User-Side Evil Twin Attack Detection Using Time-Delay Statistics of TCP Connection Termination

En-Chun KUO, Ming-Sang CHANG, Da-Yu KAO*
Department of Information Management, Central Police University, Taoyuan City 333, Taiwan
***Corresponding author: camel@mail.cpu.edu.tw, Tel: + 886 3228 2321*5100**

Abstract— **Open wireless network services are now freely shared in the most of the public areas but have barely protection about communication data between the web server and the client-side. Evil Twin Attack (ETA) appears to be a legitimate Wi-Fi Access Point (AP) and becomes a common attack in smart home environments where attackers can compromise the security of the connected devices. By setting up a rogue access point, deceiving users into establishing the network connection with the same SSID as the legitimate one, the attacker can launch the man-in-the-middle attack and steal some private information. To identify the fake APs, this paper presents an improved and practical client-side detection method to mathematically detect the ETA by observing the time-delay of TCP connection termination between the client and the server. This proposed time-delay model is further experimented and measured from the following three date-time intervals: Initial Ending, Ending Response, and Confirmed Ending. The utility of this model is illustrated by applying it to the client side which makes it more convenient for users to deploy and ensure their security with high detection rate.**

Keywords— **Access Point, Wi-Fi Network, Evil Twin Attack, TCP Connection Termination, Time-Delay Analysis**

I. INTRODUCTION

The wireless network is now playing a significant role in the world, due to the tremendous and comprehensive advancement in wireless network technology in recent years. People could surf the Internet everywhere and anytime by using their phones and laptops connecting to wireless network, or called Wi-Fi. Recently, there has been more and more public areas providing Wi-Fi services for their customers and clients, such as hotels, coffee shops, convenient stores, students' community areas and so on. Even passengers could connect to Wi-Fi set on vehicles, for example, taxis, buses, trains, and aircrafts. The users could easily and quickly get access to the wireless networks. However, there is one of the most potent attacks on Wireless Local Area Networks (WLANs) infrastructures called Evil Twin Attack (ETA). Many wireless network clients might accidentally connect to the malicious access point, thinking it as a part of the authorized network. Once the connection is established, the attacker can orchestrate a Man-In-the-Middle Attack (MIMA) and transparently relay traffic while eavesdropping on the entire communication [1] [2] [3].

To give a clearer explanation, ETA, literally, is a fraudulent Wi-Fi access point that appears to be legitimate, and set up to eavesdrop on wireless communications. The evil twin is the WLAN equivalent to the phishing scam. This type of attack may be used to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing.[4][5][6].

When the Wi-Fi clients in the public area turn on Wi-Fi on their mobile phone or the personal computer, they will choose the wireless network name which corresponds with one name provided by the public areas. Since a wireless network could only be recognized by Service Set Identifier (SSID) and Media Access Control (MAC) address, the attacker can set up a Rogue Access Point (RAP) with the same SSID of the Legitimate Access Point (LAP) to lure Wi-Fi clients connecting to it [7][8]. If the signal from the attacker's RAP is stronger than the signal from LAP, the Wi-Fi user will definitely choose the stronger one in order to ensure the better speed and quality of the Internet. After that, the attacker could begin spying on the Wi-Fi user's data traffic. Furthermore, the attacker could make use of the vulnerability to launch the man-in-the-middle attack, such as extracting usernames and passwords from the network traffic, presenting the user with spoofed login pages, attacking the client with browser-based exploits, Domain Name System (DNS) poisoning, and much more [7] [9].

The ETA usually could be broadly spilled into two basic options. While the client connects to the RAP, the attacker could use the Wi-Fi interface card to connect to the LAP, being a rogue network user and transferring the client's network traffic to the Internet. This is one of the ETA options which called ETA using the single ISP gateway; another option is ETA using the different ISP gateway. Due to the well-developed of mobile broadband network connection, the Internet access speed is getting faster. Some attackers will use its own cellular broadband link as a hotspot as well as a rogue AP, deceiving the wireless network users into connecting to the rogue AP. In this scenario, the attackers will be in between the RAP and its broadband connection [7] [9].

