Evil-Twin Detection on Client-side

Songrit Kitisriworapan
Department of Computer Engineering
Kasetsart University
Chatuchak, Bangkok, Thailand
songrittom@gmail.com

Aphirak Jansang
Department of Computer Engineering
Kasetsart University
Chatuchak, Bangkok, Thailand
aphirak.j@ku.ac.th

Anan Phonphoem*
Department of Computer Engineering
Kasetsart University
Chatuchak, Bangkok, Thailand
anan.p@ku.ac.th

***Abstract*—The unauthorized access is an important security threat in wireless networks. However, a user that might be deceived for connecting to a rouge access point is also quite dangerous scenario. The rouge access point, called Evil-Twin (ET), can be easily setup without users' noticeability. An attacker might eavesdrop or redirect the traffic for hacking or phishing purposes. In this paper, an Evil-Twin detection on client-side has been proposed. By investigating the frame RTT and its corresponding MCS, the simulation results revealed that the mechanism can be able to correctly identify the existing of ET. The implementation is also very simple by requiring user to move around the area for collecting data.**

***Keywords*—Wireless intrusion detection, Wireless evil-twin attack, ET detection, Unauthorized access, Man-in-the-middle**

I. Introduction

The availability of public WiFi is currently common in the city. However, regular users might not be realized that they are connecting to a non-legitimate access point (AP) setup by an attacker. These rouge access points, called Evil-Twin (ET), masquerades itself to act as a regular legitimate AP by using the same SSID. The attacker might also provide higher transmission power of ET than normal regulations which cause more preferable for the user's device to automatically connect. The ET can be easily setup by using a regular notebook computer, mobile phone, or a cheap SOHO grade AP which can be installed nearby the target user without the awareness of the network administrator or regular users. Hence, the ET becomes MitM (Man-in-the-middle attack) which can create serious security problems to the current connected users by eavesdropping or editing the current data traffic especially when sensitive information has been transferred.

In traditional method, the ET Attack (ETA) detection can be implemented at the Network or Host level, called Network-based IDS (NIDS) and Host-based IDS (HIDS) respectively. For network level, a monitoring device is necessary to be installed inside the target network for collecting and analysing. Although the network information will be quite completely collected, extra devices and operation cost are required. In contrast, for host level, an software agent is mandatory installed on the user device for monitoring any unusual behaviour appeared in the event log without the network administration involvement. It is also called user-side detection. Even though only the limited information passing in and out its own device can be utilized, the abnormally behaviour is still be able to detect with acceptable accuracy. Furthermore, for implementation, it is much more convenient for users than the network level detection.

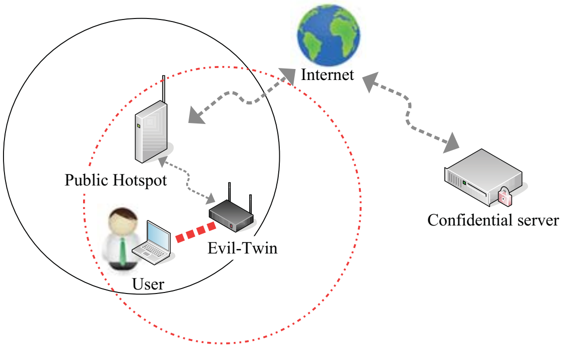


Fig. 1: System overview

Normally most commercial security products aim for protecting the network from unauthorised access to their premises. Some example security products [1]–[4] provide devices' management tools for periodically scanning and detecting any unauthorized access into the network. However, the security concern is obviously not for protecting users for using WiFi in the public area. Moreover, the vulnerability study in WPA [5] also found that it is possible for an attacker to create the ET in the present of WPA.

In this research, the ET existence detection technique by using RTT (Round Trip Time) and MCS (Modulation Coding Scheme) value collected from user's device has been proposed. The performance of the mechanism has been evaluated by the network simulator 3 (NS3).

