Hindawi
Security and Communication Networks
Volume 2019, Article ID 2718741, 10 pages
https://doi.org/10.1155/2019/2718741

Research Article

SLFAT: Client-Side Evil Twin Detection Approach Based on Arrival Time of Special Length Frames

Qian Lu, Haipeng Qu, Yuzhan Ouyang, and Jiahui Zhang

Department of Computer Science and Technology, Ocean University of China, Qingdao 266100, China

Correspondence should be addressed to Haipeng Qu; quhaipeng@ouc.edu.cn

Received 11 March 2019; Accepted 18 April 2019; Published 2 June 2019

Academic Editor: Angelos Antonopoulos

In general, the IEEE 802.11 network identifiers used by wireless access points (APs) can be easily spoofed. Accordingly, a malicious adversary is able to clone the identity information of a legitimate AP (LAP) to launch evil twin attacks (ETAs). The evil twin is a class of rogue access point (RAP) that masquerades as a LAP and allures Wi-Fi victims' traffic. It enables an attacker with little effort and expenditure to eavesdrop or manipulate wireless communications. Due to the characteristics of strong concealment, high confusion, great harmfulness, and easy implementation, the ETA has become one of the most severe security threats in Wireless Local Area Networks (WLANs). Here, we propose a novel client-side approach, Speical Length Frames Arrival Time (*SLFAT*), to detect the ETA, which utilizes the same gateway as the LAP. By monitoring the traffic emitted by target APs at a detection node, *SLFAT* extracts the arrival time of the special frames with the same length to determine the evil twin's forwarding behavior. *SLFAT* is passive, lightweight, efficient, hard to be escaped. It allows users to independently detect ETA on ordinary wireless devices. Through implementation and evaluation in our study, *SLFAT* achieves a very high detection rate in distinguishing evil twins from LAPs.

1. Introduction

With the rapid advance of wireless network techniques and wide spread of mobile devices, Internet usage has been converting from stationary computers with cables to mobile devices using wireless connections. People are accustomed to using the Wi-Fi technique for work, entertainment, shopping, paying and all aspects of life, regardless of their locations. Accordingly, the wireless local area network (WLAN) has become an integral part of our daily life. A wireless AP as a wireless access device utilizes radio waves to provide communications with users' devices and connects them to the Internet. Nowadays, in addition to universities and homes, more and more businesses are providing a complimentary Wi-Fi network in cafes, restaurants, airports, and hotels in order to attract consumers and provide them with better services [1, 2].

Although the wireless network area network (WLAN) greatly facilitates our work and life, it also brings a lot of security problems to wireless users [3, 4]. In past decades, various attacks have emerged against wireless networks. One of the most prominent issues is the rogue access point (RAP) that is a wireless AP installed on a network without any authorization from network administrators [5, 6]. To mount an evil twin attack, a malicious adversary should fake a RAP, which has the same Service Set Identification (SSID) with a legal access point (LAP), then, improving the Received Signal Strength Indication (RSSI) of evil twins or sending de-authentication frames to attract victims connecting the evil twin. Users lacking adequate security knowledge and awareness are vulnerable to be tricked by attackers, resulting in a series of grave consequences [7, 8]. Once a victim is deceived by the evil twin, all victims' traffic will be relayed through the evil twin; as a result, some sensitive information like passwords, credit card information can be easily stolen by attackers. An advanced adversary is also capable of manipulating DNS servers, controlling routings, and initiating other phishing attacks, e.g.,fake an online payment webpage [9, 10].

Worse still, launching an ETA is quite simple for an adversary. Because some software and deployable tools are freely available and quite easy to use even for the person without experience and professional skills, generally, there are two ways an adversary can use to access the evil twin to the Internet. The first is called ETA using LAP's Internet access.

For such type of ETAs, two Wireless Network Interface Cards (WNIC) are required. One WNIC is used to imitate a normal wireless user and associate with the LAP, and the other one is exploited to release the Wi-Fi signal of evil twin for attracting victims. The second type is called ETA using mobile Internet access. In such kind of ETAs, malicious adversaries can share their own cellular network (e.g. 4G) broadband to relayed victims' traffic to the Internet, instead of relying on a LAP. In both types of ETAs, adversaries act as an intermediary and easily conduct a Man-in-the-Middle (MITM) attack [11].

Its severity has caught a remarkable amount of attention from media and researchers. In this paper, we put forward a novel client-based solution specifically against ETA using LAP's Internet access, achieving a very high detection rate. Our detection technique makes the following contribute to the field of WLANs security:

(i) We propose a passive client-based detection mechanism that determines evil twin's forwarding behavior by comparing arrival time of special length data frames. Our approach has the following properties: (1) Client-side and passive approach, (2) Not require to connect suspicious AP during detection, (3) Suitable for open and encrypted networks, (4) Independent of dedicated devices, (5) Independent of upper layer protocol details, and (6) Hard to be escaped by an attacker.

(ii) We have implemented our approach in a prototype system called ETD-SLFAT. Extensive experiments have been done to evaluate our tools in real network environments with different experiment parameters, which achieves outstanding performance.

The remainder of the paper is organized as follows. Section 2 overviews the related work. Section 3 describes the attack model and the basic idea of the proposed mechanism. Then, *SLFAT* is detailed in Section 4. In Section 5, we evaluate the performance of *SLFAT* in real-world experiments. The analysis, limitations, and future work are discussed in Section 6. Finally, the paper is concluded in Section 7.

2. Related Work

Much work has been done by researchers to address the evil twin attacks. To have more insight into these techniques, we classify them into two categories based on who is responsible for detecting evil twin attacks.

