User-Side Wi-Fi Evil Twin Attack Detection Using SSL/TCP Protocols

Omar Nakhila[ab], Erich Dondyk[c], Muhmmad Faisal Amjad[d] and Cliff Zou[e]
[a c d e] Dept. of EECS, Univ. of Central Florida, FL, USA
[b] Dept. of Computer Engineering, College of Engineering, Univ. of Mosul, Mosul, Iraq
[ab]omar_hachum@knights.ucf.edu, [c]erich@knights.ucf.edu, [d]faisal@eecs.ucf.edu, [e]czou@cs.ucf.edu

***Abstract*—Evil Twin Attack (ETA) refers to a rogue Wi-Fi Access Point (AP) that appears to be a legitimate one but actually has been set up to eavesdrop on wireless communications [1]. Most of existing detection techniques assume that the attacker will use the same legitimate wireless network gateway to pass through victim's wireless data. These detection methods will fail if the attacker uses a different gateway, such as using his own broadband cellular connection through his own smartphone. In this paper, we present a new client-side detection method to detect such an ETA that uses a different gateway from the legitimate one. It relies on SSL/TCP connection to an arbitrary remote web server to avoid attacker's misleading message, and trying to detect the changing of gateway's public IP address by switching from one AP to another in the middle of the SSL/TCP connection. The detection method is on the client side which makes it more convenient for users to deploy and ensure their security.**

***Index Terms*—Evil Twin Attack, Wi-Fi security, TCP, SSL.**

I. Introduction

Nowadays, 802.11-based wireless local area networks, or called Wi-Fi, are everywhere [2]. People use wireless network in their daily life bases, shopping online and paying bills to name a few. This makes Wi-Fi an attractive target for intruders to compromise and to eavesdrop wireless client information.

In recent years, more and more businesses, such as some fast food restaurants, coffee shops, retail stores, have set up Wi-Fi access points to provide free wireless Internet service in order to attract and better serve their customers. These sites are also called hotspots. Most of the time, Wi-Fi hotspots have no or very limited security protection. Clients will only need to search the airwave and connect to the wireless network. No mean of encryption or authentication is used besides the wireless network name (SSID). Because of the lack of security protection, hotspots are vulnerable to the popular and well-known Evil Twin Attack.

Evil Twin Attack (ETA) refers to a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications [3]. The attack starts when an attacker sets up a rogue AP in a place that provides free wireless Internet service such as coffee shop. Since Wi-Fi wireless networks in most hotspots do not provide any type of encryption and authentication, an attacker can configure a rogue AP to start transmitting the same SSID that used by the legitimate hotspot AP. For a Wi-Fi client, if the perceived signal power from the attacker's AP is stronger than the perceived signal power from the legitimate AP, either because the attacker's AP is closer to the client, or it has a more powerful transmitting antenna, the client will be tricked to switch its Wi-Fi connection from the legitimate AP to the rogue AP. What makes the attack even worse is that such switching of AP is usually automatic and transparent to users [4].

When the rogue AP hijacks the Wi-Fi connections from clients, the rogue AP usually has two options to connect to the Internet. First, the rogue AP can itself behaves as a normal Wi-Fi client and uses the legitimate AP to connect with the Internet. This is the classical ETA well studied by many researchers [3] [5] [6].

The second Internet access option for an ETA is to use cellular broadband connection [3] [6] as illustrated in Figure 1. This type of ETA will become more popular nowadays due to the increase in the Internet access speed of mobile connections, such as 4G Long Term Evolution (LTE) or WiMAX [7]. In this approach, the attacker uses a different gateway compared with the legitimate AP.

For the second ETA approach, the traditional time delay based detection method introduced in [3] will not work. Because the attacker uses a different gateway, it is quite possible that an Internet connection through the rogue AP has a shorter time delay than through the legitimate AP. Facing this attack challenge, we must design a different detection approach for this second type of Evil Twin Attack.

In this paper, we improved the Wi-Fi security by :

- Presenting a novel detection method to deal with the second type of ETA. Basically speaking, the detection technique will detect whether or not different gateways are used by multiple APs in one hotspot location that have the same SSID. As far as we know, each hotspot will always use the same gateway for Internet access no matter how many legitimate APs have been set up in the same hotspot [8].
- The detection method is a secure client-side approach that does not rely on any support from hotspot networks or dedicated servers. In addition, no training data or authorized trusted AP list will be used in the ETA detection. It can be easily deployed together with any existing first-type ETA detection method such as [3] [5] [6] in order to securely detect both types of ETA.
- Finally our detection method was implemented and evaluated in a real life environment.

