COMPUTERS & SECURITY 74 (2018) 41–54

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Gateway independent user-side wi-fi Evil Twin Attack detection using virtual wireless clients

Omar Nakhila [a,*], *Muhammad Faisal Amjad* [b], *Erich Dondyk* [c], *Cliff Zou* [d]

[a] *Department of Electrical & Computer Engineering, University of Central Florida, FL, USA*
[b] *National University of Sciences and Technology, Islamabad, Pakistan*
[c] *Amazon.com, Inc., Cambridge, Massachusetts, USA*
[d] *Department of Computer Science, University of Central Florida, FL, USA*

ARTICLE INFO

Article history:
Received 26 May 2017
Received in revised form 10 December 2017
Accepted 17 December 2017
Available online 28 December 2017

Keywords:
Wi-Fi security
Evil Twin Attack
LORCON
Open WiFiHop
Virtual wireless client

ABSTRACT

Complimentary open Wi-Fi networks offered by most coffee shops, fast food restaurants and airports are inherently insecure. An attacker can easily deceive a wireless client (WC) by setting up a rogue access point (RAP) impersonating the legitimate access point (LAP), which is usually referred as Evil Twin Attack (ETA). To pass a victim's wireless data through to the Internet, an attacker may use the same LAP's gateway, or use a different gateway, such as broadband cellular connection. Most of the existing ETA detection techniques assume that the attacker will use a specific wireless network gateway to pass victim's wireless data. In this paper, we present a real-time client-side detection scheme to detect ETA regardless of the attacker's gateway selection. The proposed ETA detection system considers both ETA scenarios in parallel by creating two Virtual Wireless Clients (VWCs). The first VWC monitors multiple Wi-Fi channels in a random order looking for specific data packets sent by a server on the Internet. Meanwhile, the second VWC warns the WC when the wireless network uses two different gateways by switching from one AP to another in the middle of a secure connection. The effectiveness of the proposed detection method has been mathematically modeled, prototyped and evaluated in real-life environment with a detection rate close to 100%.

1. Introduction

Wireless networks provide connectivity to the Internet for smart phones, mobile PCs and tablets. The growth and use of wireless devices has increased data traffic on cellular networks (Ericsson, 2015). Some businesses such as coffee shops, fast food restaurants and airports offer free Wi-Fi services to their clients. Besides offloading data traffic from cellular networks (Seufert et al., 2016), the use of Wi-Fi provides a fast and budget friendly alternative to a wireless client (WC) when it comes to accessing the Internet (Lanze et al., 2015). However, for ease of access, these Wi-Fi networks provide no security in terms of authentication or encryption. When a WC wants to access a Wi-Fi network, she must agree to the "Public Wi-Fi Access Terms and Conditions" in which the Wi-Fi provider assumes no responsibility for the security/privacy of the WC's information (Mustafa and Xu, 2014).

Insecure Wi-Fi networks provide a tempting environment for attackers to initiate many attacks, one of them is called Evil

* *Corresponding author.*
E-mail address: omar_hachum@knights.ucf.edu (O. Nakhila).
https://doi.org/10.1016/j.cose.2017.12.009
0167-4048/

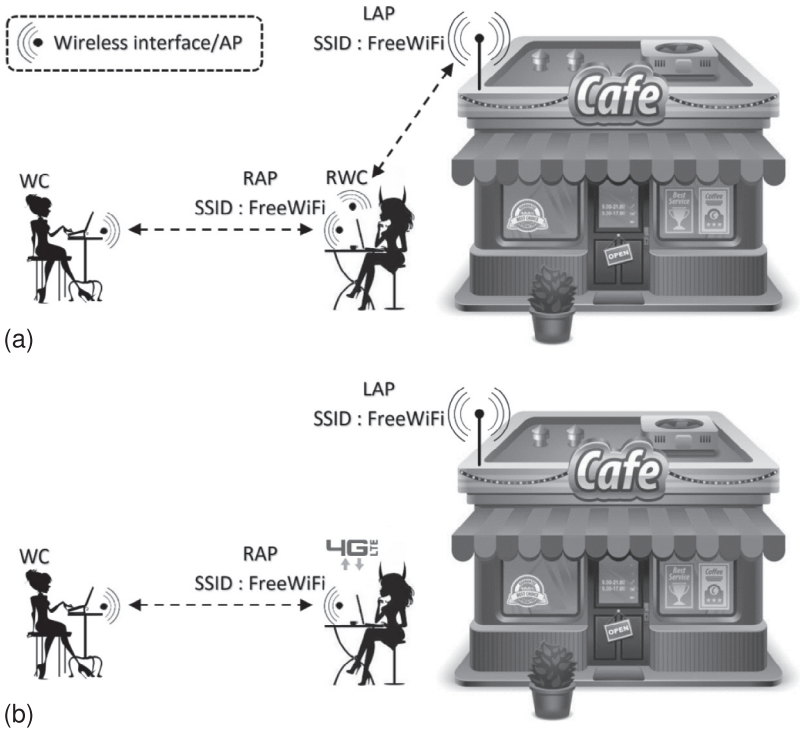


Fig. 1 – Illustration of ETA scenarios. The RAP can successfully lure WC connecting to it instead of the LAP when it provides stronger/better signal to those WCs. (a) Evil twin attack using single ISP gateway. The attacker pass through WC data to the Internet using LAP. (b) Evil twin attack using different ISP gateways. The attacker uses her own mobile data connection (4G-LTE) to pass through WC data to the Internet.

Twin Attack (ETA) as illustrated in Fig. 1. ETA refers to a Wi-Fi rogue access point (RAP) impersonating a legitimate access point (LAP) to eavesdrop WC's Wi-Fi data (Lanze et al., 2015; Mustafa and Xu, 2014; Nikbakhsh et al., 2012; Panch and Kumar Singh, 2010; Song et al., 2010; Yang et al., 2012). Since a Wi-Fi network can only be recognized by its SSID and MAC address, the attacker can set up a RAP with the same SSID of the LAP. Furthermore, the attacker's RAP may have better and more powerful signal than the LAP, which will lure the WC to connect to it first (Intel, 2014).