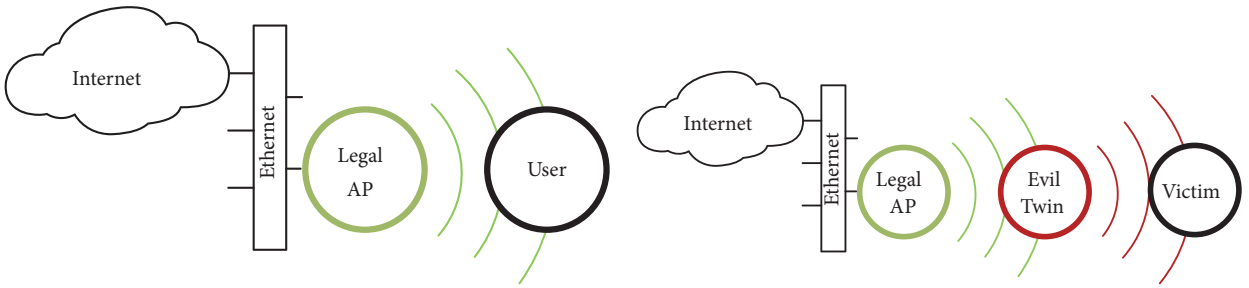
2.1. Admin-Side Approaches. The first category is the admin-side detection approach that the network operator is the one charge of identifying ETAs and preventing users to connect them. Administrators usually create an authorization list through prior information collection, which records LAPs' identity information such as SSID, BSSID, location, and AP hardware. During the detection, surrounding APs are scanned by a network administrator to calculate their fingerprints, then the fingerprints are compared with the authorized list to determine the detection result. Thus, many researchers are dedicated to finding out which information can be used as a fingerprint uniquely to determine an AP. In [12–14], they monitor the Radio Frequency (RF) airwaves and collect extra information at the core network to generate APs' fingerprints. Some researchers take advantage of the AP's fixed physical location to identify malicious APs, but this method can easily lead to a false negative when an evil twin is set up near the LAP. In addition, the malicious AP an attacker prepared is usually different from the legitimate one; this makes their WNIC chips different. Therefore, such chip information extracted from wireless frames can also be used as a device fingerprint to help the operator recognize the evil twin.

Another ETA detection scheme that belongs to admin-side category is the clock skew detection method. Jana et al. [15] firstly introduce clock skews into 802.11 domain and propose that the clock skew of each AP, extracted from Timing Synchronization Function (TSF) timestamps in beacon frames, is the unique and unavoidable physical fingerprint. The clock skew is caused by tiny yet observable speed deviations of the crystal oscillator-based clocks. Through calculating target AP's clock skew and comparing with feature database, an evil twin can be distinguished from LAPs. Afterwards, these approaches are enhanced in [16, 17]. Particularly, Lanze et al. combine clock skew with device-intrinsic temperature that greatly improves the detection accuracy [18].

Obviously, such admin-side approaches are limited because authorization lists or feature database records the LAP are essential in the detection process. If not, these methods will fail. Moreover, several solutions require administrators to deploy wireless sensors in a wide range of wireless networks or collect traffic at a central aggregation, which is very costly and complicated. In summary, this category has several, or all, limitations about requirements, expenses, and instantaneity, so these approaches are not suitable for mobile users independently to detect ETA in real time.

2.2. Client-Side Approaches. The second detection category is a client-side detection scheme that refers to users preventing themselves from ETAs without any help from the administrator. Many researchers propose client-side ETA solutions based on a phenomenon called evil twin hop, since the evil twins need to increase an extra hop to offer its Internet connection to wireless users. In [19], Han et al. proposed a timing-based detection approach that uses the Round Trip Time (RTT) between the client and the DNS server to identify whether a given AP is legitimate. The evil twin can be detected because it introduces an extra time delay between victims and the LAP. However, RTT-based approaches cannot provide an accurate detection because many reasons, such as interference and collision, can add a delay on RTT and result in a false positive.

Another evil twin hop detection mechanism is presented in the studies of [20, 21]. The authors modify the client's driver to measure Interpacket Arrival Time (IAT) between two consecutive packets sent from the same server as the detection statistic to distinguish one-hop and two-hop wireless channels. If the IAT exceeds the pre-trained threshold,



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

Figure 1: Illustration of normal and attack network topologies.

it indicates that the connected AP is an evil twin using two-hop channel. However, such methods belong to active detection methods and require wireless users to associate with suspect APs during detection, which may increase the risk of information leakage. Moreover, in order to get the knowledge of Server IAT, extensive training should be done.

In [7, 22], Lu et al. present a lightweight detection solution depending on the high correlation of effective data frames (EDFs) forwarded by an evil twin. This work filters EDFs sent by target APs, gets EDFs statistics of target APs and each connected user, and calculates the correlation coefficient between each EDF statistic. An evil twin attack can be determined if a correlation coefficient exceeds the preset threshold. This method is simple yet effective. However, if an attacker realizes the method, they can initiate evasion attack to escape ETA detection. The attacker can reduce the correlation of the evil twin's forwarding behavior by deliberately consuming the bandwidth on the evil twin side, which will lead to a low detection rate.

In [23], a novel watermarked packet based detection scheme is proposed. This method randomly connects a target AP and actively sends a watermarked packet to a dedicated server, then continuously switches and scans other Wi-Fi channels searching any transmission of the watermarked packet. Although this method achieves high accuracy, it requires an external server on the Internet and assumes the server is authentic. Afterwards, such method is improved by Nakhila et al. [24]; they overcome several security vulnerabilities in Open WiFiHop. However, an external server is still required.

The study of [25] prevents wireless users from ETAs based on protocol modification. Kumar et al. propose that a new identifier 'COUNT' can be added to the information list of client side and AP side. Such identifier records the number of successful connections for each client and AP. Before a client connects to a target AP, a malicious AP can be determined if the values of 'COUNT' stored in the client side and the AP side are different. However, since this solution relies on the adapted protocol, it is not practical to change existing drivers and firmware in a large scale.

Hsu et al. propose a client detection scheme that uses the acknowledgment number and sequence number in an IP packet as a basis for determining whether a forwarding behavior exists in a surrounding wireless network [26]. If the same acknowledgment number and sequence number appear multiple times, an ETA warning is issued to wireless users. However, since this method relies on the details of the IP packet header, it is only suitable for open wireless networks. Moreover, such method uses one network card to sniff wireless traffic, so only the evil twin working on the same channel as the LAP can be detected.