The paper will be organized as follows. Section II discusses the related work of previous ETA detection. In Section III we presented several intuitive solutions and show why they are not effective in ETA detection. The design of the new detection method and developed prototype will be presented in Section IV. Then, we evaluate the statistical performance of the new detection method in Section V. Finally, limitation and conclusion will be present in the last two sections.

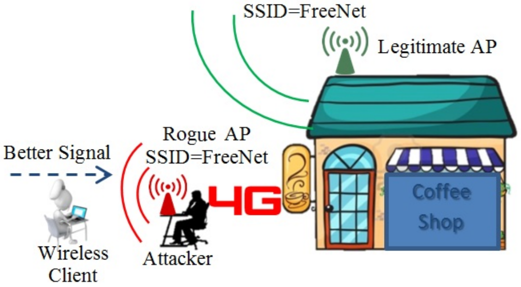


Fig. 1: Illustration of the second type of Evil Twin Attack that we focus on in this paper. The Rogue AP can successfully lure clients connecting to it instead of the legitimate AP when it has stronger/better signal to those clients. This ETA uses cellular broadband connection that has a different gateway compared with the legitimate AP.

II. Related work

ETA in wireless networks is a threat that can transfer the privilege from a legitimate wireless network administrator to an attacker to become the gateway of a wireless client (victim). In this scenario, all the wireless traffic from the victim will pass though the attacker node. At this point, the attacker can apply a desired man in the middle attack (MITM) to exploit any vulnerability that can leak information about the victim. MITM in this situation will be hard to detect since the victim will be in a separate wireless network (attacker wireless network) than the legitimate wireless network.

The detection of ETA was under the spotlight for many years. Researchers have been investigating detection methods that can alert the wireless network administrator/client about the presence of this type of attack. Each detection method has its own working environment. To have more insight about these types of detections, we divided them into two categories. The categorization was based on who will be responsible for the ETA detection.

The first category is administrator side detection. In this category, administrators are the one responsible for ensuring wireless client protection from ETA. Administrators scan the airwaves and match between APs found transmitting nearby with an authenticated APs list that have been previously created on the administrator side. Each AP should have a fingerprint that can be used to identify itself. Such a fingerprint can be the MAC address of the AP or its location [3]. The strength of this type of protection depends on the fingerprint used to recognize the AP. For example, if the location is the fingerprint of an AP, this type of detection may trigger false positive alert of a potential ETA if there is a nearby AP that transmitting in a close range to the authenticated APs [5]. Also, attacker may change the rogue AP characteristics to match the ligament AP. For instance, the attacker can change the MAC address of a rogue AP to one of the authenticated APs. Researchers were investigating different type of fingerprints that can be used to distinguish one AP from another [9].

Administrator side detection will also add more cost to the total wireless network construction price. This is because administrations need to install wireless sensors devices to continuously scan the airwaves to gather information about the available transmitting APs. To lower the cost, researchers proposed that workstations can turn into wireless sensors [10]. In general, administration side detections are limited, expensive and not available in many cases [3].

The second category of ETA detection methods is user side detection. This type of detection is more preferable than the administrator side detection since the wireless clients will ensure their protection against ETA. One of the detecting method techniques that falls in this type of category [3] propose that by measuring the travel time of packets between the wireless client and a nearby server, the wireless clients can detect the presence of ETA. This is because when an attacker uses the rogue AP to pass through wireless client data, there will be an extra wireless hop between the wireless client and the legitimate AP. This extra wireless hop will add more time compared to the direct connection between the wireless client and the legitimate AP.

However, this method assumes that the attacker will use the legitimate wireless network gateway to pass through client data traffic. This detection will fail especially when the attacker uses faster Internet connection compared to the legitimate wireless network. In this scenario, the attacker can delay the response time of the propagating packets between the server and the wireless client to match the propagation time of the packets passing through the legitimate AP. In addition, this method suffers from wireless signal strength fluctuations and the data traffic load on the APs that may vary the response time between the wireless client and the server [3].