After the WC connects to the RAP, the attacker can snoop on the WC's data traffic and/or launch man-in-the-middle attack (MIMA). For example, using ETA, an attacker can infer mobile keystroke by detecting the change in the channel state information when the wireless client moves her hand and fingers. Mobile keystroke can be recognized even when the wireless client is using HTTPS. Another example, SSL strip attack (Marlinspike, 2009) that forces the WC to use HTTP instead of HTTPS. Furthermore, DNS spoofing attack (van Rijswijk-Deij et al., 2014) where the WC receives incorrect IP address when requesting a certain domain. This results in directing the WC to visit malicious website rather than the actual website.

Once the WC is connected to the RAP, the attacker have two options to direct WC's data traffic to the Internet. First, the attacker can use another Wi-Fi interface card and connect to the LAP as a rogue wireless client (RWC). The attacker use the RWC to pass the WC traffic to the Internet. Both LAP and RAP use the same ISP gateway as shown in Fig. 1a. Hence, we call this attack option as *ETA using single ISP gateway*.

The attacker has another option to avoid connecting to the LAP. Due to the increase in Internet access speed of mobile broadband connections, such as 4G Long Term Evolution (LTE) or WiMAX, the attacker can use her own cellular broadband link to connect the WC to the Internet (Nikbakhsh et al., 2012; Yang et al., 2012). In this scenario, the attacker is placed between the RAP and her broadband connection as illustrated in Fig. 1b. We call this attack option as *ETA using different ISP gateways*.

Specifically, we have made the following contributions to the Wi-Fi security in this paper by:

- Presenting a novel detection method to deal with both types of ETA simultaneously. 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 (SMC Network, 2008).
- Furthermore, the proposed ETA detection will monitor multiple Wi-Fi channels in a random order looking for special wireless frames. These frames are sent from a dedicated public server on the Internet. By capturing these special wireless frames, WC can detect the ETA using single ISP gateway instantaneously.

- To speed up the detection process, each ETA detection procedure was carried out by a dedicated VWC. Using one wireless interface card, WC creates two VWCs to detect both ETA scenarios simultaneously.
- Our ETA detection is designed as a real time ETA detection solution for deployment on the client side which makes it more preferable than the network administrator side solutions (Song et al., 2010; Yang et al., 2012) since a WC can ensure her security without any assistance from network administrators. Also, the WC does not need to have any information about the Wi-Fi network configuration, any training data or fingerprints of the Wi-Fi network devices, as required by existing solutions (Lanze et al., 2014; Mustafa and Xu, 2014)
- Finally, we have presented the evaluation of our detection technique, whose effectiveness was mathematically modeled, prototyped and evaluated in real life environment.

Table 1 – Notations and acronyms.

Notation	Definition
ETA	Evil twin attack
WC	Wireless client
VWC	Virtual wireless client
AP	Access point
ISP	Internet service provider
LAP	Legitimate access point
RAP	Rogue access point
RWC	Rogue wireless client
4G (LTE)	4th Generation Long Term Evolution
P_d	Detection probability
P_m	Detection missing probability
N	Number of wireless channels
k	Attacker disconnect/connect from/to LAP
D	Time required by WC to switch between two APs
RTT	Round trip time
PIS	Public information server

2. Related work

ETA is an effective, yet simple to implement attack that targets Wi-Fi networks. To attract more clients, coffee shops and fast food restaurants tend to offer free Internet access via Wi-Fi networks. The attacker can use off the shelf Wi-Fi devices to initiate an ETA on these Wi-Fi networks. Also, the attacker can stop the attack at any point of the process making such attack untraceable (Song et al., 2010).

One can think of setting up VPN connection through any of the Wi-Fi APs as the panacea of ETA. Although, all the WC data traffic will be encrypted, VPN is not available for all users and has numerous points of failure (Scott et al., 1998).

ETA has caught the attention of researchers for many years. However, the detection methods proposed so far are partial (Lanze et al., 2015). Most ETA detection methods are bound to work in very specific environments. In Lanze et al. (2015), researchers divided ETA detection into three different categories: ① protocol modification, ② hardware fingerprinting and ③ non-hardware identification. On the other hand Song et al. (2010) and Yang et al. (2012), divide ETA detection into two categories: ① comparing data traffic at different locations of the Wi-Fi network with a known authorized list, and ② checking if the source of the data traffic is coming from a wireless or a wired network.

In this paper we classify ETA detection into two main categories: ① network administrative side, and ② client side detection. In network administrator side ETA detection, the network administrator will be responsible for detecting and/or assisting the WC to detect ETA. Since the network administrator will have all the information about the Wi-Fi network, she can have a list of fingerprints of all devices constructing the Wi-Fi network. Table 1 illustrates the notations and acronyms used throughout the paper.

A fingerprint is any information that can be used to distinguish a single device or a group of devices from another. For example, AP hardware and location can be used as a fingerprint. In Jana and Kasera (2010), AP clock skew was used as a fingerprint. Using clock skew as a fingerprint was further improved by Lanze et al. (2014). However, without having an authorized AP list beforehand, this ETA detection will fail. Also, AP location can be used as fingerprint. On the other hand, nearby AP may trigger a false positive of an ongoing ETA (Song et al., 2010).

Furthermore, the network administrative side detection will add more cost to the Wi-Fi network construction. The network operator may have to install wireless sensors and collect traffic data at the switch/router to be compared with the available fingerprint authorization list. Another key point in this type of detection, is that the WC will be unaware of the level of protection, (if any) that a specific Wi-Fi network is using against ETA. To sum up, administrator side ETA detection is limited, expensive and not available in many scenarios (Yang et al., 2012).

Client side ETA detection is the second category in our classification where the WC is solely responsible for detecting an ETA. This type of detection is preferred, as the WC is the one who will ensure her own security against ETA. In Nikbakhsh et al. (2012), the WC uses a traceroute command to display router's information between the WC and each router on the path to a certain destination. The WC executes a traceroute command to a certain destination through a random AP. After that, the WC switches to another AP and execute traceroute again to the same destination. If the route information using both APs are the same, then no ETA alarm will be triggered. On the other hand, if the information is not the same it means that one of the APs is RAP.

Although this ETA detection may succeed, it is vulnerable and limited. For instance, most network security administrators block traceroute commands from being executed for security purposes (Sherwood, 2008). Additionally, traceroute uses ICMP which is vulnerable to replay attack. The attacker can store the traceroute communication between the LAP and the WC and send it to the WC when she connects to the RAP.