3. Problem Statement and Principle

The ETA has been an unsettled problem for decades in WLANs. In this section, we introduce the wireless network background and analyze the basic observation.

3.1. Background. In a wireless network, wireless APs periodically broadcast their SSIDs in order to make users discover and connect to them. Yet the SSID of a LAP is easy to be spoofed by a malicious adversary. By cloning the same SSID with a target LAP, the attacker can set up an evil twin to disguise as the legitimate one. Unfortunately, common users are not able to distinguish the LAP from the evil twin, so that innocent clients may automatically associate with the evil twin when they receive a better SSID from it.

Figures 1(a) and 1(b) show the network topology of a normal model and an attack model, respectively. In Figure 1(a), a legal AP utilizes radio waves to communicate the wireless client and then connect them to the Internet via Ethernet; on the other hand, Figure 1(b) illustrates the attack scenario where an evil twin is inserted between the legal AP and victims. It is also capable of providing victims with Internet access through the legal AP. In this case, when the victim user tries to access the remote server, actually the information will be intercepted by the evil twin because it relays the whole traffic between the LAP and victim like a middleman.

3.2. Baisc Idea. In order to achieve our objective described in Section 1, we need to explain, in this paper, what features can be utilized to determine the ETA on the user side. To answer this question, we present a recapitulate about our detection principle, and the details will be explained in Section 4. *SLFAT* discovers the ETA based on malicious forwarding behavior. As mentioned above, the evil twin needs to rely on a LAP to provide Internet services for victims and forwards

all network packets between the LAP and victims. Thus, the forwarded data frames will be bound to present a significant correlation in time [22].

Unlike [22], we use the same special length effective data frames (SL-EDF) emitted by target APs, instead of the quantity statistics of the EDF, as an indicator to determine the malicious forwarding behavior. In order to quickly and effectively distinguish malicious forwarding behavior, *SLFAT* firstly monitors the frames emitted by the two (or several) target APs, filters out the SL-EDF shared by the two suspect APs, then extracts their arrival time generated on the detection node. If such pair of SL-EDF is relayed by the evil twin, their arrival time received at the detection node should be approximately equal, and a reasonable time interval between them should exist because of the forwarding behavior. After extracting and comparing multiple groups of the arrival time in SL-EDF sent by target APs, an ETA can be detected if multiple pairs of the arrival time in SL-EDFs present malicious forwarding behavior. The detailed detection method will be introduced in Section 4.

In a real environment, which factors may influence the detection result and how to avoid them? Under the real network circumstance, we must consider the fact that the phenomena of packet loss and packet delay are not rare events, especially in a multi-hop wireless network with high traffic load. Fortunately, the packet loss does not have any impact on our detection results because only the SL-EDFs shared by both target APs (evil twin or LAP) are needed by *SLFAT*. For packets delay, since we determined the ETA based on the arrival time of the SL-EDF sent by target APs, a time window in *SLFAT* is trained and set to distinguish the relayed SL-EDFs from most extraneous frames with coincident length. However, we cannot rule out that an adventitious frame with coincident length happens to fall into the time window, so multiple groups of SL-EDFs gathered in monitor stage are utilized for comprehensive evaluation. Eventually, malicious forwarding times of SL-EDFs can be used to distinguish between the LAP and the evil twin. Furthermore, an attacker is impossible to frequently drop or delay packets to avoid dropping the SL-EDF in the time window because it will directly lead to an unstable and low-speed Wi-Fi service and lose its attraction to the victims.

4. The Proposed Mechanism

After giving the network background and basic idea, we introduce our client-based detection technique, *SLFAT*, that satisfies all the advantages mentioned in Section 1. *SLFAT* focuses on detecting the ETAs which uses the LAP's Internet access. In this section, we present the overview and detail the four component of *SLFAT*.

4.1. Framework Overview. The goal of *SLFAT* is to find suspicious forwarding behavior between wireless nodes. We regard such forwarding phenomenon as an indicator of ETAs. The proposed mechanism consists of four components. The four components, depicted in Figure 2, are Monitor component, Filter component, Processing component, and Judgment component. The first three modules enable clients to search for malicious forwarding behavior, and the last phase helps us determine ETAs and send its information to the clients and network administrators. The detection device we need is an ordinary laptop with an extra WNIC. Here, we give an overview of the component in *SLFAT* and the detailed procedures are further explained in following subsections.

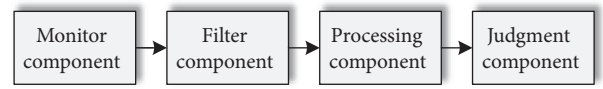


Figure 2: The four components of the proposed mechanism.

Monitor Component. This module is used to find surrounding active APs and monitor the 802.11 frames. To capture the wireless frames, the two WNICs on the detection client are set to monitor mode. Such frames are the input to the filter component.

Filter Component. The filtering module is responsible for filtering and obtaining the SL-EDFs to be processed in the processing module. This step includes three filtering operations to select suitable SL-EDFs shared by both target APs.

Processing Component. This component is the core part of *SLFAT*, which is used to judge malicious forwarding of SL-EDFs and record forwarding information. Based on extracted arrival time in SL-EDF and a predefined time window, a forwarding count is introduced to record the number of forwarding SL-EDFs between the target AP and the user, which reveals malicious forwarding behavior of the evil twin.

Judgment Component. The judgment component is responsible for determining ETAs and issuing ETA alarms. According to forwarding counts and a predefined threshold, an ETA can be determined.

4.2. Monitoring 802.11 Frames. In monitor component, the WNICs are set to *monitor mode* and are utilized to sniffing wireless frames emitted by target APs. We capture the beacon and request response frames through WNICs on detection client to generate a Wi-Fi list. The list presents information about active APs working in the surrounding wireless network, containing the SSID, MAC address, working channel, encryption method, and so on. By checking the list, we mark the multiple APs with the same SSID yet different MAC address as target APs. It is likely that an evil twin interfused in them disguises as a LAP.