This paper focuses on ETA using single ISP gateway and adopts the time-based method to monitor the TCP packets transferring between client side and server side. Our ETA detection improved the Wireless network security by:

- The ETA detection method is friendly operation solution. By observing the time delay of TCP packets transferring when webpage openings and closing, researchers could detect the difference between LAP and RAP. The office workers, travelers or other common people in Wi-Fi environment could easily launch the detection.
- The proposed ETA detection is a client-side solution which does not depend on any fingerprint provided by the network administrator. The wireless clients have no need to get any information about the wireless network configuration or authorized trusted APs, which makes it more preferable than the administrator-side detection.
- Finally, the proposed detection technique was prototyped, implemented and evaluated in real life environment.

The paper will be organized as follows. The related works of previous ETA detection are discussed in Section II. In Section III presents the detailed description of TCP connection termination and four-way handshake between client side and server side. The proposed ETA detection method will be provided in Section IV. Section V gives the observation and analysis of experimental data. Finally, limitations and conclusions will be described in the last two sections.

II. Related Works

ETA, in recent years, has been a hot issue for the researchers to find out the way to detect the RAP or to increase the Wi-Fi's security. And the types of detections are divided into two categorizations based on who is responsible for detection [7].

One of the categories is administrator-side detection. In this type of detection, the network administrators have to check all the network topology regularly and match all the wireless devices founded surrounding with the authenticated APs list which had been created on the network administrator side previously. Each AP has its own “fingerprint” which could distinguish itself, for example, the MAC address of the AP or its location [7]. And the network administrators could identify whether the AP is illegal or not by the fingerprint and the authorized list.

When it comes to the disadvantage of this type of detection, since the location being the fingerprint of AP, it might produce false positive alert of a potential ETA. Besides, the network administrations should be equipped with sensors devices and takes plenty of time to collect information about all the available APs. To sum up, administrator side detections are poor, limited and time-consuming. Nowadays, this type of detection is inappropriate in many cases [7].

Another type of ETA detection is client-side detection. The wireless network users will be solely responsible for uncovering ETA. Not only does it involve multiple methods to uncover ETA, but it is more flexibility to conduct at anytime and anywhere. There have been lots of papers addressing the client-side detection for ETA, for instance, in [7], by observing SSL/TCP three-way handshake connection between the legitimate AP and rogue AP, it could detect the ETA using the different ISP gateways. However, in this proposed detection method, it must ensure that the web server has a long Time To Live (TTL) SSL/TCP session to allow the client to switch between the APs without dropping the connection. If the web server which the client selects doesn't have a long enough TTL SSL/TCP session or not support SSL protocol, the detection may produce the false negative result. Furthermore, this method couldn't distinguish LAP and RAP apart with only client-side actions.

As for [9], it scans all the channel of LAP and RAP in a short time and finally uncovers the presence of ETA using the single ISP gateway. Although this kind of detection may work out, the method is limited in some aspect, for example, the detection method is composed of RAP, LAP, rogue wireless clients, and Public Information Server (PIS). PIS plays a vital role in the detection testbed and if the wireless network users don't have any other Internet equipment as PIS, they could not install the related software mentioned in the detection and neither do they get any information about it [9].

Another client-side detection depends on the extra delay time between RAP and the wireless network client [10]. In the scenario, the network client respectively connects to the LAP and RAP, analyzes the traveling time of TCP with ACK flag packets, and measures propagation delay between the client and APs. Nevertheless, it proposes two statistical anomaly detection algorithms in the method which might be over-complicated for the public for the reason that it mentioned the solution which would be particularly attractive to the traveling users. On the other hand, this method may be affected by wireless signal strength fluctuations. If the wireless network scenario isn't the same as the test bed set in the research, the ETA alert may not be triggered. Even though the time-based method may be affected by some variables, which is still an essential performance metric for ETA research [10] [11]. This paper will address the preferable solution and present our ETA detection design.

III. Details about TCP Connection Termination

This section provides detailed description of TCP connection termination. It seems that TCP connection termination gets less attention than TCP connection establishment, but it is still a significant packet-transferring pattern in TCP connection. Unlike three-way handshake happening in establishing the connection, when the devices intend to end the connection, it will launch TCP four-way handshake as illustrated in Figure 1.

First, the client sends the TCP packet with FIN, ACK flags to request that the connection is closed. In the period of waiting for ACK flag from the server, the client could still receive the data from the server, but it will no longer allow any data from its application or webpage to be sent to the server. The researchers call this interval Initial Ending in this paper.