Another client side detection is based on the extra time delay added between the attacker and the LAP (Song et al., 2010; Yang et al., 2012). The WC connects first to one of the APs and measures the propagation delay between the WC and a nearby DNS server. Next, the WC switches to the other AP and measures the propagation delay again to the same DNS server. The extra wireless link between the LAP and the

Table 2 – Illustrate different types of ETA detections. ETA detections that receive support from the legitimate network administrator (such as fingerprint list) is categorized as administrator side ETA detection since the detection method would fail without that support.

ETA Detection	Category		ETA ISP Gateway Detection		Limitations
	Administrator	Client	Single	Different	
Jana and Kasera (2010) and Lanze et al. (2014)	X		X	X	1 - APs fingerprints list must be collected beforehand (Jana and Kasera, 2010). 2 - APs must share the same temperature exposure (Lanze et al., 2014).
Song et al. (2010) and Yang et al. (2012)		X	X		1 - Fail to detect ETA using different ISP gateway (Song et al., 2010; Yang et al., 2012). 2 - Detection rate fluctuate with the traffic on each AP (Song et al., 2010; Yang et al., 2012).
Nikbakhsh et al. (2012)		X		X	1 - Fail to detect ETA using single ISP gateway (Nikbakhsh et al., 2012). 2 - Firewalls might filter ICMP echo request/reply (Sherwood, 2008). 3 - Vulnerable to replay attack (Sherwood, 2008).
Nakhila et al. (2015a)		X		X	1 - Fail to detect ETA using single ISP gateway (Nakhila et al., 2015a).
Nakhila and Zou (2016a)		X	X		1 - Fail to detect ETA using Different ISP gateway (Nakhila and Zou, 2016a).
Mónica and Ribeiro (2011)		X	X		1 - Fail to detect ETA using different ISP gateway (Mónica and Ribeiro, 2011). 2 - Vulnerable to replay attack (Nakhila and Zou, 2016a).
Proposed		X	X	X	None of the above

attacker will add more propagation delay compared to the direct connection of the WC to the LAP. Although this ETA detection method is effective, it suffers from wireless signal fluctuation and traffic load on the AP that may vary the propagation delay measurements (Yang et al., 2012). Also, the detection method fails if the attacker used ETA using different gateways.

Finally, our proposed ETA detection design is an extension of both Nakhila and Zou (2016a) and Nakhila et al. (2015a), whereas Nakhila et al. (2015a) used to detect ETA using different ISP gateways while Nakhila and Zou (2016a) used to detect ETA using single ISP gateway. In this work, we combined these two techniques using virtual wireless clients (Nakhila and Zou, 2016b; Nakhila et al., 2015b), a novel technique to overcome a major limitation in client side ETA detection. Most of the client side ETA detections that does not relay on training data or pre authorized fingerprint list are gateway dependent (Mónica and Ribeiro, 2011; Nakhila and Zou, 2016a; Nakhila et al., 2015a; Nikbakhsh et al., 2012; Song et al., 2010; Yang et al., 2012). The WC will fail to detect ETA, when she use an ETA detection different from the ETA type the attacker is running. However, our new comprehensive design is a gateway independent which limits the ETA false negative. Table 2 summarizes different ETA detections and their limitations.

3. 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 vulnerable solutions to the Evil Twin Attack.

3.1. *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 RAP 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.

We also assume that when ETA happens in a Wi-Fi hotspot, a WC can still receive signal from the LAP, thus it can detect that there are at least two APs with the same SSID. If a WC can only detect a single AP's wireless signal in a hotspot, we assume there is no Evil Twin attack.

3.2. *Intuitive detection schemes and their security problems*

An attacker attempting to launch an ETA has two options to connect to the Internet: using the same gateway as the LAP, or using a different gateway such as a cellphone data connection. In this paper, our ETA detection focuses on both types of ETAs and addresses each ETA type detection separately. To that end, we have combined both solutions for a comprehensive ETA detection using VWCs technique.

3.2.1. *ETA using single ISP gateway*

Open WiFiHop (Mónica and Ribeiro, 2011) is a client side detection of ETA using single ISP gateway. The detection structure is composed of a WC and a dedicated public server. First, the WC connects to a nearby AP and sends a watermarked packet to the public server. The watermarked packet is a random bit

stream that is only known to the WC. After the WC sends the watermarked packet to the public server, the WC immediately switches to other Wi-Fi channels looking for any transmission of the watermarked packet. The public server keeps replying this watermarked packet to the WC. If the WC captures the watermarked packet in other Wi-Fi channels then the initial AP is a RAP, otherwise it is LAP.

Based on the procedure described above, Open WiFiHop has the following vulnerabilities and limitations.

First, open WiFiHop is vulnerable to replay attack. The public server will only reply the watermarked packet to the WC without any modification. When the WC sends the watermarked packet to the public server, the attacker can store the watermarked packet and then disconnect from the LAP. The attacker can then start sending the stored watermarked packet to the WC. Since the attacker disconnected from the LAP, no watermarked packet will be sent on other Wi-Fi channels. In addition, when the WC returns back to the initial AP, the attacker can connect to the LAP. In this scenario, Open WiFiHop will fail to detect ETA.

Second, attacker can avoid Open WiFiHop detection by gathering information about the watermarked packets replay arrivals time and, the round trip time between the public server and the WC. When the WC sends the watermarked packet to the public server, she will immediately switch to other Wi-Fi channels looking for the watermarked packets (Mónica and Ribeiro, 2011). The attacker can simply disconnect from the LAP without even retransmitting the watermark packet since the WC is checking other Wi-Fi channels. When the WC returns back to the initial AP, the attacker can reconnect to the LAP. At this point, the WC will start receiving the watermarked packets from the public server. The attacker can also estimate when the WC returns to the initial AP simply by capturing the communication between the WC and the public server, which will pass through the attacker in the first place.

When the public server receives the watermarked packet, it will delay each reply by D time units, which is the time needed by the WC to switch from one AP to another. By measuring the time difference between two public server replies, the attacker can calculate D. Also, the WC will monitor each wireless channel by time $\geq (D + RTT)$ where RTT is the round trip time from the WC to the public server. RTT can be easily calculated since the initial communication between the WC and the public server went through the RAP.