For a clear description, we assume that there are two target APs, AP_1 and AP_2 respectively. The evil twin will be set in different channel with the LAP to avoid mutual interference at most cases. Therefore, we use two WNICs which work on monitor mode to synchronously sniff the two different channels. This mode allows WNIC monitor transmitted frames without associating with any APs. After a period of passive monitoring, we can get $file_1$ and $file_2$

1: **for all** $file_i$ **do**
2: Filtering out c_f, m_f, r_f and obtaining d'_f as file'_i
3: Selecting special length d' observed less than twenty times
4: Extracting SL-EDFs' Len_i, $ArrTime$, $DesMAC$;
5: Restoring the information in $Dict_{AP_i}$
6: **end for**
7: Deleting the different Len_i in $Dict_{AP_1}$ and $Dict_{AP_2}$
8: Obtaining the $Dict_{AP_1}$ and $Dict_{AP_2}$ restoring the same length SL-EDF

Algorithm 1: Filtering SL-EDFs sent by AP_1 and AP_2.

that respectively record the wireless frames sent from AP_1 and AP_2. The captured frames consist of control frames c_f, management frames m_f, data frames d_f. The control frame is a short message that informs the device to start or stop the transmission. The management frame is mainly used to negotiate and control the relationship between the station and the AP. And the data frame is actually forwarded between wireless nodes, so d_f may be an indicator of suspicious forwarding behavior.

4.3. Filtering Special Length Effective Data Frames. To obtain SL-EDFs sent from target APs, the filter component is designed to perform three filtering operations as shown in Algorithm 1. First, based on the MAC addresses and frame type, we filter the downstream EDFs d'_f emitted by the target AP. EDFs refer to the downstream data frames sent from target APs, which exclude c_f, m_f, and retransmitted data frames r_f. After preliminary filtration, we can get file'_1 and file'_2 that record the EDFs sent by AP_1 and AP_2 respectively.

Second, in order to efficiently find the forwarding behavior, we require to search for the least observed SL-EDFs. We scan the file'_1 sent by AP_1, select the special length d'_f observed less than twenty times, extract their destination address and arrival time, and restore them in a dictionary $Dict_{AP_1} =< Len_i, Info_i >$. Each item in $Dict_{AP_1}$ is a key-value pair. The key is the length of d'_f and the value is another dictionary $Info_i =< ArrTime, DesMAC >$ where the key is the arrival time generated by received WNIC and the DesMAC is the destination MAC address in d'_f. To determine the least observed special length, we sort $Dict_{AP_1}$ from less to more according to the number of length observation. In addition, the same process is performed on $file'_2$. After this step, we can obtain two ordered dictionaries $Dict_{AP_1}$ and $Dict_{AP_2}$ storing the information of special length d'_f.

Third, we select the SL-EDFs shared by AP_1 and AP_2. By comparing the Len_i in $Dict_{AP_1}$ and $Dict_{AP_2}$, the items with same Len_i in both dictionaries are retained and different items are deleted. This is because we just need to use the items coexisting in both dictionaries to determine the forwarding behavior. For instance, we assume that the least observed length sent by AP_1 is Len_a, Len_b, Len_c, Len_d. Meanwhile, the least observed length sent by AP_2 is Len_a, Len_c, Len_e, Len_f. Through comparison, the SL-EDFs shared by $Dict_{AP_1}$ and $Dict_{AP_2}$ are Len_a, Len_c. In fact, there are multiple groups of such SL-EDFs will be generated in the real environment. Here, we just simplify the description for convenience. The adequate groups of EDFs will be used to determine forwarding behaviors in next phase.

4.4. Malicious Forwarding Behavior Assessment. In processing component, SL-EDFs obtained in filter module are processed to assess the malicious forwarding behavior. Because the evil twin utilizes LAP's Internet access, it relays the traffic from LAP; that is, the EDFs sent from the evil twin to victims are come from LAP. Therefore, in the downstream traffic, the time for a frame sent from evil twin to the victim should be latter than the time for the same frame sent from the LAP to evil twin. In addition, the time delay between them should be within a reasonable and the smallest possible range to ensure a fast and stable network for attracting victims. Correspondingly, the arrival time, ArrTime_1 and ArrTime_2, of a same length pair of SL-EDFs should follow this rule. Although network load may affect a frame's arrival time, this does not impact our method because *SLFAT* only needs to find several pairs of approving SL-EDFs to determine the forwarding behavior. We can guarantee that this factor will not affect our method.

Algorithm 2 shows the processing component. For $Dict_{AP_1}$ and $Dict_{AP_2}$ obtained by the filter component, we select each item with the same length in both dictionaries and extract their arrival time, $ArrTime_1$ and $ArrTime_2$. Then, we calculate $\delta t = ArrTime_2 - ArrTime_1 > 0$. δt is defined as the arrival time interval between a same length pair of SL-EDF sent by two target APs. δt is used to determine whether such pair of SL-EDF is emitted at a extremely similar time and whether a suspicious forwarding behavior exists. If $|\delta t|$ is less than a predefined time window w, we consider that there may be a forwarding operation between target AP_1 and AP_2. Then we increase the forwarding number $n_{(p,q)}$ where q is the source address of the frame that arrives later and p is the destination address of the former frame. The purpose of such forwarding count is to find out the two MAC addresses used by the suspicious evil twin. An increase in $n_{(p,q)}$ indicates that the frame sent by a target AP to the user p is replayed by q, or it is an extraneous frame with coincidence length

1: **for all** items in $Dict_{AP_1}$ and $Dict_{AP_2}$ **do**
2: Selecting a pair of d' shared in $Dict_{AP_1}$ and $Dict_{AP_2}$
3: Extracting $ArrTime_1$ and $ArrTime_2$
4: Calculating $\delta t = ArrTime_2 - ArrTime_1$
5: **if** $|\delta t| \leq w$ **then**
6: Adding $n_{(p,q)}$
7: **end if**
8: **end for**
9: Output all $n_{(p,q)}$

Algorithm 2: Comparing Arrival Times of SL-EDFs.