Next, after sending ACK flags, the server now is waiting for the application or webpage on its end. Receiving the notice of application or webpage which tells that the process has been done, the server sends FIN, ACK flags to the client side at once. Before accepting the FIN flag from the server, the client side is waiting for the signal to close. The researchers call it Confirmed Response in order to represent the procedure of the server acknowledging FIN from the client side and waiting for the application closing.

Afterwards, the client side sends back the TCP packet with ACK to confirm that the connection ends. The period between the server sending FIN and the client sending ACK is named as Ending Response. The connection will be closed on the server's end with receiving ACK flags. On the other side, the client side will wait for a period a time to ensure the ACK was received. Finally, the connection will be closed completely and gracefully.

The procedure of termination could be observed readily when the webpage or application is going to be closed. Moreover, concerning that the practical detection will probably be launched by the public in the real-life environment. If the wireless client connects to the RAP, taking the connection termination as a part of detection method could meet the realistic requirements in order to end the connection with the attacker at once rather than continuously transferring the private information to the attacker. With all these reasons, researchers take the termination as our time-based statistical data, monitor the packets transferring between the client side and the server side and measure three intervals which mentioned above.

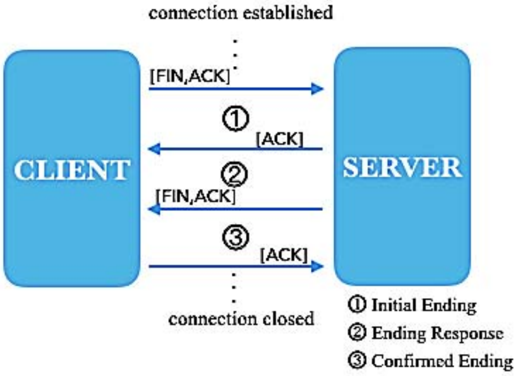


Figure 1. TCP connection termination procedure. (Four-way handshake)

IV. Proposed ETA Detection Design

This section first presents the assumption of the detection experiments as well as proposed ETA detection system with the testbed. Afterwards, it will describe how the proposed detection implements, showing the whole process of the experiments.

A. *Design Assumption*

The ETA detection method makes use of the unique wireless architecture deployed by the attack option of ETA mentioned previously — using a single ISP gateway. However, unlike the situation set in [6], adding the portable Router AP in the testbed, the proposed detection is based on the following assumption as shown in Figure 2. The portable Router AP as RAP is set up without permission in public working areas, such as in the office or notebook plug-in area in the library. The RAP set by the attacker is connected to the network interface by cable. As to LAP, it is provided by the public area mentioned above. Both of them are within the same local area network, which has to set the same Domain Name Service (DNS) to open the web pages. With the assumption, our detection method could ensure that the testbed conform to the attack option used in the proposed detection — using a single ISP gateway to provide the Internet service

Besides, using iStumbler to obtain details about access points, it could confirm that the protocol, Wi-Fi channel and frequency of LAP and RAP are the same. The signal strength was also extremely close in detection testbed. By controlling all the related attributes of the access point, researchers could get more accurate experimental data in our proposed ETA detection.

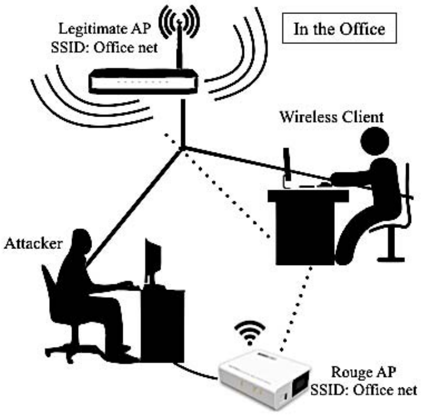


Figure 2. Illustration of our testbed in proposed ETA detection.

B. *Proposed Detection Design*

The proposed detection takes advantage of the portable router AP which is now popular with travelers and office workers due to its convenience, affordable price, and high accessibility. Moreover, multifunction is the most impressive advantage which are listed below. First, it can easily switch between Wi-Fi access point and router and be a Wi-Fi repeater in order to get better Wi-Fi quality as well as wider coverage. Secondly, it provides several connection modes including Point-to-Point Protocol over Ethernet (PPPoE), Static IP and Dynamic Host Configuration Protocol (DHCP). In addition, it could also support various encryption modes to strengthen Wi-Fi security. Last but not the least, it could be used for Network Address Translator (NAT) and Virtual Private Network (VPN) provider. Bringing with such useful and convenient elements, the office workers and the travelers could easily turn the Ethernet to Wi-Fi or extend Wi-Fi coverage, then enjoying the better wireless network accessing environment. Given that the portable AP are in great demand nowadays, and it might be taken as an instrument for ETA attack with high possibility, researchers will make it as RAP in our proposed detection.