In general, ETA detection security should not be based on information that can be gained, calculated and/or estimated by the attacker. Our proposed ETA detection using single ISP gateway procedure overcomes the vulnerabilities found in Mónica and Ribeiro (2011).

3.2.2. *ETA using different ISP gateways*

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 (Internet Engineering Task Force, 1981). 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's IP header. Based on that, in this detection method, the wireless client will send an IP packet using a given Access Point (for example AP_x) that belongs to the hotspot Wi-Fi network. Then, the wireless client will switch to another Access Point (for example AP_y) 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 the routers' addresses recorded in the IP header received from both AP_x and AP_y. Finally, the client can view the results on the server using any secure protocol.

However, similar to the traceroute packets (Nikbakhsh et al., 2012), record route packets may be dropped or ignored by many firewalls for security reasons (Sherwood, 2008). In addition, at most nine IP addresses can be recorded along the route whereas the average number of routers in any given route on the Internet is 19 to 21 (Albert et al., 1999).

2) *Detection based on TCP connection:* The second intuitive detection method that can be proposed to detect ETA using different gateways 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 AP_x) should have the wireless SSID name such as FreeWiFi (Fig. 1b) that belongs to hotspot Wi-Fi network. After connecting to AP_x, the wireless client will start a TCP 3-way handshake to a public server on the Internet. Each side (the wireless client and public server) 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 AP_x, the wireless client will then switch to a different AP (we call it AP_y) 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 AP_x. Changing the AP will have no effect on the socket information stored in each side of the connection. After switching to AP_y, the WC sends a heartbeat request to the public server.

If the two APs use the same gateway, the TCP connection will not be dropped and the wireless client should successfully receive a heartbeat response from the public server. Otherwise if the TCP connection is dropped, we know that these two APs are using different gateways. Using different gateways will prevent the public server from giving 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.

However, an attacker can conduct MIMA attack on the above detection method by impersonating the public server. This MITM can take place when the wireless client sends the heartbeat request though AP_y (which we assumed is the RAP) as shown in Fig. 2. The attacker intercepts the heartbeat request from the wireless client and starts a new connection to the public server and receives the heartbeat response. Then, because the attacker monitored the TCP connection setup between the client and AP_x (which we assumed is the LAP) at the first place, she can send the heartbeat response to the wireless client by continuing the existing TCP connection.

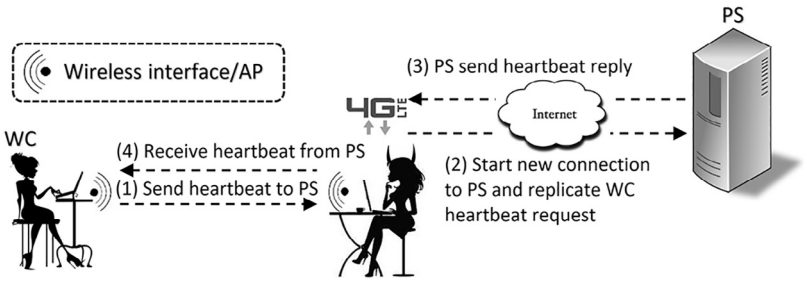


Fig. 2 – Possible man-in-the-middle attack on the ETA using different gateways detection that relies on TCP without secure connection where PS is a public server on the Internet.

4. Proposed ETA detection

4.1. *Assumptions*

For the detection of ETA using a single ISP gateway, our proposed detection system takes advantage of how the RAP/RWC send/receive data. When a WC send/receive data through the RAP, the same data will also be sent/received between the attacker's RWC and the LAP. The WC data will appear two times on the wireless channels. However, when there is no ETA, the same data could only appear once. A network administrator may extend 802.11 wireless coverage by installing more than one LAPs, however, these LAPs will be connected to the Internet using cables in which they will not replicate WC date similar to the ETA.

Furthermore, our ETA detection is based on fundamental design of the 802.11 architecture. When an AP fails to receive an acknowledgment response from a WC, it will assume the transmitted frame was lost due to collision or weak signal (Rayanchu et al., 2008; Wang and Helmy, 2011). The AP will keep sending unacknowledged frames for a certain amount of time until it determines that the WC is offline, and then disconnects it from the wireless network.

On the other hand, the design of the proposed ETA detection method for detecting different ISP 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 ISP gateway for Internet access. This type of wireless network topology can be found in coffee shops, hotels and airports (Bahl et al., 2006). Also, network administrators in these wireless networks usually assign private IP addresses to their wireless clients. These private IP addresses will be eventually translated into the public IP of the gateway using network address translation (NAT) or port address translation (PAT) (Bahl et al., 2006).

We also assume that security community can set up a public information server that can facilitate ETA detection. This PIS could be used by anyone anywhere. The server is simple to implement and maintain.

Finally, we assumed the attacker was able to clone the legitimate wireless network specifications to her rouge wireless network. The rogue wireless network is assumed to have the same network configuration and response time compared to the legitimate one. Also, the attacker's RAP has better/higher wireless signal power versus LAP, which makes it more attractive for a WC to join.

4.2. *Detection mechanism*

The proposed ETA detection mechanism focuses on the two types of gateways that can be used by the attacker. For the sake of clarity, we will explain the procedure of each ETA getaway detection separately. After that, these two proposed ETA detection mechanisms will be combined at the implementation section to produce a unified and comprehensive ETA detection.

4.2.1. *Detection of ETA using single ISP gateway*

Our ETA using single ISP gateway detection mechanism was designed to overcome the vulnerabilities found in WiFiHop (Mónica and Ribeiro, 2011) which was discussed in previous related work section. The effectiveness of our detection procedure is not based on parameters that can be gained or estimated by the attacker. Furthermore, the ETA detection is a real-time client-side method that does not rely on training data and/or Wi-Fi network fingerprint.

The proposed ETA system detection is composed of two parts: a WC and the public information server (PIS). First, by listening to the Wi-Fi beacon frames, the WC records the MAC address and the working Wi-Fi channels for all nearby APs that belong to the Wi-Fi network being tested. For simplicity, let us assume that we have only two APs in the target Wi-Fi network, AP_x and AP_y. Wi-Fi SSID is used to determine if an AP belongs to the target Wi-Fi or not. The first step does not involve any communication between the WC and any APs (i.e., passive). Fig. 3 summarizes ETA using single ISP gateway detection design.

