A Passive Client-based Approach to Detect Evil Twin Attacks

Qian Lu†, Haipeng Qu†*, Yuan Zhuang†, Xi-Jun Lin†, Yanyong Zhu† and Yunzheng Liu‡
†Department of Computer Science and Technology, Ocean University of China, Qingdao 266100, China
‡Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
*Corresponding author. E-mail: quhaipeng@ouc.edu.cn

***Abstract*—As the widespread deployment and usage of 802.11-based wireless local area networks (WLANs), Wi-Fi users are vulnerable to be attacked by a security threat called evil twins. The evil twin, a kind of rogue access points (RAPs), masquerades as a legitimate access point (AP) to lure users to connect it. Malicious adversaries can easily configure evil twins on a laptop to induce victim wireless users. The presence of such a threat continuously leads to significant loss of information. In this paper, we propose a passive client-side detection approach that allows 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 and location 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.**

I. 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 routers and users' devices, like smart phones, laptops, etc. Hence, users can conveniently use the Wi-Fi access points (APs) in WLAN to connect to 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 perilous security threats. RAP is a kind of wireless access point that is installed on a reliable network without explicit authorization from the network administrator. 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, sometimes called as fishing access point, is a category of RAP that has the same Service Set Identification (SSID) with legitimate AP, deployed by adversaries targeting to intercept sensitive information from victim users. 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 associates with legitimate AP while the other wireless card disguises 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. This leads to attackers sniffing the users' traffic and launching a Man-in-the-Middle (MITM) attack because all the packets go through RAP.

It is easy for adversaries to launch an evil twin attack successfully at public places. First, attackers can configure an evil twin on a laptop in the wireless network by using specific software. To masquerade as a legal AP and lure users to connect it, attacker configures the laptop with the same SSID like legitimate AP. Then, malicious adversaries improve the RSSI of evil twins by deploying them closer to victim users than a legitimate one or using a directional antenna. Consequently, users may be cheated to connect the evil twin when they attempt to surf the Internet through a legitimate AP. Finally, attackers can sniff the users' network traffic through evil twins. Even worse, if users' data are not encrypted, sensitive information like passwords, credit card information can be captured by attackers.

Accordingly, detecting evil twin attack is an important and challenge task for WLAN security. A variety of works has been done to address this problem. Existing approaches for detecting evil twin can be classified into two categories: administrator-based solutions and client-based solutions. Although the majority of approaches being used belong to administrator-based mechanisms, they cannot detect evil twin in real time and have a heavy overhead. Designing a client-side approach to detect evil twins is not easy for clients because users have limited resources and without authorization list.

In this paper, we propose a novel client-based solution to detect evil twin attack. Unlike previous solutions, our approach achieve 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) Regardless of whether the AP is encrypted, our method is applicable.

The paper is further structured as follows. We give a overview of related work in Section 2. Section 3 describes the problem statement and principle of our approach. Then, our proposed method is described in section 4. Section 5 discusses setup and implementation. After the results and performance analysis of our approach in section 6, we give a conclusion in Section 7.

2324-9013/17 $31.00 © 2017 IEEE
DOI 10.1109/Trustcom/BigDataSE/ICESS.2017.242

IEEE computer society

II. Related Work

In general, existing rogue AP detection methods can be classified into two categories. The first category is the admin-side solution that helps network administrators to detect unauthorized AP installed on the wireless network. Second category is a client-side solution that helps wireless users detect rogue AP without any assistance from the network administrator. Although there are various methods to detect rogue AP, each solution has its own pros and cons.

A. Admin-side solutions

The authors of [14] [5] [2] propose a kind of passive approaches for rogue AP detection which monitors Radio Frequency (RF) airwaves and gathers additional information (contains RF measurement, MAC address, signal strength, and AP control frames) at core network. Then, comparing specified fingerprints of the radio frequency with a known authorized list to determine whether the AP is an evil twin or not. However, the cost of installing sensors in a large scale wireless networks such as public hotspots is very expensive. Moreover, this approach will fail in following situations: attackers turn off the rogue AP, reduce signal strength, or use nonstandard protocols and frequencies to evade the detection during scanning.

