave consequences.

The evil twin requires two wireless cards due to the fact that it needs to access the Internet through a legitimate AP. The first wireless card is associated with legitimate AP while the other wireless card is disguised as the legal one to induce users to connect it. According to the 802.11 protocol, wireless devices connect to access point with the best Received Signal Strength Indication (RSSI) value when there are multiple APs with the same SSID. Therefore, many wireless users automatically connect to RAP as it usually has a better RSSI value than the legitimate one [2]. This leads to attackers sniffing the users' traffic and launching a Man-in-the-Middle (MITM) attack because all victims' network packets go through RAP.

It is easy for adversaries to launch an evil twin attack successfully at public places. **First**, set up evil twin. Attackers can configure an evil twin on a laptop in the wireless network by using specific software. To masquerade as a legal AP and allure users to connect it, the evil twin usually has the same SSID with legitimate AP. **Then**, force victims to connect evil twin. An attacker can force victims to connect evil twins in a passive way, e.g., malicious adversaries can improve the RSSI of evil twins by deploying them closer to victim users than a legitimate one or using a directional antenna to attract victims' connection. Adversaries with professional skills can also actively launch MITM attack to occupy services of legitimate AP or send de-authentication frames to force victim turn to evil twin. Consequently, users may be cheated to connect the evil twin when they attempt to surf the Internet through a legitimate AP. **Finally**, sniff sensitive information or launch further attack. Sensitive information like passwords, credit card information can be easily captured through evil twin's relayed traffic. Even worse, attackers can also manipulate Domain Name System (DNS) servers, control routings, and launch other phishing attack, e.g. replace the online payment webpage with the attacker's phishing counterfeit.

Accordingly, detecting evil twin attack is still an important and challenging task for WLAN security. A variety of works has been done by researchers to address this problem. In this paper, we propose a client-based solution

Manuscript received January 23, 2018.
Manuscript revised May 9, 2018.
Manuscript publicized July 2, 2018.

[†]The authors are with the Dept. of Computer Science and Technology, Ocean University of China, Qingdao 266100, P.R. China.

*An earlier version of this paper was presented at the 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications.

a) E-mail: quhaipeng@ouc.edu.cn (Corresponding author)

DOI: 10.1587/transinf.2018EDP7030

to detect evil twin attack. Unlike previous solutions, our approach achieves following advantages: (a) We do not require any authorized lists to determine evil twins. (b) It is a passive approach, thus it does not need to connect to any access point or fill any login information when detecting. (c) It can provide a real-time detection for end users. (d) Whether the AP is open or not, our method is applicable. (e) It is able to find out two MAC addresses used by an evil twin.

2. Related Works

Rogue AP detection solutions can be generally divided into two categories. One is the admin-side method. The network administrator is the one charge of detecting evil twin attacks in WLANs. The other one is the client-based approach that enables wireless users to defend evil twin attacks by themselves.

2.1 Admin-Side Solutions

Network administrators generally use a kind of solution called Radio Frequency (RF) sniffing to identify RAPs. Active APs can be sniffed by deploying sensors inside the protected area or handheld detection devices used by administrators. The authors of [3]–[5] present a type of passive solutions that combines the monitored RF airwaves with the extra information gathered at core network to generate detection fingerprints. Afterward, compared the fingerprint with the known authenticated list, RAPs can be determined if there is any discrepancy. However, this kind of approach requires the deployment of wireless sensors in large scale wireless networks to continuously scan the radio waves emitted by the AP, so the cost of these methods is very expensive. In addition, if the attacker closes the rogue AP, reduces the signal intensity, or uses non-standard protocols and frequencies to evade detection during scanning, these deliberate behaviors will directly lead to the failure of such detection methods.

In the studies of [6]–[9], researchers propose another type of network administrator-based detection scheme. They monitor traffics at a aggregation (e.g. gateway) to differentiate whether users come from wireless networks or wired networks. If this information is different from the authorized list, the AP is identified as an illegal AP. Because above technologies belong to passive detections, they neither affect normal communication between APs and users, nor introduce redundant traffic into WLANs during detections. Nevertheless, these methods are not able to provide real-time detection services for Wi-Fi users.

In general, the admin-based detection schemes have to rely on a known authorization list to detect malicious AP. Most of them are time-consuming and expensive. Moreover, it fails to provide users with real-time detection. Thus, it is necessary to propose client-side approaches to detect rogue AP without any assistance from the network administrator.

2.2 Client-Side Solutions

In [10], [11], researchers put forward a kind of timing-based approach that utilizes the round trip time (RTT) between client and DNS server to determine whether the given AP is a legal one. The evil twin is detected because it will introduce an unavoidable time delay to the DNS server while communicating with the legitimate AP. But various reasons can cause a time delay and lead to false positives such as interference, congestion and collisions in WLANs. Although this method can achieve almost 100% accuracy under the condition of a light network load, its accuracy will continue decreasing in heavy traffic-loaded WLANs.