Second, the WC randomly connects to one of the recorded APs, for example AP_x. Once the WC is connected to AP_x, the Wi-Fi network DHCP assigns network configuration such as IP address to the WC. Now that the WC is connected to the Wi-Fi network, she establishes a connection to the PIS and sends a "hello" packet. Data traffic between the WC and the PIS is encrypted. The PIS will assign a unique ID to the WC, e.g., XYZ. Such ID is capable of telling apart the communication between the WC and PIS from the communication of other WCs that may start the ETA detection at the same time in the same Wi-Fi network. After the WC receives her ID, she sends AP_x's MAC address along with the WC's ID to the PIS. In the meantime, the WC saves the Wi-Fi network connection information. Likewise, PIS saves AP's MAC address that belongs to the connection.

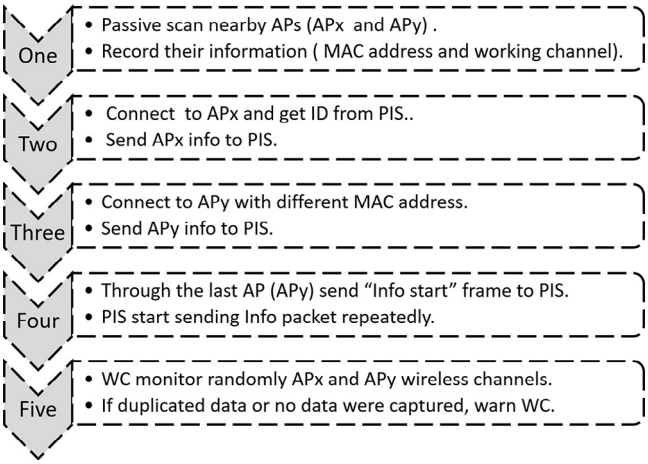


Fig. 3 – Proposed ETA detection on ETA using single ISP gateway.

Third, the WC switches randomly to other recorded APs (in our scenario, it is AP_y). At the same time, the WC changes her MAC address. After receiving network configuration using the new MAC address from AP_y, WC starts new connection to the PIS. After that, the WC sends AP_y's MAC address along with her ID to the PIS. Also, the WC saves the network configuration related to AP_y. In case there are more than two APs, the WC keeps repeating the previous procedure until going through the last recorded AP. As can be seen at this point, the WC is having two completely separate connections to the PIS.

Fourth, through the last connected AP (in our scenario, it is AP_y), the WC sends "Info Start" packet which signals the PIS to start sending info packets. When the PIS receives the "Info Start" form the WC, it start sending info packets to the WC through each connection separately. PIS keep sending info packets to the WC for a certain amount of time which is equal to Equation (3). Info packets contain the MAC address of the AP being used to establish the connection between the PIS and the WC. Also, each info packet has increment sequence numbers to prevent replay attack, as shown in Table 3.

Fifth, immediately after the WC sends info start packet, she randomly switches to one of the APs (AP_x or AP_y) channel and starts listening to the info packets sent by the PIS for a certain amount of time. WC filters all the incoming packets based on the WC's ID. As a result, all filtered wireless frames should have their destination MAC address pointing to one of the WC's MAC addresses. If not, then that frame was sent to a RWC. WC can then extract the MAC address inside the info packet to mark it as RAP. Also, if the WC did not receive an info packet from the AP that belongs to the current wireless channel, then that AP is also a RAP. Otherwise, the AP is LAP. In addition, the WC checks the sequence numbers of the info packets and ignores any packet with a sequence number that is less than or equal to the last one received.

Even if the attacker has all the timing information of the PIS sending interval and the WC switching/listening time, the ETA using single ISP gateway will fail because the WC's channel switching is random. The attacker cannot tell if the WC is listing to the RAP or the LAP. If the attacker stops sending info packets while the WC is listening to the RAP channel, our detection mechanism will detect the ETA. Also, if the attacker starts sending info packets while the WC is listening to the LAP Wi-Fi channel, the proposed detection mechanism will detect that the LAP is sending info packets to other WCs (attacker RWC). Furthermore, since every info packet has its own sequence number, the attacker can not apply the replay attack on info packets.

At the end of the detection procedure the WC marks every recorded AP as RAP or LAP. The WC now can freely connect to any of the LAPs. The PIS deletes all the information related to the WC's ID XYZ. This makes the PIS simple to implement and maintain.

Table 3 – Info Packet Data.

Packet Seq.	WC ID	AP MAC Address
1	XYZ	AP_x
2	XYZ	AP_y
3	XYZ	AP_x
4	XYZ	AP_y

4.2.2. *Detection of ETA using different ISP gateways*

The detection relies on creating a secure connection for sending and receiving heartbeats from/to PIS in a similar way as the second intuitive TCP-based detection method introduced in Section 3.2.2. When the WC starts the detection procedure, it initiates a TCP 3-way handshake through AP_x using a secure connection to PIS. Then, the client switches Internet access via AP_y and issues a heartbeat request to PIS and receive the response from the PIS.

Switching from one AP to another should not effect the current session between the WC and PIS. Also, since the WC keeps the old MAC address, she can reuse the IP address again when switching to the new AP since it is already registered in the DHCP server. However, if the wireless network gateway is different, the PIS will not be able to respond to the heartbeat request from the WC.

Using a secure connection is vital in our design to prevent the attacker from applying the MIMA attack illustrated in Fig. 2 since the attacker does not have the current TCP session's information to continue the secure 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. Similarly, if there are more than two APs 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.

4.2.3. *Comprehensive ETA detection*

Our proposed ETA using single ISP gateway detection and ETA using different ISP gateway detection can work in parallel using only one physical wireless interface card. To achieve that, a WC creates two virtual wireless clients (VWCs) in which each VWC emulates one standalone wireless client (Nakhila and Zou, 2016b; Nakhila et al., 2015b). The first VWC (VWC1) implements

the ETA detection procedure using single ISP gateway detection while the other VWC (VWC2) implements the ETA detection procedure using different ISP gateway detection.