Another solution of rogue AP detection, proposed in [16] [21] [18] [19] [20], detects the evil twin by monitoring traffics at a traffic aggregation to differentiate whether clients come from wireless networks or wired networks. If this information is different from authorization list, the AP is identified as a rogue one. However, these approaches are difficult to protect wireless users from being tricked into connecting evil twins in real time. These admin-side solutions are limited because the authorization list is indispensable. Most of them are time-consuming and expensive. Thus, it is necessary to propose a client-side approach to detect rogue AP without any assistance from the network administrator.

B. Client-side solutions

The authors of [7] [13], propose a type of timing-based approaches which use the round trip time (RTT) between the user and the 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 real AP. However, various reasons can cause a time delay and lead to false positives such as interference, congestion and collisions in WLAN.

Song et al. [17] propose a lightweight client-side 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, 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 [9] calculate each APs clock skew by extracting Timing Synchronization Function (TSF) timestamps from beacon frames. Afterwards, 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 [11] 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 require to storage. Although this approach can determine most types of attacks, the method is still lack of large-scale evaluation.

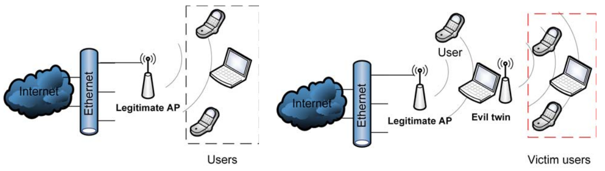
Bratus et al. [4] introduce an active behavioral fingerprinting approach. It takes advantage of request-response proactive detection techniques that can be implemented through network probing and security auditing tools such as nmap. The proposed method sends a request frame and waits for a response to determine how the device responds to the fragment frame. In detail, some wrong format data frames were actively sent by users to stimulate the wireless AP, and different AP wireless network card will make a different response to the abnormal data. By capturing these different response packets and extracting special value, the fingerprint can be calculated and utilized to detect evil twin. This approach also has its shortcoming: it takes advantage of active detection techniques that can be evaded by most adversaries. In addition, the detection approach can be interfered by normal WLAN traffic.

Another client-side solution of evil twin detection, proposed in [10], utilizes the received signal strengths (RSSs) sequences in an online detection algorithm. After measuring the similarity of normalized RSSs, fake AP could be detected if the similarity between normalized RSSs is less than the predefined threshold value.

In [6], Altaibi et al. propose a passive fingerprinting solution that depends on difficult to change the characteristics of the Radiotap length in RAP which belongs to physical layer. Radiotap length is the length of Radiotap header in beacon frame, which is generated by the receiving wireless card. Because changing this value require changing several other fields in physical layer, so it is difficult for malicious attackers to spoof. Nevertheless, in order to identify rogue AP, this approach need extensive training to obtain a large number of Radiotap lengths of all APs and set the threshold value.

Fu-Hau et al. [8]propose a client-based solution that exploits the packet forwarding behavior of RAP as an unavoidable behavior to identify the evil twin. The authors develop a detecting system called ET detector to capture wireless TCP/IP packets in the air and extract sequence number and acknowledgement number in the TCP/IP headers. If the same sequence number and acknowledgement number appear twice, the detection can determine a rogue AP exists between legitimate AP and victim users. However, this solution has a severe drawback: it works only in the case of the packet is not encrypted, otherwise it cannot extract sequence number and acknowledgement number in the TCP/IP headers.

III. Problem Statement and Principle



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

Fig. 1: Illustration of normal and attack network models

In this section, we describe the problem statement and principle of our approach.

An evil twin is a hardware-based or software-based 802.11 AP which spoofs the identity of a legitimate AP by cloning its characteristics in order to trap a user to hijack his connection. It has the same SSID with the legitimate AP so users can connect to it automatically when they receive a stronger signal from it.