Another ETA detection method that belongs to the second category and can be used to detect different gateway is traceroute command ETA detection method [6]. In this detection method, traceroute command will be used to find route information between the wireless client and a random remote server. At the beginning, the wireless client will connect to any AP and use the trace route command to find the route information between himself and any remote server. Then, the wireless client will switch to another AP and use traceroute command to record the route information between himself and the same remote server used at the first AP. Using two different APs for the same wireless network should return the same route information [6].

Nevertheless, this type of detection may fail since network administrators may configure network firewall to drop these traceroute packets for security purposes [11]. Also, an attacker can easily pass traceroute ETA detection method by simply monitoring the wireless data traffic. This monitoring is possible because traceroute uses the unencrypted ICMP protocol to gather route information between the wireless client and the remote server. Attacker can capture traceroute results sent to the wireless client using the legitimate wireless network. After that the attacker can send these results to the wireless client using the rogue wireless network. This will give the same route information for both gateways which will pass ETA detection method without triggering any alarm.

On the other hand, a wireless client can setup a VPN connection through the wireless hotspot. In this case, all the traffic between the wireless client and the hotspot will be encrypted. However, VPN is not available for all users and have numerous points of failure [12].

III. INTUITIVE DETECTION SCHEMES AND THEIR SECURITY VULNERABILITIES

In this section, we first present the adversary model. Then we present several intuitive detection schemes, and show that all of them have inherent security holes, making them unfeasible solutions to the Evil Twin Attack.

A. Adversary Model

In this paper, ETA was assumed to be implemented by an attacker with the capability to mimic the legitimate wireless network specifications. For example, the IP and the MAC addresses of the DHCP, DNS and the gateway provided by the rogue AP will be exactly the same as the ones found in the legitimate wireless network. Also, the propagation time between the wireless client and any other servers can be tuned by the attacker to give the similar result as the legitimate wireless network.

As introduced previously, a rogue AP in ETA has two options to connect to the Internet: uses the same gateway as the legitimate Wi-Fi hotspot, or uses a different gateway. In this paper, our ETA detection focuses on the second type of ETA that uses a different gateway compared with the legitimated hotspot. In real implementation, both the ETA detection on the first option (such as the system introduced in [3]) and our proposed scheme should be used together for comprehensive ETA detection.

B. Intuitive Detection Schemes and Their Security Problems

1) Detection based on route option in IP packet header: One of the intuitive detection methods that can be used to detect ETA is by taking advantage of the record route option found in IP header [13]. When this option is enabled in a packet, routers on the route between the source and destination will place their own IP addresses in the packet IP header. Based on that, in this detection method, the wireless client will send an IP packet using a given Access Point (AP1) that belongs to the hotspot Wi-Fi network. Then, the wireless client will switch to another Access Point (AP2) that also belongs to the same wireless network and send a second packet. The record route option is enabled in these two packets and the destination address of these two packets will be a special server on the Internet. When the server at the other end receives these packets, it will match between the routers' addresses recorded in the IP header received from both AP1 and AP2. Then, the client can view the results on the server using HTTPS protocol.

However, similar to the traceroute packets, record route packets may be dropped or ignored by many firewalls for security reasons [11]. In addition, only at most nine IP addresses can be recorded along the route while, the average number of routers in any given route on the Internet is 19 to 21 [14].

2) Detection based on TCP connection: The second intuitive detection method that can be proposed to detect ETA is by dividing TCP communication. The detection procedure will start after a wireless client initiates a wireless connection to a nearby AP. This AP (we call it AP1) should have the wireless SSID name such as FreeNet (Figure 1) that belongs to hotspot Wi-Fi network. After connecting to AP1, the wireless client will start a TCP 3-way handshake to a random remote webserver such as www.google.com. Each side (the wireless client and www.google.com) will create a socket connection that contains the IP address and the Port number for the other side.

After completing a successful TCP 3-way handshake through AP1, the wireless client will then switch to a different AP (we call it AP2) with the same wireless SSID. The wireless client will not start a new TCP 3-way handshake since the TCP connection is already established using AP1. Changing the AP will have no effect on the socket information stored in each side of the connection. After switching to AP2, the wireless client will send a GET html request to download an index webpage on the remote webserver.