Song et al. [12] present a lightweight technique which utilizes Inter-packet Arrival Time (IAT) between two consecutive data packets sent from the same device to hosts as a feature for evil twin attack detection. In order to achieve robust and efficient detection result, the authors develop two new statistical anomaly detection algorithms (TMM, HDT) to make the final detection. TMM and HDT combine wireless IAT network statistics and Sequential Probability Ratio Test to identify rogue AP. However, wireless clients must connect the suspicious AP during detection, as a result of which, their information may be stolen in this period. Additionally, the research effort suffers from the limitation that it requires training knowledge of Server IAT in one-hop and two-hop wireless channels.

Some researchers focus on clock skew, an unavoidable physical phenomenon, as unique characteristics or fingerprints to identify rogue APs. Jana and Kasera [13] calculate each AP's clock skew by extracting Timing Synchronization Function (TSF) timestamps from beacon frames. Then, comparing the calculated clock skew with the existing clock skew recorded in the database to determine whether the AP is an illegal one or not. F. Lanze et al. in [14] improve the detection by combining clock skew with device-intrinsic temperature-dependency. For the purpose of establishing feature database, a large number of authorized AP samples are required to storage. Although this approach can determine most types of attacks, this method is costly, time-consuming and still lack of large-scale evaluation.

Kumar et al. [15] prevent users from accessing the evil twin by modifying the communication protocol between AP and terminal devices. This solution adds a new identifier called 'COUNT', which records the number of successful connections between each client and each AP, to the information list in AP and client. Before the client establishes connection with target AP, the values of 'COUNT' respectively stored in AP and client are compared through the request-response frames. Evil twins can be detected if these two values are different. However, such detection method that based on modification of 802.11 protocol is not practical because it need to change the existing driver and firmware in large scales.

3. Problem Statement and Principle

The aim of our research is to independently detect evil twin attacks in real time without any assistance of network administrators. In this section, we present the problem statement and our detection principle. Besides, the limitation of our approach is clearly acknowledged in Sect. 6.2.

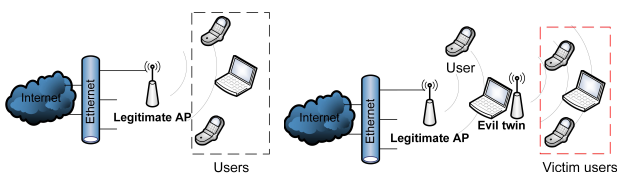
We present the network topology structure of normal AP model and evil twin model. Figure 1 (a) illustrates the normal scenario, a legitimate AP communicates with several wireless clients and connects them to the Internet through a wired network; on the other hand, in the attack scenario depicted in Fig. 1 (b), the legitimate AP and evil twin coexist in the same WLAN. The evil twin, installed by attackers, masquerades as a legal AP to lure victim users' connection, attempts to gather plenty of sensitive information and conduct more attacks. Both the evil twin and the legal AP use the same gateway as shown in Fig. 1 (b).

Compared with a normal scenario, the evil twin sits between the legitimate AP and victim users, relies on the legitimate AP to access the Internet, and forwards every packet between legal AP and victims like a 'middleman'. Therefore in ideal forwarding process, under the environment with 100% received signal strength and no wireless delay, the flow rate of effective data frames (EDFs) sent from the legitimate AP to evil twin should be equal to what sent from evil twin to victim users in every second. That is, for each moment, the EDFs flow rates of them would be similar in both quantity and trend.

Thus, we detect the evil twin attack by identifying such a forwarding behavior, which is quite different from other detection mechanism. By monitoring and gathering downstream data frames sent from target APs (legitimate AP and evil twin) to users, we are able to obtain the statistical characteristics between target AP and each connected user. Through filtering useless frames in our detection algorithms, remaining EDFs statistics are used to search for a suspicious forwarding behavior, which is detailed in Sect. 4. Note, the EDFs refer to the 802.11 non-retransmission data frames sent from the Internet, exclude the traffic that only transmits within the same subnet.

An concrete instance is given in Fig. 2 for the sake of further comprehension. We can see that there is a legal AP, an evil twin and several wireless users coexisting in WLAN. In order to relay the victims' packets to the Internet, the evil twin uses one network card to masquerade as a normal user, and connects to the legitimate AP. Variable p_3 denotes the flow rate of EDFs, a sequence records the number of EDFs captured per second, sent from the legitimate AP to the evil twin. Variable q_i represents the flow rate of EDFs sent from evil twin to each victim user. When there are multiple victims, denoted V, connecting with evil twin in the wireless network, p_3 should be equal with the sum of q_1, q_2, q_3 in the ideal case. Although some influence factors in the realistic network environment, such as forwarding delay and retransmission, may cause a slight difference between p_3 and $\sum_{i=1}^{3} q_i$, our solution takes the above factors into consideration and amends the EDFs statistical results. As a result, the evil twin attack can be detected if we can distinguish such forwarding behavior in WLAN.