Figure 1(a) shows the normal scenario where a legitimate AP coordinates several wireless clients and connects them to a wired network. Additionally, in attack scenario depicted in Figure 1(b), there is an evil twin configured by attacker deceiving users into connecting to gather plenty of sensitive information and conduct more attacks. Compared with a normal scenario, the evil twin sits between the legitimate AP and victim users as a gateway, forwards every 802.11 frames between them. Therefore, in ideal forwarding process, the flow rate of data frames 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, the flow rate and the trend of them in each moment would be similar.

Obviously, this forwarding behavior gives us the intuition to detect evil twin attacks by monitoring whether the two APs with the same SSID have similar statistics of data frames in WLAN, without any assistance from administrators.

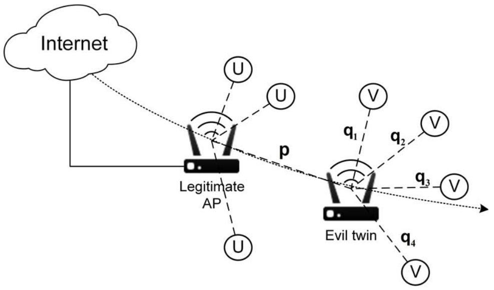


Fig. 2: Concrete instance of evil twin

In order to facilitate the calculation, we monitored downstream data frames sent by APs (legitimate AP and evil twin) to users, disregarding management frames and control frames after monitor stage. For instance, in Figure 2, variable p represents the flow rate of data frames, an array records the number of data frames captured per second, sent to the evil twin by legitimate AP. Variable q represents the flow rate of data frames sent to victim users by evil twin. When there are multiple victim users, represented V, associated with evil twin in the wireless network, p should be equal with the sum of q_1, q_2, q_3 in the ideal case. In the realistic network environment, the deviation of statistical results owing to some possible inaccuracy such as forwarding delay and retransmission, which has been taken into account, also can be modified by our algorithm.

IV. The Proposed Framework

A. System Work Flow

Figure 3 shows the processing logic of our detection solution. The key point is to find whether there is suspicious forwarding behavior between APs and users in WLAN.

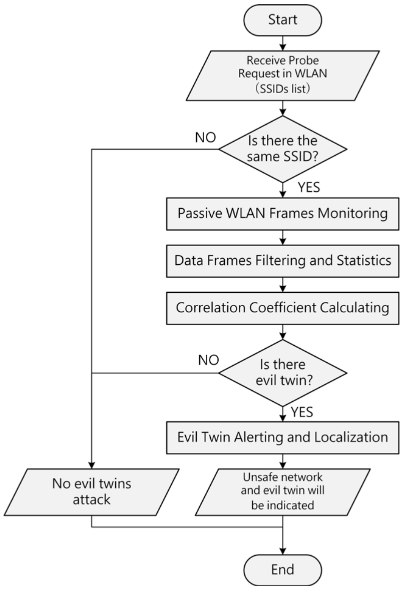

Start
Receive Probe Request in WLAN (SSIDs list)
Is there the same SSID?
NO
YES
Passive WLAN Frames Monitoring
Data Frames Filtering and Statistics
Correlation Coefficient Calculating
Is there evil twin?
NO
YES
Evil Twin Alerting and Localization
No evil twins attack
Unsafe network and evil twin will be indicated
End

Fig. 3: Processing logic of our approach

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. If there is no such situation, the algorithm will prompt users that there is no evil twins attack in WLAN. Otherwise, our approach records the MAC addresses (BSSID) of these two target APs which probably contain a real evil twin, and monitors the traffic sent from them within a monitoring period. To obtain effective data frames, a filter statement is used to filter out control frames, management frames and retransmission data frames. Then, the remaining data frames flow rate sent by 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, Pearson correlation coefficients are calculated by using the values between each user and target AP in their own arrays. Hereafter, our approach determines whether there is a correlation coefficient exceeding the threshold, if exists, reports the existence and MAC addresses of the evil twin to the network administrator and users. By doing so, evil twin can be located by using the MAC address and signal strength.