In the testbed, researchers assumed that the attacker made use of TOTO-LINK iPuppy III Wireless N Portable AP as a RAP. The RAP is connected to the network interface by cable and both RAP and LAP are in the same local area network. The Wi-Fi interface card of wireless client using is AirPort Extreme. Figure 3 illustrates our proposed ETA detection tested setup. The detection method design depends on the four-way handshake in the TCP connection termination. By observing the time delay of packets transfer between the LAP and RAP at the moment that the webpage is closed, it can distinguish whether two APs with the same SSID is RAP or not.

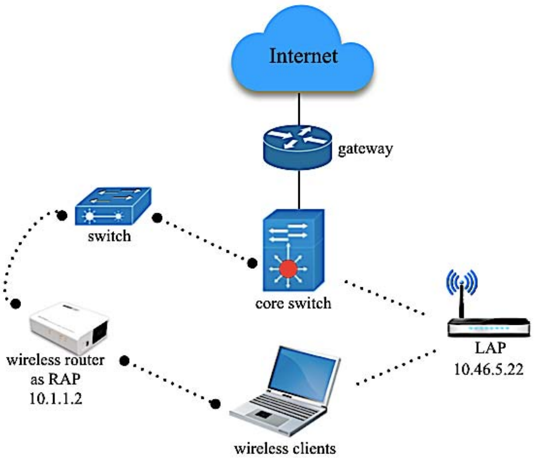


Figure 3. Proposed ETA detection testbed setup.

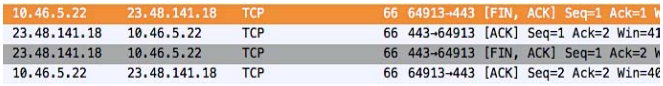
C. *Implementation*

The ETA detection client-side software was running on Mac OS Sierra 10.12.4. First of all, researchers made the wireless network connect to the LAP and opened the web browser and visiting the website www.apple.com afterward. To ensure that the webpage had been fully downloaded from the web server and prevent the website from connecting abnormally, researchers had viewed the website for 5 seconds averagely each time. After closing the browser to observe TCP four-way handshake, researchers repeated the same operations for forty times. Further, with wireless network switched to the RAP, the test mentioned previously was also launched for forty times. The web server could be any arbitrary server since the TCP connection will definitely launch four-way handshake with opening and closing the webpage.

V. Evaluation Procedure

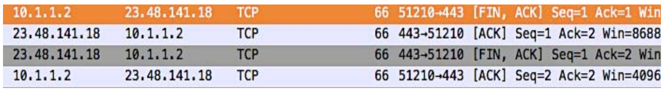
Wireshark collected the TCP packets of webpage opening and closing 40 times for RAP and LAP. After filtering out the irrelevant packets, researchers could clearly make out the packets transferring process of TCP connection termination.

Among the collected packets, there were several ports address from wireless network client side which used in the four-way handshake in the TCP connection termination. Therefore, researchers sorted out about 3-4 sets of packets in every operation and calculated the time delay between packets in the termination procedure: Initial Ending, Ending Response, and Confirmed Ending. The total number of packet-set was nearly 120 sets, which contained the complete process of TCP connection termination in each set, as shown in Figure 4 and Figure 5. The source IP addresses in the scenario belonged to the LAP and RAP respectively. The remote Apple website had an IP address 23.48.141.18 belonging to Akamai Technologies, which is the one of the world’s largest distributed computing platforms, and Apple Inc. is one of its clients.



```
10.46.5.22     23.48.141.18   TCP            66  64913→443 [FIN, ACK] Seq=1 Ack=1 W
23.48.141.18   10.46.5.22     TCP            66  443→64913 [ACK] Seq=1 Ack=2 Win=41
23.48.141.18   10.46.5.22     TCP            66  443→64913 [FIN, ACK] Seq=1 Ack=2 W
10.46.5.22     23.48.141.18   TCP            66  64913→443 [ACK] Seq=2 Ack=2 Win=40
```