In particular, we further filter the subnet traffic (like p^* and q^*) to get EDFs compared with our previous work [16]. Because the subnet traffic can affect the number of p_3 and $\sum_{i=1}^{3} q_i$, it makes them different. This kind of traffic can be generate by some operations, like V_1 *ping* V_2. Although it rarely appears in WLANs at most cases, we remove them to eliminate their impact on the similarity of the forwarding behavior.



(a) Normal AP model (b) Evil twin model

Fig. 1 Illustration of normal and attack network models.

4. The Proposed Framework

4.1 System Work Flow

According to the theoretical analysis in the period section, we put forward a client-side approach to detect evil twin attacks. The proposed focuses on detecting the evil twin attacks that legitimate AP and evil twin use the same gateway, which is detailed in Sect. 3. Figure 3 shows the processing logic of our detection solution. During the detection process, the key point is to find whether there is a suspicious forwarding behavior between target APs and users in WLAN.

At the beginning, our approach scans all available APs to check whether there are multiple APs with the same SSID in current wireless network environment. Because the evil twin needs to rely on a legitimate AP to access the Internet shown in Fig. 1 (b), we don't consider the situation that the legitimate AP is shut done by attackers. Thus, if there are no multiple APs with the same SSID, the algorithm will prompt users that there is no evil twins attack in WLAN. Otherwise, our approach records the MAC addresses (BSSID) of these

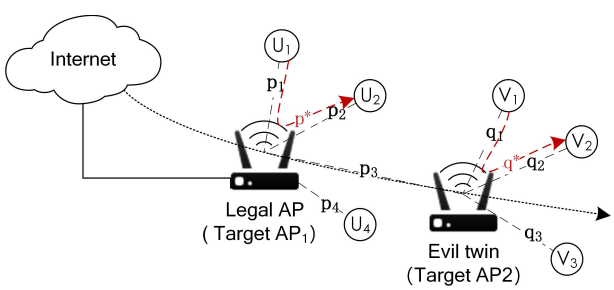


Fig. 2 A concrete instance of the evil twin.

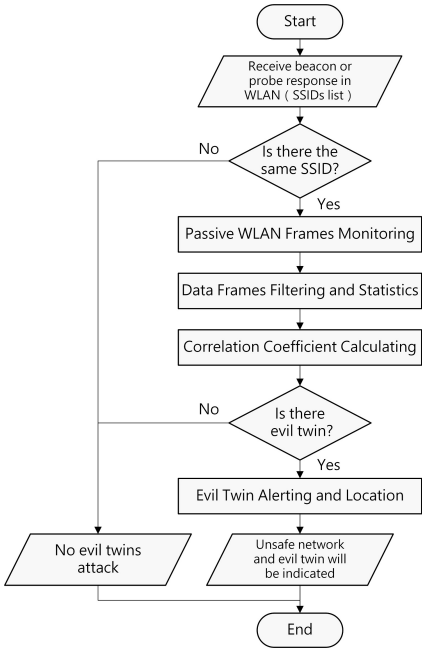


Fig. 3 Processing logic of our approach.

target APs which probably contain an evil twin, and monitors the traffic sent from them within a monitoring period. To obtain EDFs, a filter statement is used to filter out subnet traffics, control frames, management frames and retransmission data frames. Then, the remaining EDFs flow rate sent from the target APs to each user is recorded in an array respectively. In order to determine whether there is a forwarding behavior in the network, the Pearson correlation coefficients between target AP and appropriate users are calculated by using the values stored in above mentioned arrays. Hereafter, our approach determines whether there is a correlation coefficient exceeding the threshold. If exists, triggers an alert and reports the MAC addresses of the evil twin to network administrators and users. Eventually, our approach can locate the evil twin according to the MAC address and signal strength.

4.2 Main Steps of Proposed Framework

The main steps in proposed framework consist of four stages. The first three stages are the evil twin detection stage, and the last stage helps us to locate the evil twin. As shown below, Fig. 4 illustrates the proposed framework and briefly explains each stage.

4.2.1 Passive WLAN Frames Monitoring Stage

If there are two target APs with the same SSID, it indicates that an evil twin perhaps exists in the network. We need to make further judgments. In order to monitor the 802.11 frames emitted by the target AP, we require to get their basic information from beacon frames or probe response frames. The basic information mainly includes SSID, MAC address,

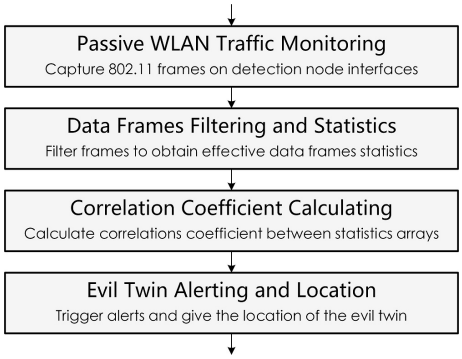


Fig. 4 Main steps of proposed framework.

channel number, etc. Since different target APs work in different channels in most cases, we use two wireless network cards to synchronously monitor the aforementioned channels to analyze whether there is a suspicious forwarding behavior. In addition, the wireless network interface cards (WNICs) in detection client should be set on monitor mode. This mode enables a wireless network cards to snif wireless traffic without associating with APs. After a period of passively monitoring, the wireless network trace which consists of control frames, management frames and data frames can be captured in designated channels. The different kinds of frames captured by this step are denoted as c_i, m_i, d_i, respectively.