B. 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, Figure 4 illustrates the proposed framework and briefly explains each stage.

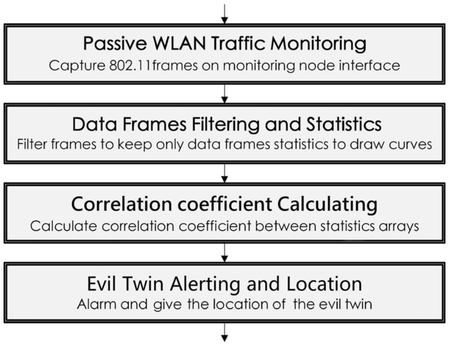

Passive WLAN Traffic Monitoring
Capture 802.11frames on monitoring node interface
Data Frames Filtering and Statistics
Filter frames to keep only data frames statistics to draw curves
Correlation coefficient Calculating
Calculate correlation coefficient between statistics arrays
Evil Twin Alerting and Location
Alarm and give the location of the evil twin

Fig. 4: Main steps of proposed framework

1) Passive WLAN Frames Monitoring Stage: The wireless network interface card should be set on monitoring mode to capture the traffic in WLAN, after a period of passively monitoring, the wireless network trace is captured which consist of control frames, management frames and data frames. The control frames, management frames and data frames captured by this step are respectively represented as c_i, m_i, d_i.

2) Data Frames Filtering and Statistics Stage: We are only interested in the frames that sent by target APs, and the aim of this part is to filter out the effective data frames flow rate sent by APs. AP_i and U_i are used for representing access points and wireless users respectively. As mentioned in Section 3, data frames are totally forwarded between two nodes, so management frames, the control frames and the retransmitted data frames are filtered in this stage, keeping only the effective data frames d'_i. For instance, d'_s is the number of effective data frames sent by AP_i to U_i in sth second. Afterwards, we gather the statistics of the effective data frames sent by target APs and record them in $AP_iU_j = [d'_1, d'_2, \ldots, d'_n]$. The data record format of AP_iU_j is a dictionary while each of which is a key-value pair. The key is the MAC address of the user U_i and the value is the array $[d'_1, d'_2, \ldots, d'_n]$ sent by the AP_i to U_i, n is the monitoring time (seconds). Finally, we calculate the sum of flow rate sent from S_{AP_i} in a new array, that is, $S_{AP_i} = \sum_{j=1}^{n} AP_iU_j$.

Algorithm 1 Data frame d'_i prepocessing and statistics

```
for all $f_i$ do
    retain $f_i$ sent from target $AP_i$
    ignore ($c_i \wedge m_i \wedge$ retransmitted $d_i$) as $d'_i$
    gather statistics $AP_iU_j$
    calculate $S_{AP_i}$
end for
```

3) Correlation Coefficient Calculating: In order to avoid being discovered by users since bringing a huge delay to the network, malicious attackers will not configure multiple evil twins for the same SSID in most cases. Although our method is effective in that condition, we give a situation like most cases where have two target APs in current WLAN for convenient and clear description, that is, there are one legal AP and one evil twin for the same SSID. The correlation coefficients C_{AP_1,AP_2U_j} are calculated by S_{AP_1} and AP_2U_j using the Pearson correlation coefficient formula. The same procedure may be easily adapted to obtain C_{AP_2,AP_1U_j} calculated by S_{AP_2} and AP_1U_j. The Pearson correlation coefficient is:

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

Pearson correlation coefficient metric measures how highly correlated are two arrays and is measured from -1 to +1, that is, are there any abnormal similarities between multiple data frame arrays. The higher the score of it is, the greater the effective data frame flow rate in arrays are correlated. There are several benefits to using this metric. The first is that the accuracy of the score increases when data is not normalized. Another benefit is that it can correct for any scaling within an attribute, while the final score is still being tabulated. Therefore, it can still be used when data frame arrays have reasonable difference caused by wireless network quality.