Pseudo Code 1: Proposed ETA detection Procedure.

```
Record nearby APs info. having target SSID
Create VWC1 and VWC2
Set different MAC addresses to both VWCs
Both VWCs connect to one of the recorded APs
Both VWCs receive network conf. from DHCP server
Each VWC establishes a secure connection to PIS
VWC1 Sends "hello" pkt. to PIS
VWC1 Gets WC ID from PIS
VWC1 Sends current AP MAC Addr. and WC ID to PIS
VWC1 Saves connection info.
while not connected to all other recoreded APs do
    VWC1 assigns new MAC Addr.
    VWC2 keeps original MAC addr.
    Both VWCs connect to one of the remaining APs
    VWC1 gets network conf. from DHCP server
    VWC2 reuses pervious network conf.
    VWC2 sends heatheats to PIS
    if No heartbeat reply recived from PIS then
        Display ETA using single ISP was detected
        Exit both ETA detection procedures
    end
    VWC1 establishs a new secure conn. to PIS
    VWC1 sends AP MAC Addr. and WC ID to PIS
    VWC1 saves connection info.
end
Display ETA using single ISP was not detect
Stop VWC2
VWC1 Sends "Info start" pkt. to PIS
PIS Start sending Info pkts each D sec
while Each AP channel should be monitored four times do
    VWC1 randomly switchs to one of the APs ch.
    VWC1 filters traffic based on VWC1 ID
    VWC1 reads all filtered Info pkts
    if Info pkt was found then
        if Info pkt Seq. ≤ than previous one then
            Ignore Info pkt.
        end
        else
            if Wireless frame not sent to VWC1 then
                Extract AP MAC addr. from info pkt
                Mark extracted AP MAC Addr. as RAP.
            end
            else
                Ignore Info Pkt.
            end
        end
    end
    else
        Mark AP belongs to current ch. as RAP
    end
    Mark non RAP marked APs as LAP
end
```

Using our previous scenario of two APs (AP_x and AP_y), both VWCs connect to AP_x using different MAC addresses. The Wi-Fi network DHCP server assigns network configuration such as IP address to both VWCs. Each VWC receives different IP addresses since they have different MAC addresses. Both VWCs start a secure connection to the PIS. VWC1 keeps communicating with PIS to get the unique ID and sends AP_x information. After that, both VWCs switch to AP_y.

During the transition from AP_x to AP_y, VWC1 changes her MAC address while VWC2 keeps her previous MAC address. When both VWCs connect to AP_y, VWC1 receives a new IP address from the DHCP server. VWC1 starts a new connection to the PIS using the newly received network configuration. Then, VWC1 sends AP_y's MAC address along with her ID to the PIS. The VWC1 saves the network configuration related to AP_y. On the other hand, VWC2 reuses her original IP address and sends a heartbeat request to PIS using the secure connection that was created through AP_x.

If VWC2 does not receive heartbeat response from PIS through AP_y, the proposed detection stops and gives the WC a warning that ETA using different ISP gateways is active on the current Wi-Fi network. However, if the heartbeat was received from AP_y then, both VWCs switch to the next recorded AP. In our scenario the last AP was AP_y so, VWC2 informs the WC that both APs (AP_x and AP_y) are using the same ISP gateway. At this point, detection of ETA using different ISP gateways stops, while VWC1 continues the detection process of ETA using single ISP gateway. VWC1 sends info start packet and randomly switches to one of the APs (AP_x or AP_y) channel and starts listening to the info packets sent by the PIS as shown in Fig. 4.

4.2.4. *Proposed detection efficiency*

In our ETA detection, the VWC1 monitors all the recorded APs' Wi-Fi channels randomly. Given the attacker has all our ETA detection timing, she should decide when to disconnect/connect from the LAP to avoid being detected. Since info packets have encrypted sequence numbers, the attacker cannot save a copy and replay it to VWC1. When the attacker disconnects from the LAP, she cannot send any info packets using the RAP. Since the WC monitors each APs' Wi-Fi channel for one time unit, the miss detection probability P_m of VWC1 missing the detection of ETA using single ISP gateway, can be calculated as:

$$P_m = \frac{k}{N} \times \frac{N-k}{N} \tag{1}$$

where N is the number of recorded APs' wireless channels and k is the number of times the attacker disconnects/connects from/to the LAP. The attacker's goal is to find the best value for k in order to maximize the missing probability P_m. This can be calculated by finding the roots of the P_m's derivative, given as:

$$\frac{dP_m}{dk} = \frac{N-2k}{N^2} \tag{2}$$

The roots of Equation (2) are 0 and N/2. Applying $k = N/2$ to Equation (1) yields $P_m = 0.25$. Given that $P_m = 0.25$, the VWC1's ETA detection probability $P_d = 1 - P_m = 0.75$. To increase P_d, we increased the number of times the VWC1 monitors each recorded AP's Wi-Fi channel as shown in Table 4. Monitoring each recorded AP's Wi-Fi channel for one time will make the ETA detection probability to be $P_d = 0.75$. Thus monitoring four times will make our proposed ETA using single ISP gateway detection probability ≈ 100%.

On the other hand, the attacker can not affect the detection efficiency of the ETA detection using different ISP gateways. If the attacker prevented or allowed VWC2 from connecting to the PIS, in both cases, she will not receive the heartbeat