4.2.2 Data Frames Filtering and Statistics Stage

At this stage, we aim at filtering above wireless frames to obtain the EDFs emitted by target APs and to get EDFs statistics between target AP_i and each connected user U_j. Specifically, the frames sent by target APs can be easily distinguished based APs' BSSIDs. Then we filter out c_i, m_i, retransmitted data frames and the subnet traffic, we acquire the effective data frames denoted as d'_i. We use a dictionary data record format to store them. For AP_i, each item in the dictionary is a key-value pair. The key is the MAC address of associated user U_j and the value is an array $D_i = [d'_1, d'_2, \ldots, d'_n]$ that records the relevant number of EDFs per second, while n is the total monitoring time. For instance, $AP_1\,[U_2] = [d'_1, d'_2, d'_3, d'_4]$ denotes the number of EDFs sent from AP_1 to U_2 within four seconds. Finally, we calculate the sum of EDFs sent from AP_i in a new array S_{AP_i}, that is, $S_{AP_i} = \sum_{j=1}^{n} AP_i[U_j]$.

Algorithm 1 Preprocessing and statistics

1: **for all** f_i **do**
2: retain f_i sent from target AP_i
3: filter out ($c_i \wedge m_i \wedge$ retransmitted $d_i \wedge$ subnet traffic) as d'_i
4: gather statistics for each AP_i
5: calculate S_{AP_i}
6: **end for**

4.2.3 Correlation Coefficient Calculation

This is a significant step in finding the malicious forwarding behavior. Through previous parts, we have already got $AP_1[U_j]$, S_{AP_1}, $AP_2[U_j]$ and S_{AP_2}. Then, we calculate the correlation coefficients $C_{S_{AP_1},AP_2[U_j]}$ between S_{AP_1} and each active $AP_2[U_j]$ using the Pearson correlation coefficient formula. The same procedure may be easily adapted to obtain $C_{S_{AP_2},AP_1[U_j]}$ between S_{AP_2} and each active $AP_1[U_j]$. We utilize the Pearson correlation coefficient to measure how highly correlated are two arrays. That is, how much abnormal similarities between multiple EDFs arrays. The higher the score is, the greater the EDFs flow rate in arrays are correlated. The Pearson correlation coefficient is:

$$C_{(x,y)} = \frac{\sum(X-\overline{X})(Y-\overline{Y})}{\sqrt{\sum(X-\overline{X})^2 \sum(Y-\overline{Y})^2}}$$

There are two benefits to using this metric. One is that the formula provide a quantitative standard to normalize the similarity between -1 and 1, giving users a more intuitive observation. Another benefit is that the accuracy of the score increases when data is not normalized. Therefore, it can still be used when EDFs arrays have reasonable difference caused by wireless network quality.

Compared with the algorithms in our previous work, the improved algorithm still takes inactive users' statistics into S_{AP_i}, but cancels to calculate correlation coefficients between inactive users and corresponding S_{AP_i}. The purpose is to improve the efficiency of algorithm detection and reduce unnecessary calculation and comparison.

Algorithm 2 Calculating correlation coefficient

```
for active U_j connected AP_2 do
    calculate C_{S_{AP_1},AP_2[U_j]}
end for
for active U_j connected AP_1 do
    calculate C_{S_{AP_2},AP_1[U_j]}
end for
```

4.2.4 Evil Twins Detection and Location

At this stage, the algorithm checks all $C_{S_{AP_1},AP_2[U_j]}$ and $C_{S_{AP_2},AP_1[U_j]}$. If there is a correlation coefficient $C_{S_{AP_i},AP_k[U_j]}$ exceeding the threshold value (TSV), it indicates that an evil twin exsits in WLAN. AP_i and U_j are the two MAC addresses using by the evil twin. AP_i is the network card used by evil twin to release Wi-Fi signals, and U_j is the other network card used by evil twins to disguised as a normal user and connect the legal AP. An alarm will be sent to administrators and users to protect them from connecting the evil twin. Finally, our approach is able to locate the evil twin according to the MAC address and the signal strength.