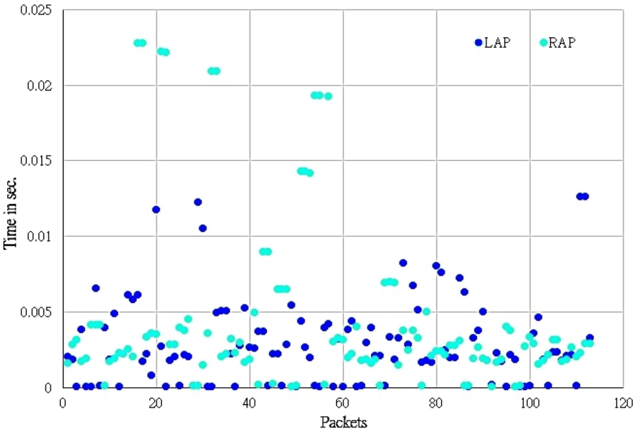
Figure 4. The source IP address (10.46.5.22) is the Legitimate Access Point, which is in private IP address range for the testing environment.



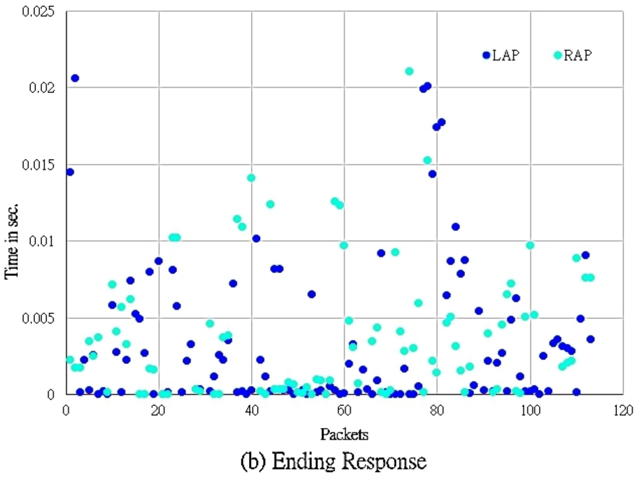
```
10.1.1.2       23.48.141.18   TCP            66  51210→443 [FIN, ACK] Seq=1 Ack=1 Win
23.48.141.18   10.1.1.2       TCP            66  443→51210 [ACK] Seq=1 Ack=2 Win=8688
23.48.141.18   10.1.1.2       TCP            66  443→51210 [FIN, ACK] Seq=1 Ack=2 Win
10.1.1.2       23.48.141.18   TCP            66  51210→443 [ACK] Seq=2 Ack=2 Win=4096
```

Figure 5. The source IP address (10.1.1.2) is the Rogue Access Point, which was set in private IP address range as the LAP in the testing environment.

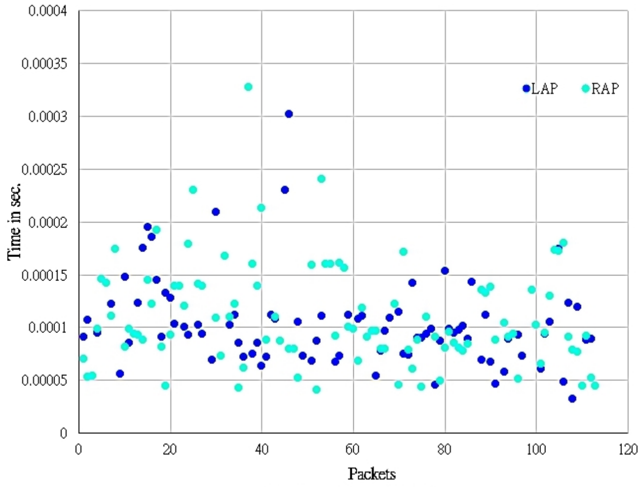
Figure 6 illustrates the experimental data of the testbed measurements for time intervals. It could show that the RAP took relatively long time in Initial Ending than the other two intervals. Figure 7 also shows the average value and sum of time intervals. Both of two statistical charts yield the same conclusion and there are apparent differences in time delay between LAP and RAP in Figure 7. Table 1 gave the statistical results of time intervals and average time duration in TCP connection termination in the proposed ETA detection. Since Confirmed Ending is the period of time for the server to wait for the webpage closing down, this interval generally took longer time than the others time intervals. Despite the fact that there were some packets took extremely more time to transfer between client side and server side, leading to that part of the statistical result of each time interval shown in figure 6 and Table 1 seems illogical, the sum and average value as shown in Figure 7 and Table 1 still support our assumption of proposed ETA detection. That is, the generalization derived from the time delay data in TCP connection termination agreed with our assumption that the packets transferring between clients side and server side using RAP took significantly more time than using LAP.