II. Literature Review

The ET existence detection on wireless networks by using statistical techniques can be found in [6] [7]. However, by collecting traffic data without permission, users might encounter with serious legal issues due to the organization security policy.

The client-side detection, host level, efforts can be found in [8], [9]. The key concept is to capture the abnormal delay in the wireless direct link to AP. The system firstly records

* Corresponding Author

978-1-7281-3361-4/19/$31.00 ©2019 IEEE

Authorized licensed use limited to: SHIBAURA INSTITUTE OF TECHNOLOGY. Downloaded on February 02,2023 at 06:44:37 UTC from IEEE Xplore. Restrictions apply.

the reference delay, by sending some probing frame in the wireless direct link to the DNS server. Then the reference delay will later be used for comparing with the acquired delay. By using the statistical differentiate of RTT, the multi-hop connection can be noticed. If the delay difference is over a dynamic threshold, the system reports the existence detection of ET.

The enhanced rouge AP detection technique [10] by using temperature along with clock skew for improving the detection accuracy has been proposed. Clock synchronization is one of the most fundamental communication issues. By connecting to an AP, the clock of users' device will be synchonized with the AP's clock. Later on the clock for each device might drift and no longer synchonized due to physical properties of the hardware device including the battery life [11] which can be used for detecting the rouge AP. Of course, clock skew modelling is not a straight forward task.

Many more works on detecting are under investigation. Researchers [7] proposed the detection mechanism by using inter packet time (IPT) of the TCP-Ack pair via an access point. While [12] proposed the eavesdropping technique to monitor an access point via LAN. [13] proposed to use the received signal strength indicator (RSSI) for generating a fingerprint of the genuine AP for detecting the ET.

III. The proposed mechanism

The main focus of our studies is to distinguish between the single-hop (to a legitimate AP) and double-hop (to an ET access point) WiFi connection as shown in Fig. 1. The proposed mechanism has been implemented as the client-side detection. For a public location that might be the first time visit for a user, there will be no known information beforehand. Once users try to make WiFi connection, they themselves should be able to check for the existence of ET, with a certain level of confidence.

To identify the ET, the differences of frames' round trip time (RTT) will be used for making decision. After moving around for a certain locations, at each position, 10 frames are collected for corresponding RTT and MCS which later be averaged and compared to the decision condition as shown in Table I. However, each RTT can varied according to the current link condition. Generally, the driver of the WiFi NIC promptly select a suitable MCS based on the received signal quality. From the selected MCS index, the physical transmission rate, $PhyTxRate$, will be chosen.

The RTT depends on the communication delay in the link layer. The delay mainly composes of queueing (d_q) and transmission delay(d_{tr}). The queueing delay varies according to the amount of transferring traffic, while the transmission delay has been changed according to the packet size and its transmission rate. Each frame d_{tr} can be calculated as shown in Eq. 1 which varies according to $PhyTxRate$.

$$d_{tr} = \frac{F_{size}}{PhyTxRate} \tag{1}$$

F_{size} represents the size of Ethernet maximum transfer unit (MTU) frame.

In this paper, the ping packets are used for calculated the RTT. Hence, with IP header, ICMP header and ICMP payload of 20, 8 and 1,472 bytes, respectively, the F_{size} becomes 1,500 bytes as regular MTU frame.

The reliability of ET detection depends on the amount of RTT data. To get the sufficient amount of different RTT values, users have to move around the current location. For each move, both RTT and corresponding MCS will be collected and compared with other locations. In our assumption, with the same MCS value, the RTT value should be nearly the same. Otherwise, the double-hop connection possibly occur which means that, in the surveying area, the ET might exist.

In regular single-hop connection condition, with the low MCS value (low physical data rate), the corresponding RTT should be high. In contrast, with high MCS value (high physical data rate), the corresponding RTT should be low. Otherwise the double-hop connection via ET might occur in case of high MCS value with also high RTT. However, in some cases that both MCS and RTT become low, it is unsuitable for making any conclusion. The decision condition can be summarized in Table I.