1: **for all** $n_{(p,q)}$ **do**
2: **if** $n_{(p,q)} \geq$ TSV **then**
3: Triggering an ETA alert and send p, q
4: **else** $\{n_{(p,q)} <$ TSV$\}$
5: Prompting both APs are safe
6: **end if**
7: **end for**

Algorithm 3: Evil Twin Identification and Alerting.

that happens to fall into the time window. After processing adequate pairs of SL-EDFs, we can get all $n_{(p,q)}$, recording the forwarding number between different MAC addresses.

4.5. Evil Twin Identification and Alerting. In judgment component, ETAs can be identified according to $n_{(p,q)}$. As shown in Algorithm 3, if each $n_{(p,q)}$ is less than our default threshold value (TSV), it means that all $n_{(p,q)}$ are within the normal range. There is no malicious forwarding behavior between AP_1 and AP_2, i.e., no evil twins; otherwise, if there is a $n_{(p,q)}$ that exceeds the threshold, an ETA detected target APs. Consequently, p of $n_{(p,q)}$ is one WNIC that the evil twin used to impersonate a normal user and deceive the LAP's Internet connection, and q is the other WNIC that is responsible for releasing evil twin's signal. Finally, such information and ETA alarm will be sent to users and the administrator, and the MAC addresses can help admin to find and cut off the evil twin's connection to the LAP.

5. Evaluation

In this section, we first introduce our experimental setup. Then, the detection result is described in detail. Ultimately, the effectiveness and time efficiency of *SLFAT* are, respectively, presented.

5.1. Experimental Setup. We conduct extensive experiments under the network environment of our university campus. The experimental testbed is built including two subgroups: normal scenario and attack scenario. The normal scenario consists of a LAP and several wireless devices. The LAP is a TP-LINK WDR5620 Wi-Fi router, and it coordinates the wireless users and connects them to the Internet through the wired network as depicted in Figure 3.

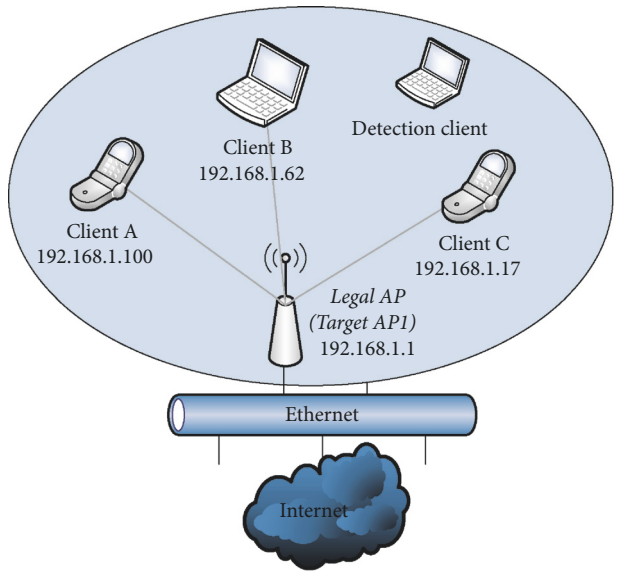


Figure 3: Experimental setup for normal scenario.

On the other hand, the attack scenario shown in Figure 4 contains a LAP, some wireless clients and an evil twin. The evil twin is set between the LAP and victims. Specifically, we use the WiFi Pineapple NANO (https://www.wifipineapple.com/pages/nano) to simulate the evil twin in the attack scene. The Pineapple is a ready-made machine that is specifically designed for wireless security penetration testing. For researchers and adversaries, it is a popular and convenient

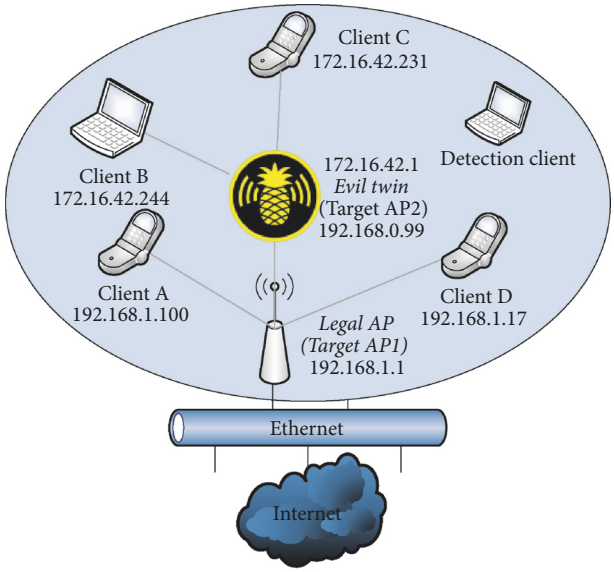


Figure 4: Experimental setup for attack scenario.

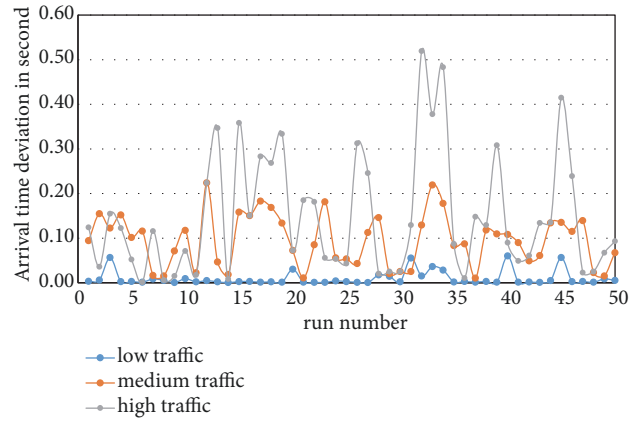


Figure 5: δt between a same length pair of SL-EDFs.

tool that helps them deploy a rogue AP. Our WiFi Pineapple NANO has two WNICs. One (Atheros AR9331) acts as an evil twin alluring victims' connection, and the other one (Atheros AR9271) pretends to be a normal user connecting LAP for relaying the traffic between victims and LAP. Compared to manually configuring evil twins using tools such as Hostapd, Udhcpd, and Iptables, the WiFi Pineapple greatly facilitates the process of building evil twins.