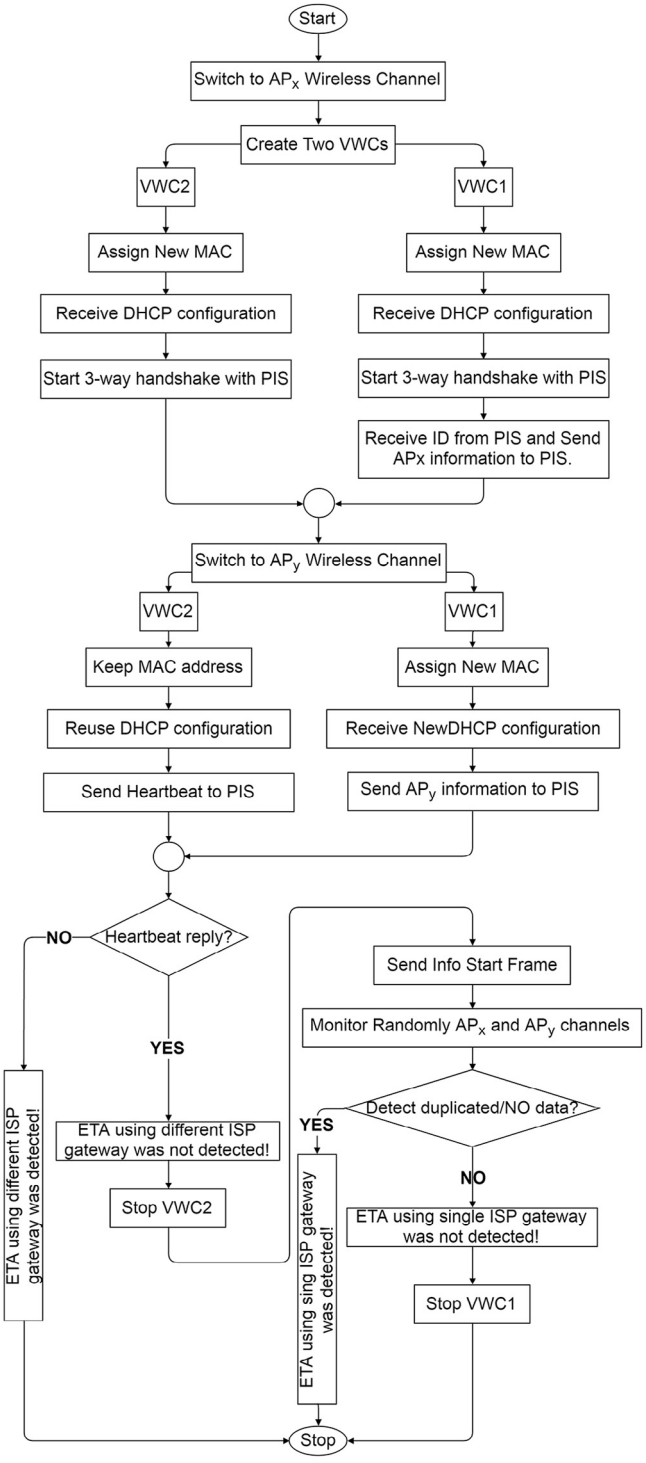


Fig. 4 – Proposed ETA detection on both ETA using single ISP gateway and ETA using different ISP gateways.

response from the ISP. In this case, the detection efficiency is 100% and it is independent from the attacker.

4.3. *Implementation*

The ETA comprehensive detection WC/PIS software were implemented using C language. Both WC/PIS were installed on Linux OS based machines. TCP protocol is used to carryout communication between the two of them. We used Loss Of Radio CONnectivity (LORCON2) (Wright and Kershaw, 2016) library to create multiple VWCs. LORCON2 is an open source library used to create crafted 802.11 wireless frames. WC uses LORCON to send/receive wireless frames using Wi-Fi interface card. As soon as VWCs connects to the AP, they start communicating using UDP protocol with the Wi-Fi DHCP server. The Wi-Fi network's DHCP server sends the network configuration to both VWCs. Each VWC follows different procedure to detect the ETA. Pseudo Code 1 illustrates the proposed ETA detection design.

Table 4 – Proposed ETA using single ISP gateway detection/missing probability.

Monitor Ch. Freq.	Miss Probability	Detection Probability
1	25%	75%
2	6.25%	93.75%
3	1.5625%	98.4375%
4	0.390625%	99.609375%

5. Evaluation

Our proposed ETA detection was tested in real work places such as Dunkin' Donuts, Starbucks and Panera bread. We also implemented a Wi-Fi network testbed to evaluate our proposed ETA detection. Wireshark software was used to monitor all communications between the VWCs and the PIS. Both the VWCs and the PIS software were installed on Kali Linux OS. The WC Wi-Fi interface card is wireless N dual-band USB adapter (TPE-NUSBDB). We assumed the attacker used D-link DIR890L Wi-Fi router to set up the RAP, and ASUS AC1900 Wi-Fi router to connect to the LAP. Where the LAP is also D-link DIR890L Wi-Fi router. However, our ETA detection mechanism will work with any other Wi-FI router that can be bought off-the-shelf. Fig. 5 illustrates the testbed set up. We repeated our proposed ETA procedure trails for 50 runs.

First, the WC listens to the Wi-Fi beacon and records the APs information such as the working channel and the MAC address. In our testbed, the WC recorded the working channels and MAC addresses of RAP and LAP. After that, the WC created two VWCs and randomly connected to one of the APs, e.g., RAP. The average time needed for both VWC1 and VWC2 to complete (1) initialize the wireless interface card to work on the RAP wireless channel; (2) pass the authentication phase; (3) pass the association connection phase, was 0.12 seconds with variance of 0.003 seconds as shown in Figs 6, 7, 8 respectively. After both VWCs were connected to RAP, they both received network configuration from the DHCP server. The average time to obtain a valid IP address using RAP was 0.42 seconds with variance of 0.0019 seconds as shown in Fig. 9. After that, both VWCs established a separate secured connection to the PIS. However, only VWC1 received her ID, Immediately, VWC1 sent RAP MAC address along with her ID to the PIS. Both VWCs should finish their procedures at each AP to be able to switch to the next AP. The time needed to finish communicating to PIS on the Internet through RAP was 0.043 seconds with variance of 0.0007 seconds as shown in Fig. 10.

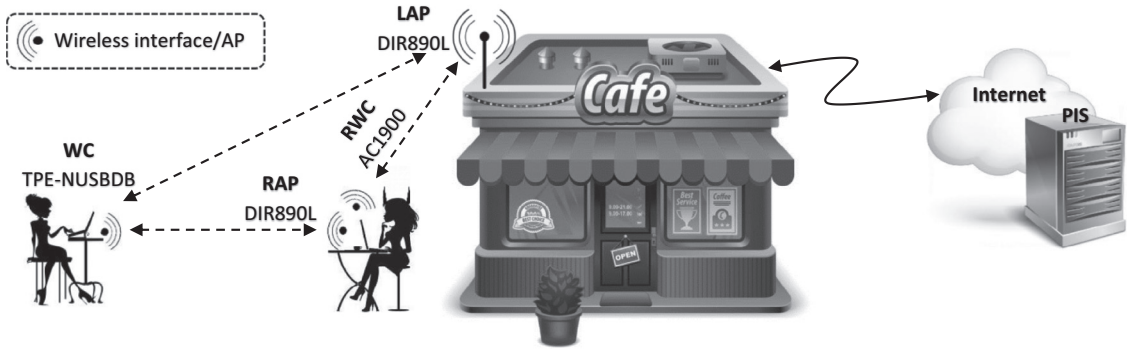


Fig. 5 – Proposed ETA evaluation testbed set up.