(a) Initial Ending

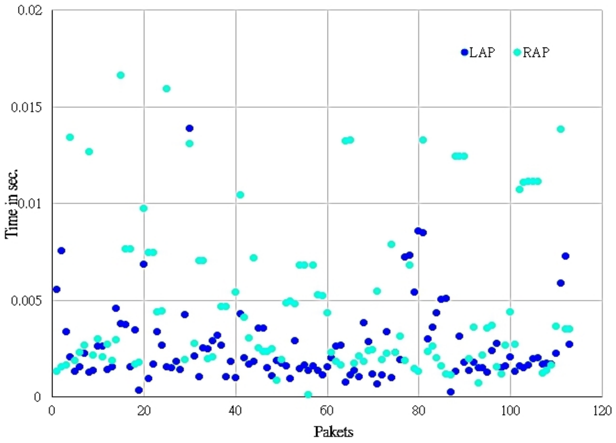


(b) Ending Response

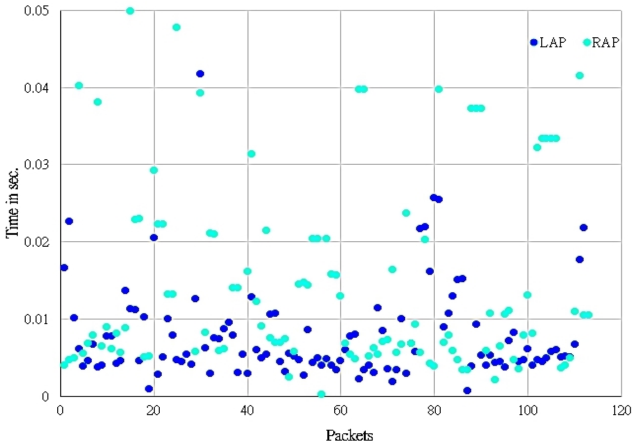


(c) Confirmed Ending

Figure 6. Three time-delays between packets in the TCP termination procedure for ETA detection. (a) Initial Ending (b) Ending Response (c) Confirmed Ending.



(a) Average Value



(b) Sum

Figure 7. The sum and the average value of three time intervals in the TCP termination procedure for ETA detection. (a)Sum (b) Average Value.

TABLE 1. AVERAGE VALUE OF TIME INTERVALS

LAP/RAP Time Intervals	Detection time in sec Using Legitimate access point	Detection time in sec Using Rogue access point
Initial Ending	0.00327695	0.00443718
Ending Response	0.00360042	0.01958561
Confirmed Ending	0.00124400	0.00181559
Average value of three time intervals	0.00270713	0.00861279
Average value of time duration to finish termination	0.00812138	0.02583839

VI. DISCUSSION AND LIMITATIONS

This paper proposes the detection method of the ETA using the single ISP gateway. If the method is combined with ETA detection of the ETA using the different gateways, then nearly all kinds of MIMA could be detected. The proposed ETA detection only involves the one legitimate AP and a rogue AP in the office. If there are more than two AP in the environment, the wireless could also make use of the detection method, and distinguish LAP and RAP by comparison the time intervals of TCP connection termination. Compared with [10], the proposed method could be more intuitive and convenient. Without any algorithm, it could readily detect out the rogue access point. The ETA detection method could be easily operated, without any Wi-Fi's network fingerprint or train data, which makes it more preferable for the wireless network customer, such as office worker, travelers in hotels and the public. With universality and accessibility of the portable AP increasing, the proposed detection method could play its full role.

The limitation of the ETA detection scheme will be listed below. First, our ETA detection method focuses on ETA using single ISP gateway. If the attacker launches the ETA by using different ISP gateways, our detection method could probably not work out. But it still has the possibility to detect, and researchers will make intensive study in the future work.