TABLE I: Decision conditional for ET detection

MCS value	RTT value	Decision
high ↑	high ↑	ET potentially exists
low ↓	high ↑	no ET exist
high ↑	low ↓	no ET exist
low ↓	low ↓	inconclusiveness

IV. Performance Evaluation

The test scenario are setup as shown in Fig. 2. ST stands for the user station or user's device. AP and ET represent the legitimate access point and ET access point, respectively. In the experiment, the traffic load at the AP are generated by regular devices. Each node represents one traffic stream. The number of nodes is varied from one to n. d_2 represents the distance between the ET and AP. Meanwhile, d_1 represents the distance between ST and connecting AP which can be distinguished into two cases: connect to ET as shown in Fig. 2a or directly connect to legitimate AP as shown in Fig. 2b.

A. Simulation Setup

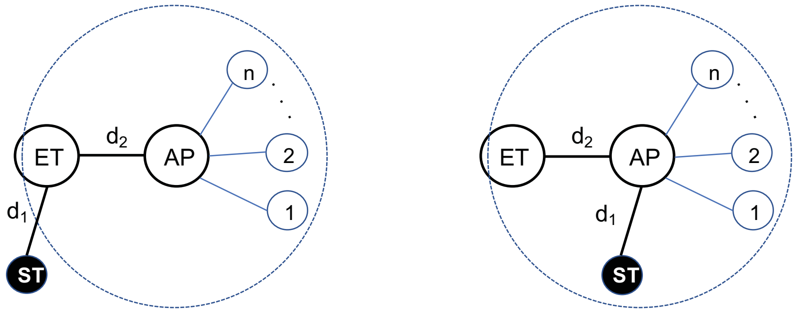
Our proposed mechanism has been evaluated by the network simulator 3 (NS3) version 3.26. The setup parameters show in Table II.

The user's device (ST) traffic is generated based on the v4ping model in NS3. Due to the limited RTT timing report which only shown in millisecond, in our experiment, the v4ping model has been modified to report in microsecond level. The source code can be found in [14].

B. Simulation Results

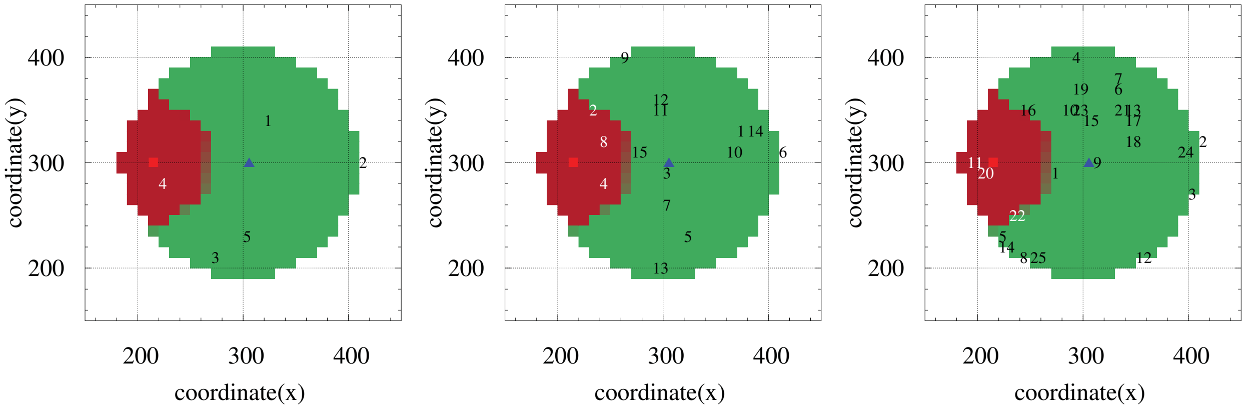
The area of 500 x 500 meters are defined as a visiting site. AP locates at position (300,300), while ET locates at position

Authorized licensed use limited to: SHIBAURA INSTITUTE OF TECHNOLOGY. Downloaded on February 02,2023 at 06:44:37 UTC from IEEE Xplore. Restrictions apply.