Algorithm 2 Calculating correlation Coefficient

```
for all $U_j$ connected $AP_2$ do
    calculate $C_{AP_1,AP_2U_j}$
end for
for all $U_j$ connected $AP_1$ do
    calculate $C_{AP_2,AP_1U_j}$
end for
```

4) Evil twins Detection and Location: The algorithm checks all the $C_{AP_1,AP_2U_j}$and C_{AP_2,AP_1U_j}, and if there is a correlation coefficient C_{AP_i,AP_kU_j} exceeding the threshold value (TSV), indicating that AP_i and U_j are the two MAC addresses of evil twin. 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 $C_{AP_i,AP_kU_j}$ do
    if $C_{AP_i,AP_kU_j} \geqslant$TSV then
        trigger an evil twin attack alert($AP_i$)
        record the MAC addresses of $AP_i$ and $AP_kU_j$
        locate($AP_i$)
    else $\{C_{AP_i,AP_kU_j} <$TSV$\}$
        prompt no evil twin attack
    end if
end for
```

V. Setup and Implementation

We build experimental testbed to test our method where contains two scenarios: benign scenario and attack scenario. The benign scenario consists of two legitimate APs and several wireless devices, as shown in Figure 5. These two AP coordinates users and connects them to a wired network. Figure 6 shows the attack scenario where two legitimate APs connecting to the wired network, an evil twin disguised as an normal user to connected to a legitimate AP, and some wireless users associate with legal APs and evil twin. The evil twin has the same SSID with the legitimate one so users can connect to evil twin automatically when it has stronger Radio Signal Strength. Sniffers in each figure are set for monitoring the wireless traffic and detecting possible attacks. After building benign scenario above, implementation of our experiment is based on the attack scenario which contains three steps:

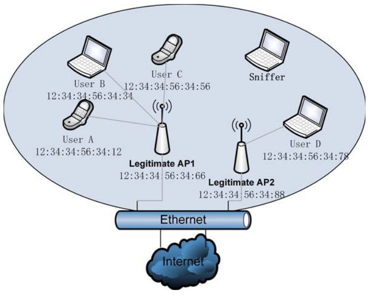


Fig. 5: Experiments setup for normal scenario

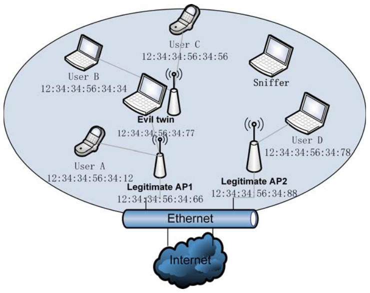


Fig. 6: Experiments setup for attack scenario

1) Evil twin construction
2) Wireless traffic capture
3) Traffic analysis

A. Evil Twin Construction

An evil twin has been set up on a laptop with two USB wireless network adapters. The laptop has 8GB RAM and I7 processors running Ubuntu 16.04LTS system. One of the wireless cards is Tenda W311M acting as an evil twin which deceives users into connecting it, the other one is TP-LINK WN722N for transmission of packets to legitimate AP. In order to avoid interference of two 2.4Hz USB wireless cards, Tenda wireless card is connected by a USB extension line to the laptop for extending distance between two WNICs.

We used Hostapd, Udhcpd and Iptables to set up a rogue AP-Hostapd for construction of wireless access points, Udhcpd for DHCP server and Iptables for retransmission of packets. TP-LINK wireless card connects the legitimate AP while Tenda wireless card releases wireless signal of the same SSID with it.

B. Wireless Traffic Capture

Because of different APs working in different channels at most cases, monitoring different channels with two wireless cards synchronously is more accurate comparing with frequency hopping using one wireless card. We choose two onboard WNICs (one Realtek PCIe GBE Family Controller and one Ralink RT3290), which performed best in previous experiments. Aircrack suite has been used to capture wireless traffic. Laptops with Airmon-ng and Airodump-ng of aircrack can easily capture wireless packets in specific channel.

C. Traffic Analysis