Second, when the clients launch the detection method, it will need to collect more than 20 sets of packets for the four-way handshake. That is, the clients have to open and close the webpage for 3 to 4 times in order to collect enough packets sets and measure the duration of the TCP connection termination. Therefore, with every webpage opening for 5 seconds then closing, the whole detection process will take about one minute including the data-analysis time. It will be slightly time-consuming to operate the detection method.

Third, the time-based method could be affected by several factors, such as the received signal Strength Indicator (RSSI), data traffic load, Internet speed, DNS response time, and so on. Those factors may vary the propagation delay time of packets between the client side and the server sides. Despite the fact that the time-based method could suffer from the elements mentioned above, time-delay evaluation still plays a vital role in packets analysis. Although it will be challenging, researchers will continuously concentrate on making the improvement of the solution in the future work.

Finally, if there is only the RAP in the environment without any LAP, the detection method would not work out successfully. Since the method distinguished the LAP from RAP by comparing the time-delay difference of packets transferring in our ETA detection, it will be limited to detect the RAP directly without any LAP as the control group.

VII. Conclusions

This paper proposed a real-time client-side ETA detection of ETA using single ISP gateway. Since there will be an extra switch or wireless hop for the portable AP as a rogue access point to establish the network connection, it will take more time to transfer the packets. In proposed detection, researchers measured the duration of TCP connection detection procedure and analyzed three time interval: Initial Ending, Ending Response, and Confirmed Ending to distinguish the LAP from RAP. The detection technique is a lightweight and client-side method. Furthermore, the detection method was prototyped and implemented in real life scenarios with high detection rate. Finally, the detection technique could be combined with other detection using different ISP gateways, to enhance the detection rate and provide an all-around detection method.

Acknowledgment

This research was partially supported by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-107) and the Ministry of Science and Technology of the Republic of China under the Grants MOST 106-2221-E-015-002-.

References

[1] Oriyano, S. P., *CEH v9: Certified Ethical Hacker Version 9 Study Guide (3rd Edition)*, John Wiley & Sons, Inc., pp. 1-222, 2016.

[2] Modi, V. and Parekh, C., "Detection & Analysis of Evil Twin Attack in Wireless Network," *International Journal of Advanced Research in Computer Science*, Vol. 8, No. 5, pp. 774-777, 2017.

[3] Ramachandran, V. and Buchanan, C. *Kali Linux Wireless Penetration Testing*: Beginner's Guide, Packt Publishing Ltd, pp. 117-135, 2015.

[4] Yu, J., "Applying TCP Profiling to Detect Wireless Rogue Access Point," *Proceedings of The 2014 World Congress in Computer Science, Computer Engineering, and Applied Computing*, pp. 1-7, 2014.

[5] Xie, G., He, T., and Zhang, G., *"Rogue access point detection using segmental TCP jitter*." Proceedings of the 17th International Conference on World Wide Web, pp. 1249-1250, 2008.

[6] Zhang, F., He, W., Liu, X., and Bridges, P. G., *"Inferring users' online activities through traffic analysis,*" Proceedings of the fourth ACM conference on Wireless network security, pp. 59-70, 2011.

[7] Nakhila, O., Dondyk, E., Amjad, M. F., and Zou, C., "User-side Wi-Fi Evil Twin Attack Detection Using SSL/TCP Protocols." *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 239-244, 2015.

[8] Sak, B. and Ram, J. R., *Mastering Kali Linux Wireless Pentesting*, Packt Publishing Ltd, pp.145-180, 2016.

[9] Nakhila, O. and Zou, C., "User-side Wi-Fi Evil Twin Attack Detection Using Random Wireless Channel Monitoring," 2016 *IEEE Military Communications Conference (MILCOM)*, pp. 1243-1248, 2016.

[10] Yang, C., Song, Y., and Gu, G., "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.

[11] Song, Y., Yang, C., and Gu, G., "Who Is Peeping at Your Passwords at Starbucks?—To Catch an Evil Twin Access Point," *2010 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 323-332, 2010.

En-Chun Kuo is a student at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan

Ming-Sang Chang is a Professor at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. His academic research interests include broadband network, performance analysis, and network planning.

Da-Yu Kao is an Associate Professor at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. With a Master degree in Information Management and a Ph.D. degree in Crime Prevention and Correction, he had led several investigations in cooperation with police agencies from other countries for the past 20 years. He can be reached at camel@mail.cpu.edu.tw.