If the two APs use the same gateway, the TCP connection will not break and the wireless client will start downloading the index webpage from the remote webserver successfully. Otherwise if the TCP connection is broken, we know that these two APs use different gateways. Using different gateways will prevent the webserver to give a positive response to the wireless client because the IP address and/or the port number of the wireless client will be different using the second gateway.

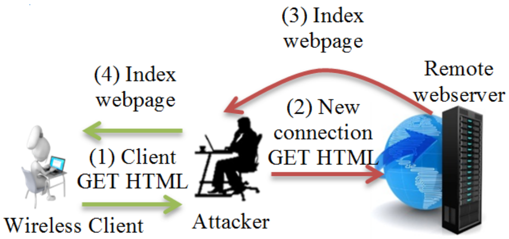


Fig. 2: Possible man-in-the-middle attack on the ETA detection that relies on TCP connection without SSL.

However, an attacker can conduct MITM attack to the above detection method by impersonating the remote webserver role. This MITM can take place when the wireless client starts downloading the index web page though AP2 (which is the attacker AP). The attacker at this point can catch the GET html request from the wireless client and start a new connection to the remote webserver and retrieve the index webpage. Then, because the attacker can monitor the TCP connection setup between the client and AP1, the attacker can send the index webpage to the wireless client by continuing the existing TCP connection. This MITM is illustrated in Figure 2.

IV. PROPOSED DETECTION DESIGN

A. Design Assumption

The design of the proposed ETA detection method for detecting different gateways is based on the following assumption: a Wi-Fi hotspot may deploy more than one AP for better quality and wider coverage. However, all APs belonging to the same hotspot will always use a single gateway for Internet access. This type of wireless network topology can be found in coffee shops, hotels and airports [10]. Also, network administrators in these wireless networks usually assign private IP addresses to their wireless customers. These private IP addresses will be eventually translated into the public IP of the gateway using network address translator (NAT) or port address translator (PAT) [10].

B. Proposed Detection Design

The detection relies on SSL/TCP connection for webpage retrieval in the similar way as the second intuitive TCP-based detection method introduced in previous Section III-B. When the wireless client starts the detection procedure, it initiates a TCP 3-way handshake though AP1 using SSL connection to an arbitrary remote webserver that supports HTTPS connections (such as to https://www.google.com). Then, the client switches Internet access via AP2 and issues HTTP GET command to retrieve webpage content.

By using SSL connection, we can prevent an attacker from applying the MITM attack illustrated in Figure 2 since the attacker does not have the current TCP session's information to continue the SSL/TCP connection with the wireless client.

Our proposed detection method will distinguish whether two access points with the same SSID use the same network gateway or not. If there are more than two APs existed in a hotspot, our detection schemes work in the same way by checking each AP one after another to find whether all existing APs use the same gateway or not.

The detection method will be on the wireless client side which is more desirable than the administrator-side detection. Client-side design gives a security-sensitive user more control over her Wi-Fi connection security, and can be used in any Wi-Fi hotspots regardless of what security mechanism a hotspot has implemented.

In addition, no fingerprint will be used in the detection. The client will not need to have any previous information about the APs installed in a Wi-Fi hotspot. Furthermore, the detection method will not be based on a protocol or a protocol option (such as ICMP or record route option) that might be blocked by network administrators for security purposes.

C. Implementation

The ETA detection client software prototype was implemented using C language and run on Linux machine. We developed the software by modifying a C language socket source code from [15] [16] to accomplish the proposed ETA detection. The source code for the wireless client software can be downloaded from https://github.com/mysofthub/SSL-TCP-ETA. The program will automatically start the SSL/TCP socket connection through the first AP with an arbitrary webserver, and then start downloading the index webpage from the webserver using the second AP.

The webserver implemented in our prototype was www.google.com because it is more reliable than most other webservers, and most importantly, it has a long time-to-live SSL/TCP connection (240 seconds based on our measurements). This will give the wireless client plenty of time to switch from one AP to another without the SSL/TCP connection to have timeout.

Pseudo Code 1: SSL/TCP based Evil Twin Attack Detection.

```
Connect to AP1
Start SSL/TCP 3-way handshake to www.google.com
Verify www.google.com certificate
if www.google.com certificate is valid then
    Switch to AP2
    GET command to download index.html
    if www.google.com starts sending the index.html webpage then
        Print no ETA detected
    else
        The connection was rejected
        Print ETA detected
    end
else
    Print server certificate error!!
end
```

The program will connect to the first AP1 using AP1's SSID and MAC address. Since there will be more than one AP with the same SSID, the MAC address of the AP will be the reference to switch between different APs. After finishing the SSL/TCP 3-way handshake, the program will automatically switch to the second AP (AP2) and start downloading the index webpage from the webserver.