Algorithm 3 Detection and location

```
for all C_{S_{AP_i},AP_k[U_j]} do
    if C_{S_{AP_i},AP_k[U_j]} ⩾TSV then
        trigger an evil twin attack alert(AP_i)
        record the MAC addresses of AP_i and U_j
        locate(AP_i)
    else {C_{S_{AP_i},AP_k[U_j]} <TSV}
        prompt no evil twin attack
    end if
end for
```

5. Evaluation

5.1 Setup and Implementation

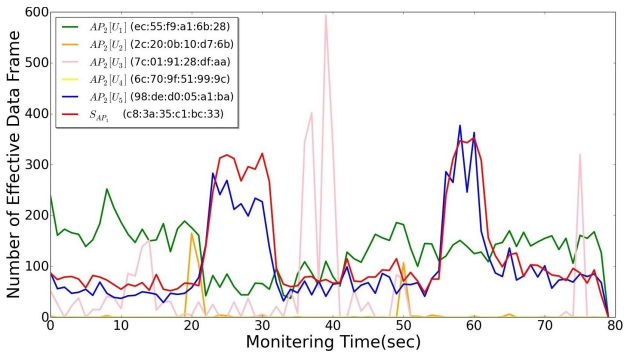
To verify our detection approach, we build the experimental testbed which can be divided into two groups: benign scenario and attack scenario. The benign scenario consists of several legitimate APs and a number of wireless devices. The legal APs coordinate users and connect them to a wired network. We use a laptop and an additional USB WNIC as a detection client for monitoring 802.11 traffic and detecting possible attacks.

Compared with benign scenario, we deploy another laptop with two USB WNICs to simulate an evil twin in attack scenario. The laptop has 8GB RAM and I7 processors running Ubuntu 16.04LTS system. One WNIC (Tenda W311M) acts as an evil twin alluring users' connection, and the other one (TP-LINK WN722N) relays wireless packets to legitimate AP. Tenda W311M is connected with an USB extension line to the laptop for extending distance between two WNICs to avoid interference of two 2.4Hz WNICs. To set up the rogue AP, we used *Hostapd* to construct access points, *Udhcpd* to set up a Dynamic Host Configuration Protocol (DHCP) server and *Iptables* to retransmit wireless packets.

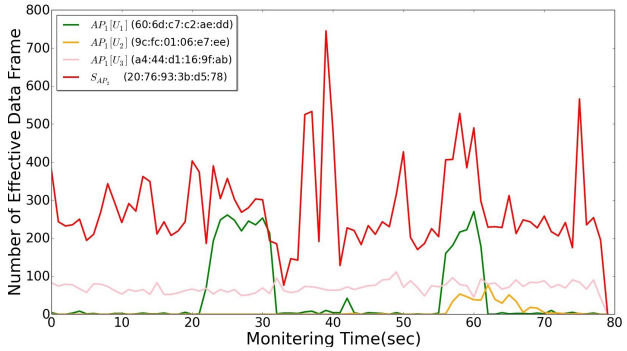
Additionally, we implement a prototype detection system called Evil Twin Spotter (ET-spotter). At most cases, different APs work in different channels. So monitoring different channels with two WNICs synchronously makes result more accurate compared with frequency hopping using one WNIC. We choose an onboard WNIC (Ralink RT3290) and a plug-and-play WNIC (EDUP EP-N 8508GS) on one laptop. ET-Spotter, which written in Python, enables two WNICs to monitor traffic synchronously in two processes, filter and analyze the traffic, compute correlation coefficient, then output the results. *Scapy* has been used to capture wireless traffic. *PyShark* and *Matplotlib* are utilized for analyzing and filtering packets to get analytical results. *Matplotlib* is a 2D plotting library to plot EDFs statistics figures. After computations of correlation coefficient using *Numpy*, MAC addresses of the possible evil twin can be distinguished based on the output results.

5.2 Results

To simulate evil twin attack scenario, we configured an evil



(a) The EDFs curves of S_{AP_1} and $AP_2[U_j]$



(b) The EDFs curves of S_{AP_2} and $AP_1[U_j]$

Fig. 5 The EDFs curves between target AP and users.

twin on a laptop as described in Sect. 5.1. It had the same SSID with a legitimate campus AP, and the legal AP generated a good RSSI to users between 60% and 100%. The evil twin was located near the victim users so that it provided a better signal than legal AP. In addition, the evil twin and legitimate AP worked in the 6 and 11 channels, respectively. Based on ET-spotter, we have done extensive experiments to verify our detection algorithm and analyzed large quantities of measured results to get a empirical TSV (0.56).

We enumerate and analyze one of the typical experiments results (Exp1). In Exp1, there are 5 users associated with legal AP and 3 victims connected the evil twin. At the detection client, we receive the RSSI from the legitimate AP and the evil twin are around −48dBm and −39dBm, respectively. During detection, these wireless users connect target APs and surf the Internet, such as watching video, brush micro-blog.

To present the experimental result more intuitively, the EDFs flow rate statistical figures are drawn by ET-spotter. Figure 5 show the results under the environment of Exp1. Obviously, the curves of S_{AP_1} and AP_2U_5 in Fig. 5 (a) are very similar in both quantity and trend, and the correlation coefficient between them is up to 92%. This indicates AP_1 (c8:3a:35:c1:bc:33) relayed the EDFs which sent from AP_2 to $[U_5]$ (98:de:d0:05:a1:ba). Thus, AP_2 is the legitimate AP, while U_5 and AP_1 are two MAC addresses of the evil twin. AP_1 is the malicious signal release part for evil twin, and U_5 is the other part that pretends to be a normal user to connect legal AP_2. More correlation coefficient are illustrated in Tables 1 (a) and (b), respectively.