(a) Double-hop connection (b) Single-hop connection

Fig. 2: Testing scenarios



(a) Five moving positions (b) Fifteen moving positions (c) Twenty-five moving positions

Fig. 3: Examples of moving patterns in an experiment

TABLE II: NS3 setup parameters

Parameter	Value
Number ICMP per test	10 packets
ICMP Interval	10pkt/s
ICMP payload size	1472 bytes
GuardInterval	800ns
RTS Threshold	65535 bytes
Rate control algorithms	MinstrelHtWifiManager
SetSeed	12
SetRun	5
Simulation Time	10s

(220,300). For the experiment, the user randomly walks around the site. For each move, the user may automatically connect to AP or ET according to the received signal strength.

In Fig. 3a, a user made five moves. Only one out of five positions felt into the double-hop connection zone (20%), the rest were in the single-hop zone. In this case, the algorithm wrongly reported that no ET existed. However, in Fig. 3b, Fifteen moves were simulated. For the case of two positions felt in the double-hop connection zone (20%), the algorithm reported that ET existed.

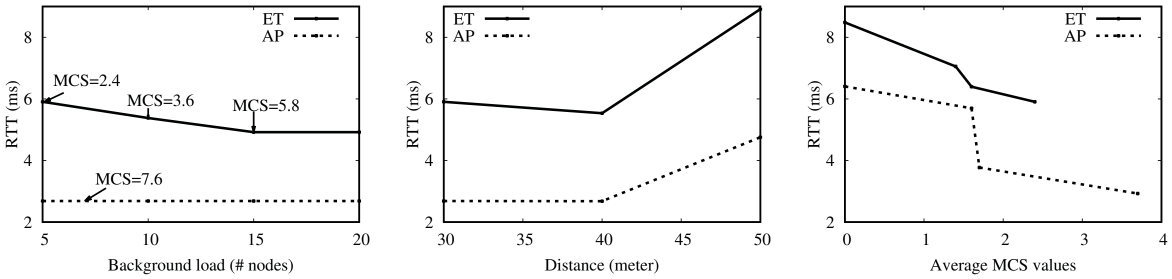
Similarly, Fig. 3c shown the simulation of Twenty-five moves. In the case of 12% of moving location felt into the double-hop connection zone, the algorithm also correctly reported the existing of ET.

Moreover, the proposed mechanism has been further investigated for various parameters. Fig. 4 displayed the simulation results of RTT by varying the AP's Load, distance between ET and AP (d_2) and MCS values. The results shown that RTTs of single-hop connection are always lower than the double-hop connections with all cases. By increasing the number of moving locations, the results revealed that more moves gave higher ET detection rate as shown in Fig. 5. However, the results might vary according to the randomly moving patterns.

V. Discussion and Conclusion

The wireless Evil-Twin attack can create dangerous security threats, especially for public location that a user has never been visited. By simply investigating the RTT of the ping probing frames, the user might be able to identify the existing of ET. However, only RTT cannot accurately be used for identification. The proposed mechanism found that by using

Authorized licensed use limited to: SHIBAURA INSTITUTE OF TECHNOLOGY. Downloaded on February 02,2023 at 06:44:37 UTC from IEEE Xplore. Restrictions apply.