The remote server can be any arbitrary webserver that supports HTTPS protocol. The Pseudo Code 1 above illustrates the proposed ETA detection.

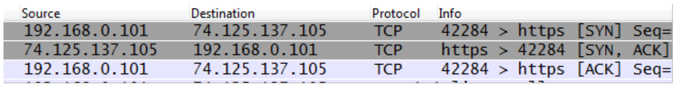
V. EVALUATION

A. Evaluation Procedure

By using Wireshark [17] to capture network traffic, we have verified that the proposed ETA detection is effective in detecting the the second type of ETA in which the rogue AP relies on a different gateway (such as 3G or 4G data service) to provide Internet access.

In the first test where two APs were using the same gateway, the proposed ETA detection will start by the wireless client connecting to the first AP. The wireless client would obtain its IP address from the DHCP server. The connection information between the wireless client and the webserver was shown in

Figure 3. The IP address obtained by the wireless client was in the private IP range (192.168.0.101) and the source port address that was used in the 3-way handshake is (42284). The remote Google website had an IP address of 74.125.137.105.

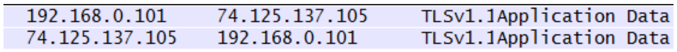


```
Source            Destination        Protocol  Info
192.168.0.101     74.125.137.105     TCP       42284 > https [SYN] Seq=
74.125.137.105    192.168.0.101      TCP       https > 42284 [SYN, ACK]
192.168.0.101     74.125.137.105     TCP       42284 > https [ACK] Seq=
```

Fig. 3: SSL/TCP 3-way handshake using AP1.

The wireless client source IP was translated at the gateway to a public IP address. At this point, the webserver created a socket connection using the public IP address of the wireless client and the port address given to the wireless client at the gateway. After verifying www.google.com certificate, the program disconnected from AP1 and connected to AP2.

Although the wireless client switched the wireless connection from AP1 to AP2, Wireshark did not catch any connection termination packets sent from the wireless client to the webserver. At this point, the wireless client had an active connection to the webserver through AP2. After that, the wireless client program would send a GET command to retrieve html index page as shown in Figure 4.

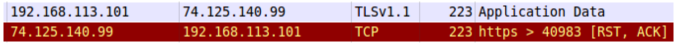


```
192.168.0.101     74.125.137.105     TLSv1.1Application Data
74.125.137.105    192.168.0.101      TLSv1.1Application Data
```

Fig. 4: Successfully downloading index webpage using AP2.

When the detection program started receiving the index webpage, the program would display safe wireless network message to the wireless client. This proved that the socket information stored in the webserver matched the GET HTML request connection, meaning that both APs were using the same gateway.

In the second test, we setup the two APs to use different gateways. The wireless client IP address in this scenario was 192.168.113.101 and Google website IP address was 74.125.140.99. When the wireless client switched to AP2 and sent GET html to the webserver, the remote webserver sent RST/ACK packet to the wireless client for termination of the existing connection. The connection was terminated by the server because the information stored in the SSL/TCP socket did not match the information received by the wireless client. This action has been verified by our Wireshark capturing as shown in Figure 5.



```
192.168.113.101   74.125.140.99     TLSv1.1   223 Application Data
74.125.140.99     192.168.113.101   TCP       223 https > 40983 [RST, ACK]
```

Fig. 5: The server closed the connection with the wireless client when AP1 and AP2 used different gateways.

Since the webserver terminated the connection, the wireless client was not able to download the index webpage. In this case, the program would display an ETA warning message to the wireless client.

B. Detection Time Delay Analysis

Unlike paper [3], our proposed detection method is not based on any time measurement for detection. This is more desirable because time-based methods need to monitor many packets in order to obtain accurate measurement, which makes the ETA detection take a longer time to complete. In addition, time-based detection will be unreliable when an attacker uses his own broadband cellular data service for the rogue AP as illustrated in section II.