Additionally, in both scenarios, we take advantage of a laptop and an extra USB WNIC as the detection device. The laptop has 4 GB RAM and Intel Core2 T6570 processor running Kali Linux 4.17.0 system. The onboard WNIC is Ralink RT3290 and the additional USB WNIC is TP-LINK WN722N. We utilize the two WNICs to synchronously monitor different channels, which makes the detection results more accurate. A prototype detection system, ETD-SLFAT, is developed for ETA detection. ETD-SLFAT is installed on the detection device to provide real-time detection for users.

5.2. Training and Results. To set appropriate thresholds of the time window w and the forwarding count $n_{(p,q)}$, we have conducted 150 groups of experiments under three different traffic conditions. We have measured the arrival time interval δt of each pair of SL-EDFs produced by the evil twin and measured the different forwarding count $n_{(p,q)}$ produced by the evil twin and extraneous frames. Through 150 groups of experiments under different traffic conditions, we also deduce the influence of network traffic on the performance of our tool (ETD-SLFAT). Because our principle is based on the arrival time interval δt between the same length pair of SL-EDF to determine the forwarding behavior, δt is a key threshold value to differentiate ETAs from LAPs. To simulate three different traffic conditions, several wireless users are associated with the LAP to generate constant traffic, i.e., low (2Mbps), medium (8Mbps), and high (16Mbps) traffic network environments. The experimental setup is described in Section 5.1.

In each network traffic scene, we have performed 50 groups of experiments, i.e., in a total of 150 groups in three network conditions. We select the maximum δt in each experiment to generate Figure 5. Figure 5 shows 150 δt in such three network conditions. In low traffic scenario, the average value of δt between the same length pair of SL-EDF is about 0.00427 seconds with standard deviation of 0.01596 seconds. In a medium traffic environment, the average value of δt is about 0.05944 seconds with standard deviation of 0.05732 seconds. Accordingly, it shows the average δt is about 0.10871 seconds with standard deviation of 0.14974 seconds in high network traffic scene. The experimental result shows that the average δt increases with the increase of network traffic. It also reveals that, in our experimental environment, every arrival time interval δt between the same pair of SL-EDF in our experiment is less than 0.6 seconds, so we set the time window threshold to 0.6 seconds, i.e. $w = 0.6$s.

According to the threshold of the time window ($w = 0.6$s), we statistically calculate the SL-EDFs' forwarding frequency appearing within w among the 150 sets of experiments and obtain the Figure 6. Figure 6 is a scatter plot depicting 300 points. In the figure, the abscissa represents the run number of experiments, and the ordinate represents the statistical value in each experiment. Each X value in the figure corresponds to two Y values, i.e., Y_1 and Y_2 ($Y_1 < Y_2$). That is, each experiment corresponds to 2 points in the graph. Y_2 indicates the number of times that the evil twin forwards SL-EDFs. Y_1 indicates that maximum times of innocent $n_{(p,q)}$ that has extraneous frames with coincident length falls into the time window. Obviously, there is a gap between each pair of Y_1 and Y_2. This gap can be exploited to distinguish between the forwarding behavior of the evil twins and the extraneous frames with coincident length. To describe the ideal threshold value of $n_{(p,q)}$, we denote the minimum frequency, among our 150 groups experiments, of true malicious forwarding SL-EDF produced by evil twin as *ETFreq_min*. Meanwhile, we denote the maximum frequency, among our 150 groups experiments, of extraneous frames with coincident length as *CoinFreq_max*. We consider that the

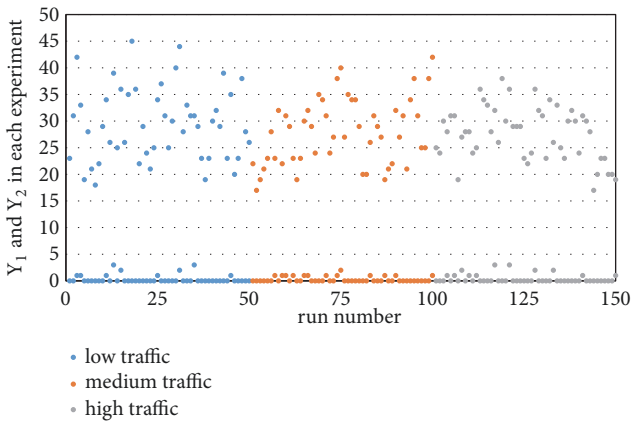


Figure 6: The maximum times of extraneous frames with coincident length falls into the time window (Y_1) and the times of evil twin forwards SL-EDFs (Y_2) in 150 groups of experiments.

ideal threshold value of $n_{(p,q)}$ is the average of the deviation between the *CoinFreq_max* and *ETFreq_min* as Equation (1).

$$TSV = \frac{CoinFreq\_max + ETFreq\_min}{2} \quad (1)$$

We enumerate and analyze a typical experiment result (Exp.1). The profiles of corresponding experimental parameters are presented in Table 1. During the detection process, four victims and five normal users connected to the target APs, conducted the most common Internet behaviors like watching video and listening to music. The suspicious forwarding times $n_{(p,q)}$ for $MAC < p, q >$ are shown in Table 2. Note, p represents a suspicious MAC address that the evil twin used to impersonate a normal user while q denotes the other suspect MAC address responsible for releasing evil twin's signal. For the convenience of expression, we use the last 2 bytes of the MAC address to represent a complete address. Obviously, in Table 2, the $n_{(p,q)}$ of MAC<8665, B6C8> is 23, which are significantly higher than others. This indicates AP_2 (02:03:7f:bf:b6:c8) relayed the SL-EDFs which was sent from AP_1 to the malicious user (U_{mal}) (00:11:7f:12:86:65). Thus, target AP_1 is LAP, while U_{mal} and AP_2 are two MAC addresses of the evil twin; that is, AP_2 is the malicious signal release part for evil twin, and U_{mal} is the other part that pretends to be a normal user to connect legal AP_1.