Table 1 Person correlation coefficient of Exp1.

(a) Person correlation coefficient between S_{AP_1} and $AP_2[U_j]$

Target AP	Target $AP_2[U_j]$				
	$AP_2[U_1]$	$AP_2[U_2]$	$AP_2[U_3]$	$AP_2[U_4]$	$AP_2[U_5]$
S_{AP_1}	−0.258	0.110	−0.182	0.07	**0.928**

(b) Person correlation coefficient between S_{AP_2} and $AP_1[U_j]$

Target AP	Target $AP_1[U_j]$		
	$AP_1[U_1]$	$AP_1[U_2]$	$AP_1[U_3]$
S_{AP_2}	0.281	0.152	0.018

Table 2 Detection rate under different RSSI and locations.

Location	RSSI levels				
	A	B	C	D	E
Loc.1	97.94%	98.04%	96.94%	95.10%	85.29%
Loc.2	97.67%	97.67%	96.51%	95.35%	84.88%
Loc.3	97.93%	96.74%	96.77%	95.70%	86.02%

5.3 Effectiveness

To evaluate the detection accuracy and efficiency of our approach, we conducted about 1400 groups of experiments used ET-spotter at different locations, with different experimental parameters (RSSI, users number, and victims number).

We divide the RSSI into 5 levels: A(100%–80%), B(80%–70%), C(70%–60%), D(60%–50%) and E(50%–40%). Level A, B, C indicate corresponding AP can provide user a good stable Wi-Fi service. As the RSSI attenuation from A to E, the communication capacity between the wireless user and the AP is gradually reduced. If the RSSI decrease to level E, even though a wireless user can probe the AP's signal, it is hard to stably connect the AP or access to the Internet.

Table 2 shows that our detection method can reach a high detection rate (over 96%) when RSSI level is relatively high (A, B, C). Because of the high RSSI, the ability to monitor the target AP is strong, the lost wireless frames are less, and enough EDFs can be captured to for statistical analysis. When the RSSI falls to level D, our algorithm also achieves a decent detection rate over 95%. Additionally, the accuracy drops rapidly since RSSI decrease to level E. This phenomenon is caused by the difficulty to monitor target AP and the loss of partial EDFs. However, if the RSSI received from evil twin is lower than that of legitimate AP or evil twin provides a low-speed network (like level D, E), it will lose attraction to victim and lead to the failure of the evil twin attack. To sum up, ET-spotter could detect the evil twin attacks at most cases.

5.4 Time Efficiency

We also evaluate the time efficiency of our approach under

different RSSI levels. The total detection time consists of two parts: monitoring time and processing time. Through verification, EDFs collected in 30 seconds are able to output a correct result. In our experiment, the user number of the legal AP is about 3–8, and the evil twin has about 2–4 users. According to the experimental data, the time of frame processing and correlation coefficients calculation is no more than 8s. Totally, our algorithm can output the detection results within 38 seconds.

6. Discussion and Future Work

6.1 Analysis

Our proposed approach allows users themselves to independently detect evil twin attacks in real time, which is an obvious advantage over admin-based methods [5], [17]. In spite of ET-spotter is a client-side detection, it can also be used by administrators to examine their networks. The laptop with an USB WNIC is so portable that our ET-spotter may be more preferred in a wide range of situations such as companies, airports, offices, etc. Particularly, since its low expenditure (only need a laptop and an USB WNIC), it is a good choice for some places that are reluctant to spend more money on the ETA detection. Some expensive approaches, like AirDefence 7.4, have reached $8466.

Furthermore, with the enhancement of users' security awareness, most Wi-Fi networks have adopted the encryption technique. So, some solutions rely on the details of the upper layer protocol are no longer applicable [18]. ET-spotter, based on traffic statistical characteristics, can be utilized in both open and encrypted network. Compared with the methods based on hardware fingerprint features, such as clock skews [19], [20], our method doesn't need to establish a large fingerprint database. Furthermore, since our approach is a passive method, it is more difficult to be realized by attackers than active detecting methods [21], [22].

In addition, ET-spotter is effective for the hidden AP problem. In such a situation, the hidden AP does not send beacon frames to the network, only the person who knows the hidden AP can connect it by manually entering its SSID and password. Once such a customer is available, we can learn its SSID through the probe and association request frames that are sent to the hidden AP. Then continue to follow the normal steps to detect evil twin attacks.