Nevertheless, time delay is still a very important performance metric. Therefore, we have analyzed time delay in our evaluation. The wireless APs used in the test bed were NETGEAR FWG114P and D-LINK DIR-601. These APs also operated as DHCP, DNS servers and gateway. The wireless client in the test bed used Ubuntu Linux based OS with an Intel(R) Centrino(R) WiMAX 6150 WLAN card.

We measured the time delay for four main steps in the detection procedure:

- The time to connect to AP1 and obtain a valid IP address from the DHCP server.
- The time to finish the 3-way SSL/TCP handshake.
- The time spent to switch from AP1 to AP2 and obtain/reuse a valid IP from the DHCP server.
- The time to receive response from the webserver.

The test was repeated 50 times for each measurement. In the beginning of each trial, the APs (including DHCP, DNS and the gateway) were turned off and back on to ensure fresh reading. Figure 6 illustrated the results of the test bed measurements when the two APs used the same gateway.

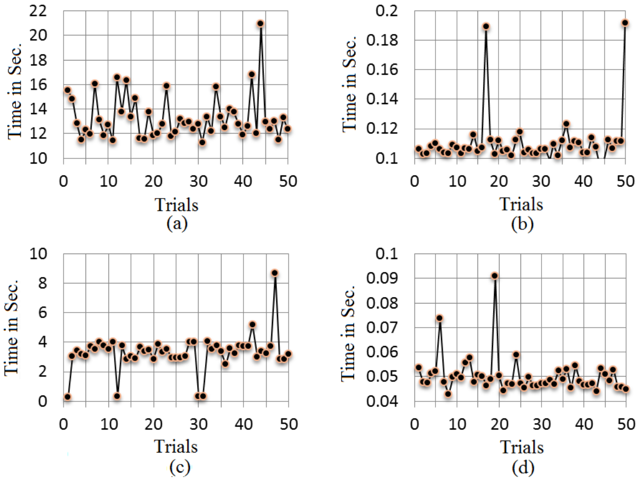


Fig. 6: ETA detection procedure time duration when AP1 and AP2 use the same gateway. (a) connecting to AP1. (b) 3-way SSL/TCP handshake. (c) switching to AP2. (d) receiving a response from the webserver.

The time spent to connect to AP1 and the switching time from AP1 to AP2 was relatively big compared to the other time measurements. The average time to connect to AP1 and AP2 was 13.3 and 3.3 seconds, respectively. The time needed to connect to AP1 was larger than AP2. Form our observation, the reason behind this time difference (about 10 seconds) was the time duration to obtain a valid IP address from the DHCP server for the first time using AP1. On the other hand, it will take less time to reuse the same IP address using AP2. Also, the connecting time from one wireless network to another may vary and it depends on the manufacturing types and models of the wireless network devices.

The time duration to finish the 3-way handshake and to receive a response from the webserver was relatively shorter than the connecting time. In our test bed, fast Internet speed link was used (>10 Mbps). The average time duration to complete the 3-way handshake was 0.1 seconds, while the average time to receive a response from the webserver was 0.05 seconds. These time values depend on many factors such as the Internet speed, DNS response time and webserver's response time.

In the end, we want to emphasize that although the test time of the detection method may vary according to many factors as explained above, these factors will not affect the detection effectiveness of the proposed technique.

VI. Discussion and Limitations

In our paper we only discussed the scenario where there is one legitimate AP and one rogue AP. If the client receives more than two AP signals, our detection method can be used without any change to switch between each reachable APs one by one. Each AP switching should be done in the middle of the SSL/TCP connection. If any one of these APs uses a different gateway, the SSL/TCP connection will break and produce alarm. This will alert the user of an ETA.

In our method, client software will verify the remote server's certificate. This will prevent the attacker from creating a fake remote server to bypass our detection procedure. Also, since our ETA detection starts its communication on port 443, SSL strip attack [18] will not be feasible since that attack is based on the transition between port 80 and port 443.

Our proposed ETA detection scheme has its own limitations. We discuss these limitations below.

First, we clearly stated that our detection method was focused on detecting ETA using different gateways. If the attacker uses the same legitimate gateway to pass client data, our detection method will not work. However, combining our detection method with other methods that were used to detect ETA using the legitimate gateway (such as [3]) will produce an effective and comprehensive ETA detection system.