We wrote a script in ET-spotter with PyShark library and Matplotlib library for the purpose of analyzing and filtering packets to get analytical results. The script initially imports all frames of two APs with the same SSID. Data frames sent by target APs which have not been retransmitted are reserved in new array by filter. PyShark library has the same filter language with Wireshark.

Then we called interfaces of Matplotlib which is a 2D plotting library for Python to plot effective data frame figures. After computations of correlation coefficient using Numpy library, MAC address of the possible evil twin can be distinguished according to output results.

VI. Results and Discussion

In this section, we have done extensive experiments to evaluate the detection accuracy and efficiency of our approach. Our experiments were set up in a university campus with more than 20,000 students. To simulate evil twin attack scenario, we configured an evil twin on a laptop as described in 5.1. It has the same SSID with a legitimate campus AP generating a good RSSI to victim users between 80% and 100%. One of the laptop wireless cards was configured as the AP part of the evil twin, and the other one connected legitimate campus AP pretended to be a normal user. Based on ET-spotter, we have analyzed large quantities of measured results to get a empirical TSV (0.56) under the experimental environment with 5-12 legal AP and 10-40 wireless users. We enumerate and analyze one of the typical experiments in subsection 6.1. The specific experiment parameters are respectively shown in Table I.

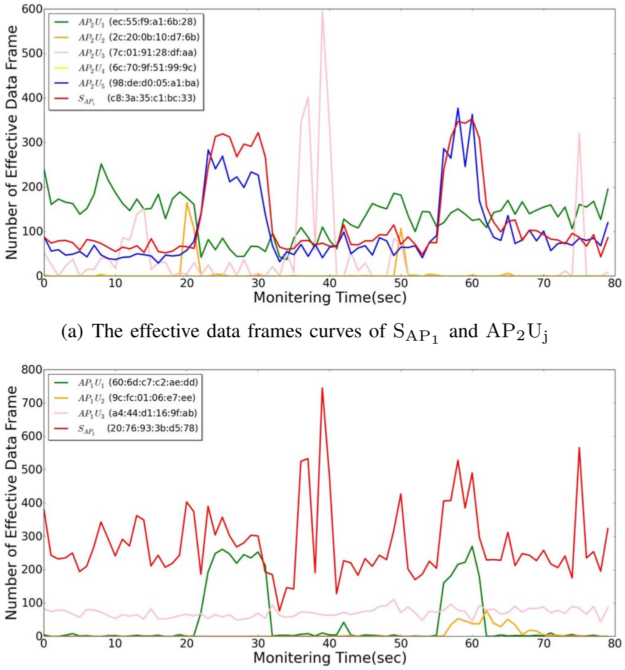
TABLE I: Detailed experiment parameters for 6.1

NoA[a]	NoU[b]	NoV[c]	RSSI of legitimate AP	RSSI of Evil Twin
15	5	3	85%	90%

[a] means the number of all wireless users in current WLAN
[b] means the number of wireless users associated with legitimate AP
[c] means the number of victim users associated with evil twin

A. Results

The curves of S_{AP_1} and AP_2U_5 in Figure 7(a) are very similar in both quantity and trend, and the correlation coefficient between them is up to 92%. Other correlation coefficients are shown in 7(b). It is obvious that AP_2U_5 (98:de:d0:05:a1:ba) forwarded effective data frames received by AP_1 (c8:3a:35:c1:bc:33). Thus, AP_1 is the malicious signal release part for evil twin, and AP_2U_5 was deliberately disguised as an normal user associated with legitimate AP_2 (20:76:93:3b:d5:78) to forward users' packets. More correlation coefficient between target APs and users are listed in Table II and Table III.



(a) The effective data frames curves of $\mathrm{S_{AP_1}}$ and $\mathrm{AP_2U_j}$

(b) The effective data frames curves of $\mathrm{S_{AP_2}}$ and $\mathrm{AP_1U_j}$

Fig. 7:

TABLE II: Person correlation coefficient between $\mathrm{S_{AP_1}}$ and $\mathrm{AP_2U_j}$

Target AP	$\mathrm{AP_2U_j}$				
	$\mathrm{AP_2U_1}$	$\mathrm{AP_2U_2}$	$\mathrm{AP_2U_3}$	$\mathrm{AP_2U_4}$	$\mathrm{AP_2U_5}$
$\mathrm{S_{AP_1}}$	-0.258	0.110	-0.182	0.07	**0.928**

TABLE III: Person correlation coefficient between $\mathrm{S_{AP_2}}$ and $\mathrm{AP_1U_j}$

Target AP	$\mathrm{AP_1U_j}$		
	$\mathrm{AP_1U_1}$	$\mathrm{AP_1U_2}$	$\mathrm{AP_1U_3}$
$\mathrm{S_{AP_2}}$	0.281	0.152	0.018

B. Evaluation of Detection