6.2 Discussion

For another discussion point, although our detection method achieves outstanding performance, once an attacker has realized our detection method, an attacker may try to reduce the correlation of the evil twin's forwarding behavior by consuming the bandwidth at the evil twin end for avoiding detection. For this special evasion attack against our method, we conducted another 150 groups of experiments in different Wi-Fi networks in our university campus. We set the legal AP and evil twin on the 2.4GHz working channels (channel 6 and channel 11). The number of victims connecting evil twin is 2–3, and the number of users associating with legal AP is 3–5 (including evil twin). We request wireless users and victims to conduct most common Internet behaviors like browsing shopping websites, watching videos, and playing mobile games. Although the devices in the experimental scenarios support the 802.11b/g/n protocols, the actual wireless transmission rate of the LAP is approximately 12Mbps. We all know that the actual transmission rate of the wireless network is much less than the theoretical value because the wireless network environment is very complicated and it can be disturbed by many factors. In our experiment, we measured the LAP's real-time transmission rate fluctuating in the range of 4Mbps–19Mbps, as a result of interference, reflection, loss, and administrator speed limit, but most of the time, it remained at the average of 12Mbps.

For the evil twin, because the laptop with WNICs is not a dedicated routing device, its routing and forwarding capabilities are inferior to that of normal routers. After using the laptop to construct the evil twin, its average transmission speed of the Wi-Fi network is only about 3.6Mbps, which is also fluctuating based on environmental factors. And we simulate the three most common evasion behaviors from an attacker at the evil twin side, i.e. browsing the web, listening to music, and watching videos. Our 150 experiments show that when an attacker consumes a small or moderate amount of traffic (less than 1.5Mbps, such as browsing a web page and listening to music) on the evil twin's laptop, ET-spotter can still maintain a good performance with 98% accuracy and the correlation between the forwarded traffic can still exceed the threshold. But, as the occupied bandwidth of the attacker increases, the accuracy of our method gradually decreases. When the attacker deliberately consumes a large amount of traffic on the evil twin side (such as watching a video, at least 300KBps, i.e. 2.34Mbps) to avoid the detection, we realize that the correlation of the traffic becomes lower and forwarding behavior becomes difficult to confirm. The detection accuracy drops to 38% when attacker consumes most of the bandwidth.

However, such evasion behavior will rapidly reduce the bandwidth available to victims, and three victims in our experiments apparently feel that the connected AP (evil twin) is slowing down. They even want to switch the Wi-Fi due to the low speed network. Especially in public places, such as airports and railway stations where the Wi-Fi speed is relatively low, if the attacker occupy a mass of bandwidth on the evil twin side, this low-speed network will lose its attraction to the victims, cause the victims to disconnect from it, and eventually lead to the failure of evil twin attack. At the same time, however, we realize that this may be a vulnerability of our detection methods. In particularly, if the equipment used to construct the evil twin is more advanced or the wireless transmission rate is significantly faster like 802.11ac, this problem may become prominent. Therefore, we plan to further study and address this evasion attack against our

approach in the future.

6.3 Limitation

Although above results show that our approach has an exceptional performance in determining evil twin attack, some limitations of our approach should be noted. Because ET-spotter is based on the forwarding behavior to detect evil twins, so there must be at least one user associates one of the target AP. The wireless user should surf the Internet such as browse website, watch videos, etc. If the user only connecting the evil twin instead of using it, it is difficult for ET-spotter to identify the evil twin attack through statistical EDFs arrays. Fortunately, this restriction can be broken by users themselves, the user can use their others auxiliary device, such as tablet, smart phones, to help ET-spotter detect evil twins.

Another minor limitation is that this detection method requires two wireless network cards to simultaneously monitor the traffic in WLANs. Thus, in addition to the built-in wireless adapter in the mobile device, another wireless network card is necessary. But in realistic situation, it is not a difficult thing to carry an USB wireless network card. Nevertheless, we are trying to use one wireless adapter to solve the above limitation.

6.4 Future Work

Although it's convenient to carry an extra USB WNIC, we are still trying to use a single laptop WNIC to accomplish the evil twin detection without affecting the detection rate. Additionally, ET-spotter has been implemented and applied on Linux operating system (OS). In our future work, we plan to apply our approach in other popular OS to protect more users from evil twin attacks, and address the possible attack against our detection approach.

7. Conclusion

In this paper, we present a passive client-side detection mechanisms to protect wireless users from evil twin attacks. We are the first to use the statistical characteristics of 802.11 data frames to detect the ETA. The approach does not depend on the details of the upper protocol, so it can effectively detect evil twin attacks whether AP is open or encrypted. The users or administrators can not only know the MAC address of the evil twin used to release signals, but also find out the MAC address used by the evil twin to disguise as a legitimate user. In addition, we implement our method into a python tool, ET-spotter, on Linux system. Extensive experiments in different experimental conditions demonstrate the accuracy and effectiveness of our approach, and ET-spotter can output a detection result within 38 seconds.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61379127), the Public Science and Technology Research Fund Projects of Ocean of China (No. 201105033).