5.3. Effectiveness. In order to evaluate the effectiveness of ETD-SLFAT, we conducted additional 450 sets of experiments under different traffic conditions in our university campus. The experimental accuracy results are shown in Table 3. They indicate that ETD-SLFAT can achieve 100% detection rate without false positives in low and medium traffic conditions. In a high-traffic environment, the detection rate is about 97.33%. Because of the increase of queuing delay or transmission delay at the relayed node, a part of the SL-EDF emitted by the target APs may drop out of time window, resulting in false negatives. However, there is no false positive based on the evaluation results.

Table 1: Experiment parameters for Exp.1.

target AP1	fc:2f:ef:64:82:2a
target AP2	02:03:7f:bf:b6:c8
user number of LAP	5
victim number of ET	4
RSSI of LAP	-50
RSSI of Evil Twin	-36
network traffic statement	medium

Table 2: The experiment result for Exp.1.

$MAC < p, q >$	$n_{(p,q)}$
$MAC < 196A, B6C8 >$	0
$MAC <$ **8665, B6C8** $>$	**23**
$MAC < 822A, B6C8 >$	0
$MAC < AEDD, B6C8 >$	0
$MAC < 7AF2, B6C8 >$	1
$MAC < B334, 822A >$	0
$MAC < DFAA, 822A >$	0
$MAC < FC17, 822A >$	1
$MAC < 01DF, 822A >$	0

Table 3: Detection rate under different network traffic conditions.

Network traffic conditions	Low	Medium	High
Detection accuracy	100%	100%	97.33%

5.4. Time Efficiency. We also evaluated the time efficiency of ETD-SLFAT under different network traffic conditions. The total detection time consists of monitoring time and processing time. Through verification, the SL-EDFs collected in 24 seconds are enough to output the correct detection results. In our evaluation experiment, the number of LAP's users ranged from 4 to 7, while the victims associated with the evil twin ranged from 2 to 4. According to the experimental data, the time of SL-EDF processing and forwarding behavior evaluation is less than 10 seconds. Therefore, our algorithm can completely output the detection result in 34 seconds.

6. Discussion

In this section, the advantages and limitations of the proposed method and future work are discussed.

6.1. Analysis. Compared to existing evil twin attack detection methods, the proposed method has several advantages in terms of expenditure, robustness, detection rate, etc. First, unlike admin-side detection methods [12, 27], *SLFAT* is a passive client-side scheme and is able to provide a real-time detection service, which allows users to ensure their security in real time. Second, when the client is detecting, the user's device does not require to connect suspicious APs,

avoiding information leakage during the association. Third, our method does not depend on other dedicated equipment, such as additional servers [23] or detection devices [17]. We only need an extra wireless network card. Fourth, *SLFAT* does not depend on the details of the upper layer protocol. Thus, it is applicable whether wireless networks are encrypted or open.

SLFAT is difficult to be bypassed by an attacker who realizes our approach, which is an advantage compared with our previous work [7]. The work [7] is vulnerable to the evasion attack. Once an attacker has realized the detection method, it may try to reduce the correlation of the evil twin's forwarding behavior by consuming traffic at the evil twin end for avoiding detection. For such evasion attack, the detection rate of the previous work drops to 38%. *SLFAT* does not suffer from such attack because it depends on SL-EDFs that coexist on both communication paths. To prevent an attacker from bypassing detection, only those shared SL-EDFs with arrival time within the time window w are considered malicious forwarded frames. Based on such strict criteria, if the number of malicious forwarded frames exceeds the threshold, the forwarded nodes are determined as an evil twin.

The proposed method is able to distinguish evil twins from Wi-Fi repeaters. Wi-Fi repeaters are often applied to extend the wireless network coverage with the same SSID. The constituted Wireless Distribution System (WDS) enables wireless users to move around the entire WLAN and automatically connect to the AP with the strongest RSSI. But this technique makes ETAs more difficult to be detected for most detection approach. We find that in IEEE 802.11, when a repeater relays the traffic through LAP, the repeater will use all the four addresses fields in the header of 802.11 frames. This is different from the evil twin scenario. Because the evil twin uses a WNIC to camouflage normal wireless users, it only uses three address fields like a normal wireless user and LAP. Our ETD-SLFAT is able to distinguish the evil twin from Wi-Fi repeater by checking the number of used address fields in 802.11 frame header.

6.2. Limitation. Our proposed solution has two limitations. One is that, since ETD-SLFAT can detect the target APs working on different channels, we need two wireless network interface cards to simultaneously monitor the specified channels. In other words, in addition to the onboard WNIC in the user's mobile device, we also need another USB WNIC. Fortunately, it is very convenient for users to carry a USB WNIC, and some high-profile laptops already contain two built-in wireless network cards. The other one is that the proposed method focuses on detecting ETAs where the evil twin utilizes the LAP's Internet access.

6.3. Future Work. Our ETD-SLFAT shows an outstanding performance against ETA that uses the same gateway with LAP. However, due to the growth of cellular mobile networks, such as 5G networks, it is also increasingly popular for attackers to connect victims to the Internet through their own cellular broadband links. So, in the future, we will conduct further research on this kind of ETA that uses attackers' access networks.

7. Conclusion

In this paper, we propose a passive as well as lightweight client-side detection technique, *SLFAT*, to prevent wireless users from evil twin attacks. Our method has a wide range of applications because it works in both encrypted or open networks and does not require any dedicated equipment. Additionally, we implement our technique into a Python detection tool called ETD-SLFAT, and extensive experiments with different conditions in a real network environment have been done to prove its excellent accuracy and effectiveness.