(a) Traffic load at AP (b) d_2 distance (c) MCS index

Fig. 4: RTT values with various parameters

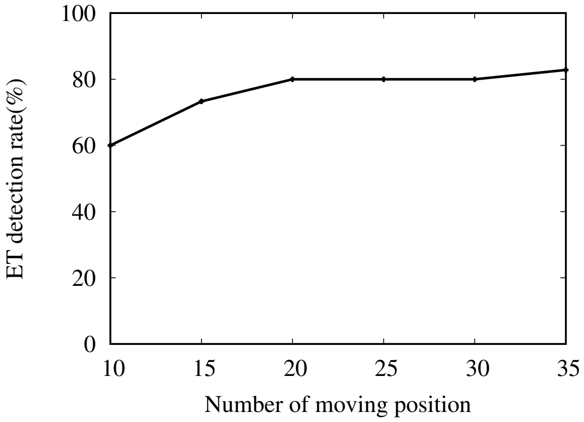


Fig. 5: ET Detection Rate

RTT values along with the corresponding frame MCS and other load parameters, the detection rate has been increased. However, more wireless parameters and scenarios are required for further investigated such as more than one ET coexisting, user's moving patterns, or higher physical data rate of IEEE802.11 standard.

Acknowledgment

This work has been partially supported by Kasetsart University Research and Development Institute, Ref.2017/2560: P-Y(D)144.60.

References

[1] M. OpUtils. (2019, Feb) Rogue device detection software. [Online]. Available: https://www.manageengine.com

[2] ESET. (2019, Feb) Rogue detection sensor. [Online]. Available: https://www.eset.com

[3] McAfee. (2019, Feb) Rogue system detection. [Online]. Available: https://www.mcafee.com

[4] ESET. (2019, Feb) Rogue management in a unified wireless network. [Online]. Available: https://www.cisco.com

[5] A. Bartoli, E. Medvet, and F. Onesti, "Evil twins and WPA2 Enterprise: A coming security disaster?" *Computers & Security*, vol. 74, pp. 1 – 11, 2018.

[6] C. D. Mano, A. Blaich, Q. Liao, Y. Jiang, D. A. Cieslak, D. C. Salyers, and A. Striegel, "RIPPS: Rogue identifying packet payload slicer detecting unauthorized wireless hosts through network traffic conditioning," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 2, pp. 2:1–2:23, May 2008. [Online]. Available: http://doi.acm.org/10.1145/1330332.1330334

[7] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, "Passive online rogue access point detection using sequential hypothesis testing with tcp ack-pairs," in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*. ACM, 2007, pp. 365–378.

[8] H. Han, B. Sheng, C. Tan, Q. Li, and S. Lu, "A measurement based rogue ap detection scheme," in *INFOCOM 2009, IEEE*, April 2009, pp. 1593–1601.

[9] ——, "A timing-based scheme for rogue ap detection," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 22, no. 11, pp. 1912–1925, Nov 2011.

[10] 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*, ser. ASIA CCS '14. New York, NY, USA: ACM, 2014, pp. 3–14. [Online]. Available: http://doi.acm.org/10.1145/2590296.2590333

[11] C. Arackaparambil, S. Bratus, A. Shubina, and D. Kotz, "On the reliability of wireless fingerprinting using clock skews," in *Proceedings of the third ACM conference on Wireless network security*. ACM, 2010, pp. 169–174.

[12] S. Shetty, M. Song, and L. Ma, "Rogue access point detection by analyzing network traffic characteristics," in *Military Communications Conference, 2007. MILCOM 2007. IEEE.* IEEE, 2007, pp. 1–7.

[13] Z. Tang, Y. Zhao, L. Yang, S. Qi, D. Fang, X. Chen, X. Gong, and Z. Wang, "Exploiting wireless received signal strength indicators to detect evil-twin attacks in smart homes," *Mobile Information Systems*, vol. 2017, 2017.

[14] S. Kitisriworapan. (2019, Feb) An application which sends one icmp echo request, waits for a replys and reports the calculated rtt. [Online]. Available: https://goo.gl/1nfM3Z

Authorized licensed use limited to: SHIBAURA INSTITUTE OF TECHNOLOGY. Downloaded on February 02,2023 at 06:44:37 UTC from IEEE Xplore. Restrictions apply.