References

[1] N. Agrawal and S. Tapaswi, "Wireless rogue access point detection using shadow honeynet," Wireless Personal Communications, vol.83, no.1, pp.551–570, 2015.
[2] B. Alotaibi and K. Elleithy, "Rogue access point detection: Taxonomy, challenges, and future directions," Wireless Personal Communications, vol.90, pp.1261–1290, 2016.
[3] N.T. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric Bayesian method," INFOCOM 2011, pp.1404–1412, 2011.
[4] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," ACM International Conference on Mobile Computing and Networking, pp.116–127, 2008.
[5] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "Enhancing the security of corporate Wi-Fi networks using DAIR," International Conference on Mobile Systems, Applications, and Services, pp.1–14, 2006.
[6] S. Shetty, M. Song, and L. Ma, "Rogue access point detection by analyzing network traffic characteristics," Military Communications Conference, Milcom 2017, pp.1–7, 2007.
[7] H. Yin, G. Chen, and J. Wang, "Detecting protected layer-3 rogue APs," International Conference on Broadband Communications, Networks and Systems, 2007, Broadnets, pp.449–458, 2007.
[8] W. Wei, S. Jaiswal, J. Kurose, and D. Towsley, "Identifying 802.11 traffic from passive measurements using iterative Bayesian inference," INFOCOM 2006, IEEE International Conference on Computer Communications, pp.1–12, 2006.
[9] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, "Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs," ACM SIGCOMM Conference on Internet Measurement 2007, San Diego, California, USA, pp.365–378, Oct. 2007.
[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.D. Mano, A. Blaich, Q. Liao, Y. Jiang, D.A. Cieslak, D.C. Salyers, and A. Striegel, "Ripps: Rogue identifying packet payload slicer detecting unauthorized wireless hosts through network traffic conditioning," ACM Trans. Information & System Security, vol.11, no.2, Article No.2, 2008.
[12] Y. Song, C. Yang, and G. Gu, "Who is peeping at your passwords at starbucks?—To catch an evil twin access point," IEEE/IFIP International Conference on Dependable Systems & networks, pp.323–332, 2010.
[13] S. Jana and S.K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," IEEE Trans. Mobile Comput., vol.9, no.3, pp.449–462, 2010.
[14] 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," ACM Symposium on Information, Computer and Communications Security, pp.3–14, 2014.
[15] A. Kumar and P. Paul, "Security analysis and implementation of a simple method for prevention and detection against evil twin attack in IEEE 802.11 wireless LAN," International Conference on Computational Techniques in Information and Communication Technologies, pp.176–181, 2016.
[16] Q. Lu, H. Qu, Y. Zhuang, X.-J. Lin, Y. Zhu, and Y. Liu, "A passive client-based approach to detect evil twin attacks," 2017 IEEE Trustcom/BigDataSE/ICESS, pp.233–239, 2017.
[17] W. Wei, B. Wang, C. Zhang, and J. Kurose, "Classification of access network types: Ethernet wireless LAN, ADSL, cable modem or di-

alup?," INFOCOM 2005, Joint Conference of the IEEE Computer and Communications Societies, vol.2, pp.1060–1071, 2005.
[18] F.-H. Hsu, C.-S. Wang, Y.-L. Hsu, Y.-P. Cheng, and Y.-H. Hsneh, "A client-side detection mechanism for evil twins," Computers & Electrical Engineering, vol.59, pp.76–85, 2017.
[19] C. Arackaparambil, S. Bratus, A. Shubina, and D. Kotz, "On the reliability of wireless fingerprinting using clock skews," ACM Conference on Wireless Network Security, pp.169–174, 2010.
[20] F. Lanze, A. Panchenko, I. Ponce-Alcaide, and T. Engel, "Undesired relatives: Protection mechanisms against the evil twin attack in IEEE 802.11," ACM Symposium on QoS and Security for Wireless and Mobile Networks, pp.87–94, 2014.
[21] S. Bratus, C. Cornelius, D. Kotz, and D. Peebles, "Active behavioral fingerprinting of wireless devices," ACM Conference on Wireless Network Security, WiSec '08, Alexandria, VA, USA, pp.56–61, 2008.
[22] F. Lanze, A. Panchenko, I. Ponce-Alcaide, and T. Engel, "Hacker's toolbox: Detecting software-based 802.11 evil twin access points," 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), pp.225–232, 2015.

Qian Lu was born in 1992. She is a Ph.D. candidate at the Department of Computer Science and Technology, Ocean University of China. Her research interest includes network security, wireless communication and cyber physical system.

Haipeng Qu is an associate professor at the Department of Computer Science and Technology, Ocean University of China. He received his Ph.D. degree from Chinese Academy of Sciences. His research interests include information security and sensor network.

Yuan Zhuang is pursuing a Master degree in Computer Science from the Ocean University of China since 2016. As a member of Cyber Security Lab, her research interests are in the fields of software security, binary exploitation and IoT vulnerabilities.

Xi-Jun Lin is a lecturer at the Department of Computer Science and Technology, Ocean University of China. He received his Ph.D. degree from Chinese Academy of Sciences. His research interests include cryptography and information security.

Yuzhan Ouyang is currently persuing his M.S. degree from the Department of Computer Science at Ocean University of China. His primary research area of interest is network security.