Data Availability

The experimental data used to support the findings are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61379127), the National Natural Science Foundation of China (No. 61827810), the Fundamental Research Funds for the Central Universities (No. 201813021), and 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] W. Wei, S. Jaiswal, J. Kurose, and D. Towsley, "Identifying 802.11 traffic from passive measurements using iterative Bayesian inference," in *Proceedings of the INFOCOM 2006: 25th IEEE International Conference on Computer Communications*, pp. 1–12, Spain, April 2006.

[3] S. Shetty, M. Song, and M. Liran, "Rogue access point detection by analyzing network traffic characteristics," in *Proceedings of the Military Communications Conference, MILCOM 2007*, pp. 1–7, USA, October 2007.

[4] H. Yin, G. Chen, and J. Wang, "Detecting protected layer-3 rogue APs," in *Proceedings of the 4th International Conference on Broadband Communications, Networks, Systems, BroadNets*, pp. 449–458, USA, September 2007.

[5] B. Alotaibi and K. Elleithy, "Rogue access point detection: taxonomy, challenges, and future directions," *Wireless Personal Communications*, vol. 90, no. 3, pp. 1261–1290, 2016.

[6] W. Wei, B. Wang, C. Zhang, J. Kurose, and D. Towsley, "Classification of access network types: Ethernet wireless lan, adsl, cable modem or dialup?" in *Proceedings of the IEEE Computer and Communications Societies "INFOCOM 2005"*, vol. 2, pp. 1060–1071, IEEE, USA, March 2005.

[7] Q. Lu, H. Qu, Y. Zhuang, X.-J. Lin, and Y. Ouyang, "Client-side evil twin attacks detection using statistical characteristics of 802.11 data frames," *IEICE Transaction on Information and Systems*, vol. E101D, no. 10, pp. 2465–2473, 2018.

[8] C. D. Mano, A. Blaich, Q. Liao et al., "Ripps: Rogue identifying packet payload slicer detecting unauthorized wireless hosts through network traffic conditioning," *ACM Transactions on Information and System Security*, vol. 11, no. 2, p. 2, 2008.

[9] F. Lanze, A. Panchenko, I. Ponce-Alcaide, and T. Engel, "Undesired relatives: protection mechanisms against the evil twin attack in IEEE 802.11," in *Proceedings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet '14)*, pp. 87–94, ACM, Québec, Canada, September 2014.

[10] S. Bratus, C. Cornelius, D. Kotz, and D. Peebles, "Active behavioral fingerprinting of wireless devices," in *Proceedings of the 1st ACM Conference on Wireless Network Security (WiSec '08)*, pp. 56–61, ACM, Alexandria, Va, USA, April 2008.

[11] F. Lanze, A. Panchenko, I. Ponce-Alcaide, and T. Engel, "Hacker's toolbox: Detecting software-based 802.11 evil twin access points," in *Proceedings of the 2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, pp. 225–232, IEEE, January 2015.

[12] N. T. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric Bayesian method," in *Proceedings of the IEEE INFOCOM 2011*, pp. 1404–1412, China, April 2011.

[13] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM Annual International Conference on Mobile Computing and Networking (MobiCom '08)*, pp. 116–127, ACM, September 2008.

[14] P. Bahl, R. Chandra, J. Padhye et al., "Enhancing the security of corporate Wi-Fi networks using DAIR," in *Proceedings of the MobiSys 2006 - Fourth International Conference on Mobile Systems, Applications and Services*, pp. 1–14, Sweden, June 2006.

[15] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 449–462, 2010.

[16] C. Arackaparambil, S. Bratus, A. Shubina, and D. Kotz, "On the reliability of wireless fingerprinting using clock skews," in *Proceedings of the 3rd ACM Conference on Wireless Network Security (WiSec '10)*, pp. 169–174, ACM, Hoboken, NJ, USA, March 2010.

[17] F. Lanze, A. Panchenko, B. Braatz, and A. Zinnen, "Clock skew based remote device fingerprinting demystified," in *Proceedings of the 2012 IEEE Global Communications Conference, GLOBECOM 2012*, pp. 813–819, USA, December 2012.

[18] 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 *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, ASIA CCS 2014*, pp. 3–14, Japan, June 2014.

[19] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue AP detection," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 11, pp. 1912–1925, 2011.

[20] Y. Song, C. Yang, and G. Gu, "Who is peeping at your passwords at starbucks to catch an evil twin access point," in *Proceedings of the 2010 IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2010*, pp. 323–332, USA, July 2010.

[21] C. Yang, Y. Song, and G. Gu, "Active user-side evil twin access point detection using statistical techniques," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1638–1651, 2012.

[22] Q. Lu, H. Qu, Y. Zhuang, X.-J. Lin, Y. Zhu, and Y. Liu, "A passive client-based approach to detect evil twin attacks," in *Proceedings of the Trustcom/BigDataSE/ICESS*, pp. 233–239, IEEE, Australia, August 2017.

[23] D. Mónica and C. Ribeiro, "WiFiHop - mitigating the evil twin attack through multi-hop detection," in *Computer Security – ESORICS 2011*, vol. 6879 of *Lecture Notes in Computer Science*, pp. 21–39, Springer, Berlin, Germany, 2011.

[24] O. Nakhila and C. Zou, "User-side Wi-Fi evil twin attack detection using random wireless channel monitoring," in *Proceedings of the 35th IEEE Military Communications Conference, MILCOM 2016*, pp. 1243–1248, USA, November 2016.

[25] 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," in *Proceedings of the 2016 International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT 2016*, pp. 176–181, India, March 2016.

[26] 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 and Electrical Engineering*, vol. 59, pp. 76–85, 2015.

[27] W. Wei, Y. Gu, K. Suh, J. Kurose, B. Wang, and D. Towsley, "Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs," in *Proceedings of the IMC'07: 2007 7th ACM SIGCOMM Internet Measurement Conference*, pp. 365–378, San Diego, Calif, USA, October 2007.