We evaluate the effectiveness of ET-spotter with some existing detection approaches shown in Table IV. Four valuable factors have been taken into consideration to analyze the performance of the existing detection approach. Our proposed client-based approach allows users to detect evil twin attacks independently in real time, which is an obvious advantage over admin-based methods, such as Radio Frequency method [14] [5] [2] and Traffic Monitor [16] [21] [18] [19] [20]. Actually, the cost of this method is very low, because it only requires the users devices as well as an additional wireless network adapter. Some expensive approaches, like [14] [5] [2], rely on installing sensors in a large scale wireless networks. Our approach is also lightweight enough to directly perform on the user's mobile devices. However, the methods based on hardware fingerprint features, such as clock skew [9] [11] and Radiotap length [6], require dedicated specialized hardware for measurement and thus cannot be performed by regular devices such as laptops or smartphones. Because our method is based on getting statistics of the effective data frame, rather than analyzing upper protocol field [8], thus regardless of whether the AP is encrypted, our method is applicable. Furthermore, our method can effectively detect the wireless network environment whether contains evil twins about 60s. Compared with the active detecting method [4], our method don't require to connect any AP or fill any login information when detecting.

TABLE IV: Comparison with existing detection approaches

Approach	Client-based	Passive	Non-hardware based	Accuracy
Radio Frequency		✓		98%
Traffic Monitor		✓	✓	99%
Clock Skew	✓	✓		84%
RSS	✓	✓		93%
Radiotap Length	✓	✓		N.A.
Active Behavioral Fingerprinting	✓		✓	N.A.
Data Frames Statistics	✓	✓	✓	96%

C. Limitation

Although above results show that our approach, Data Frames Statistics, 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 the evil twin. The victim user who is associated with evil twins should surf the Internet such as browse website, watch videos, etc. If victim user only connecting the evil twin instead of using it, it is difficult for ET-spotter to identify the evil twin attack by statistical data frames 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 a pluggable wireless network card. Nevertheless, we are trying to use one wireless adapter to solve the above limitation.

VII. Conclusion

There is always a network security threat that wireless users are vulnerable to be attacked by evil twins in WLANs so, in this paper, we proposed a lightweight client-side approach to protect wireless users from connecting such evil twin as well as locating them. Although there are several existing techniques to detect evil twin, some of them not efficient, lack accuracy, and most of them are admin-side. We implemented a prototype system, ET-spotter, on Linux operating system. ET-spotter not only can detect evil twin attack accurately and timely, but also can give the location of evil twin efficiently.

This paper makes the following contributions:

1) We proposed a lightweight client-based evil twin detection approach, which contains several advantages mentioned above.
2) We implemented our approach into a python tool, ET-spotter, on Linux system. Extensive experiments demonstrate the accuracy and effectiveness of our approach.

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] C. Arackaparambil, S. Bratus, A. Shubina, and D. Kotz. On the reliability of wireless fingerprinting using clock skews. In *ACM Conference on Wireless Network Security*, pages 169–174, 2010.

[2] 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. In *International Conference on Mobile Systems, Applications, and Services*, pages 1–14, 2006.