Second, the proposed detection method will spend about three seconds when switching from one AP to another as shown in Figure 6c. This requires that the web server should have a long time to live (TTL) SSL/TCP session to allow the client to switch between the APs without dropping the connection. In our prototype evaluation, google web servers were selected because they support SSL protocol and they also have a long TTL SSL/TCP session. We measured the TTL value of SSL/TCP session for www.google.com and the result was 240 seconds.

Third, upon detecting the presence of ETA, our detection method will not be able to identify which AP is rogue and which one is legitimate. Because both the legitimate AP and the rogue AP provide Internet access that could have the similar quality, it is very challenging to further distinguish them apart with only client-side actions.

Finally, if the client receives only rogue AP(s) signals without any legitimate AP, our detection method will not work as well. This weakness can be found in all client-based ETA detections that do not use authorized AP-list. Client cannot detect ETA since all the AP(s) will give the consistent fake results.

VII. Conclusion

In this paper, a novel ETA detection technique was proposed to detect ETA using a different gateway compared with the gateway used by the legitimate Wi-Fi hotspot. The detection technique is lightweight and is a client-side approach. The detection method was prototyped and evaluated using real-world scenarios. Also, detection time delay is generally short and time delay variance does not affect the detection effectiveness. Although our detection method only focuses on detecting ETA that uses a different gateway, it can be readily combined with a classical time delay-based ETA detection method such as [3] to provide comprehensive ETA detection.

Acknowledgement

The first author would like to acknowledge the financial support from the Higher Committee for Education Development in Iraq (HCED).

References

[1] Smith, Andrew; Strange Wi-Fi spots may harbor hackers: ID thieves may lurk behind a hot spot with a friendly name, The Dallas Morning News, Knight Ridder Tribune Business News, Washington, DC: May 9, 2007

[2] Zhang, Ning, and Hong Bao., Wireless Network Technology and Its Applications, International Conference on Networks Security, Wireless Communications and Trusted Computing 2 (2009): 635-38.

[3] Yang, Chao, Yimin Song, and Guofei Gu., Active User-Side Evil Twin Access Point Detection Using Statistical Techniques, IEEE Transactions On Information Forensics And Security 7 (2012): 1638-651.

[4] Intel.com,What is Wi-Fi roaming aggressiveness?, Intel Wi-Fi Products: Aug 12, 2014.

[5] Yang, Chao, Yimin Song, and Guofei Gu., Who is peeping at your passwords at Starbucks? - To catch an evil twin access point , Conference on Dependable Systems and Networks (DSN) (2010): 323 - 332.

[6] Nikbakhsh, Somayeh, Azizah Manaf, Mazdak Zamani, and Maziar Janbeglou, A Novel Approach for Rogue Access Point Detection on the Client-Side, 26th International Conference on Advanced Information Networking and Applications Workshops (2012): 684-87.

[7] 4G., Wikipedia [Online], http://en.wikipedia.org/wiki/4G.

[8] SMC Network, Wireless Hotspot Solutions, 2008.

[9] S. Jana, S.K. Kasera, On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews, Mobile Computing, IEEE Transactions on (March 2010): 449 462.

[10] Bahl P, Chandra R, Padhye J, Ravindranath L, Singh M, Wolman A, Zill B.,Enhancing the security of corporate Wi-Fi networks using DAIR, Proceedings of the fourth international conference on mobile systems, applications, and services, Uppsala,(2006).

[11] Robert Sherwood, Discovering and Securing Shared Resources on the Internet, Doctor of Philosophy Dissertation, Univ. of Maryland, 2008.

[12] Scott, Charlie, Paul Wolfe, and Mike Erwin. Virtual Private Networks, Second Edition, Beijing: OReilly, 1999.

[13] RFC 791,Info. Sci. Institute, Univ. of Southern CA, USA, Sept 1981.

[14] Albert, R., H. Jeong, and A. Barabsi,Internet: Diameter of the World-Wide Web, Internet: Diameter of the World-Wide Web, 1999.

[15] OpenSSL Tutorial - Client, [Online] https://thunked.org/programming/openssl-tutorial-client-t11.html.

[16] Kenneth Ballard, Secure programming with the OpenSSL API, Part1: Overview of the API, MediNotes Corp. June 28, 2012.

[17] Wireshark Foundation software, Vers. 1.8.6.

[18] Zhang, H., Y. Shi, and Z. Xue, HTTPS Session Hijacking Based on SSLStrip, Info. Security and Communications Privacy 10 (2009): 038.