[3] P. Bhatia, C. Laurendeau, and M. Barbeau. Solution to the wireless evil-twin transmitter attack. In *Fifth International Conference on Risks and Security of Internet and Systems*, pages 1–7, 2010.

[4] S. Bratus, C. Cornelius, D. Kotz, and D. Peebles. Active behavioral fingerprinting of wireless devices. In *ACM Conference on Wireless Network Security, WISEC 2008, Alexandria, Va, Usa, March 31 - April*, pages 56–61, 2008.

[5] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless device identification with radiometric signatures. In *ACM International Conference on Mobile Computing and NETWORKING*, pages 116–127, 2008.

[6] K. Elleithy and B. Alotaibi. A passive fingerprint technique to detect fake access points,. In *IEEE Wireless Telecommunications Symposium*, 2015.

[7] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu. A timing-based scheme for rogue ap detection. *IEEE Transactions on Parallel & Distributed Systems*, 22(11):1912–1925, 2011.

[8] 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*, 2015.

[9] S. Jana and S. K. Kasera. On fast and accurate detection of unauthorized wireless access points using clock skews. *Mobile Computing IEEE Transactions on*, 9(3):449–462, 2010.

[10] T. Kim, H. Park, H. Jung, and H. Lee. Online detection of fake access points using received signal strengths. In *Vehicular Technology Conference*, pages 1–5, 2012.

[11] F. Lanze, A. Panchenko, B. Braatz, and T. Engel. Letting the puss in boots sweat: detecting fake access points using dependency of clock skews on temperature. In *ACM Symposium on Information, Computer and Communications Security*, pages 3–14, 2014.

[12] F. Lanze, A. Panchenko, B. Braatz, and A. Zinnen. Clock skew based remote device fingerprinting demystified. In *Global Communications Conference*, pages 813–819, 2012.

[13] 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 Transactions on Information & System Security*, 11(2):2, 2008.

[14] N. T. Nguyen, G. Zheng, Z. Han, and R. Zheng. Device fingerprinting to enhance wireless security using nonparametric bayesian method. In *INFOCOM, 2011 Proceedings IEEE*, pages 1404–1412, 2011.

[15] H. Qu, L. Guo, W. Zhang, J. Li, and M. Ren. *Rogue Access Point Detection in Vehicular Environments*. Springer International Publishing, 2015.

[16] S. Shetty, M. Song, and L. Ma. Rogue access point detection by analyzing network traffic characteristics. In *Military Communications Conference, 2007. Milcom*, pages 1–7, 2007.

[17] Y. Song, C. Yang, and G. Gu. Who is peeping at your passwords at starbucks to catch an evil twin access point. In *Ieee/ifip International Conference on Dependable Systems & networks*, pages 323–332, 2010.

[18] W. Wei, S. Jaiswal, J. Kurose, and D. Towsley. Identifying 802.11 traffic from passive measurements using iterative bayesian inference. *IEEE/ACM Transactions on Networking (TON)*, 20(2):325–338, 2012.

[19] 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. In *ACM SIGCOMM Conference on Internet Measurement 2007, San Diego, California, Usa, October*, pages 365–378, 2007.

[20] W. Wei, B. Wang, C. Zhang, and J. Kurose. Classification of access network types: Ethernet wireless lan, adsl, cable modem or dialup? In *INFOCOM 2005. Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, pages 1060–1071 vol. 2, 2005.

[21] H. Yin, G. Chen, and J. Wang. Detecting protected layer-3 rogue aps. In *International Conference on Broadband Communications, Networks and Systems, 2007. Broadnets*, pages 449–458, 2007.