Second, both VWCs finished communicating with RAP and started switching to LAP. During the switching from RAP to LAP only VWC1 changed her Wi-Fi interface MAC address. The average switching time between RAP and LAP was 0.2 seconds with variance of 0.0008 seconds as shown in Fig. 11. Since the MAC address of the VWC1 was changed, new network configuration was received from the DHCP server. On the other hand, VWC2 kept its original network configuration because she used the same MAC address. We assumed that both RAP and LAP gave the same exact authentication, association and DHCP response time when communicating with VWCs.

At this point, VWC2 reused the previous connection (network socket) which was setup through the RAP and sent a heartbeat request to the PIS. VWC2 received a heartbeat reply from the PIS since both RAP and LAP used the same public IP address to communicate with the PIS. VWC2 displayed a message to the WC that both RAP and LAP are using the same ISP gateway. The time needed for VWC2 to receive a positive reply from the PIS was 0.018 seconds with variance of 0.00012 seconds as shown in Fig. 12. VWC2 spent about 0.9 seconds to finish detecting ETA using different gateways.

In the meanwhile, VWC1 started a new connection to the PIS and sent LAP MAC address with her ID to the PIS. Now, the

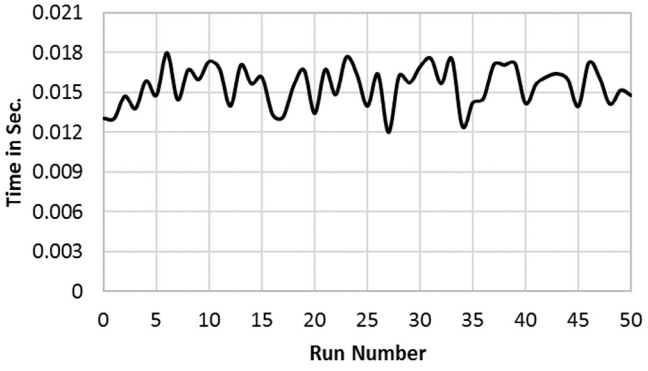


Fig. 6 – Initialize client Wi-Fi interface card to operate on RAP Wi-Fi channel.

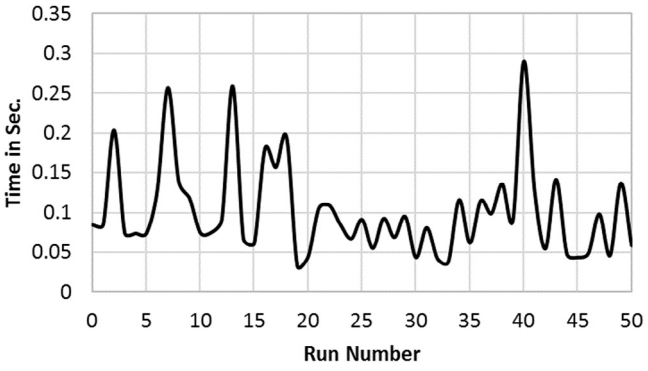


Fig. 7 – Average time for VWC1 and VWC2 to finish Wi-Fi authentication phase with RAP.

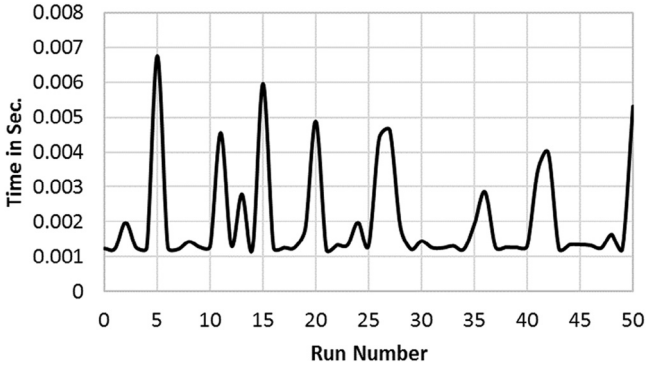


Fig. 8 – Average time for VWC1 and VWC2 to finish Wi-Fi association phase with RAP.

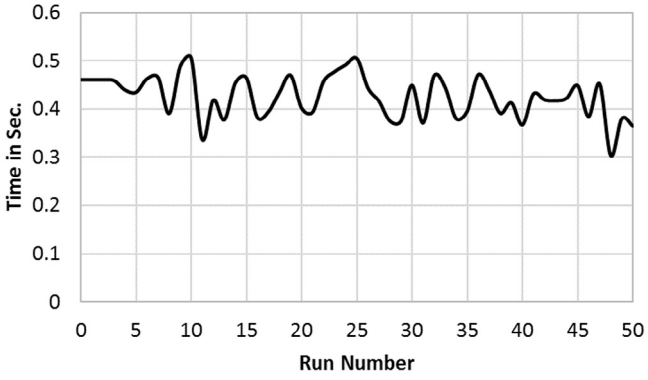


Fig. 9 – Average time for VWC1 and VWC2 to receive network configuration from DHCP server.

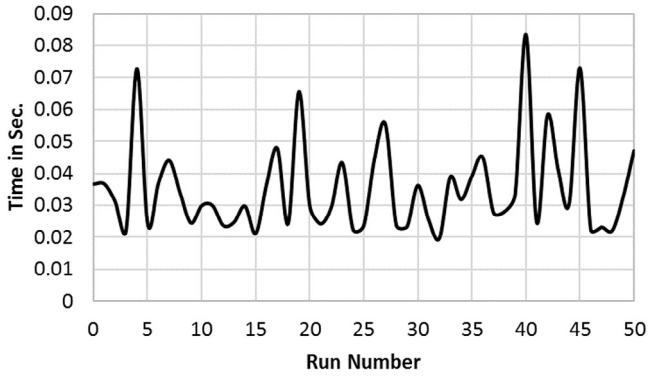


Fig. 10 – Time duration for VWC1 to finish communicating with PIS.

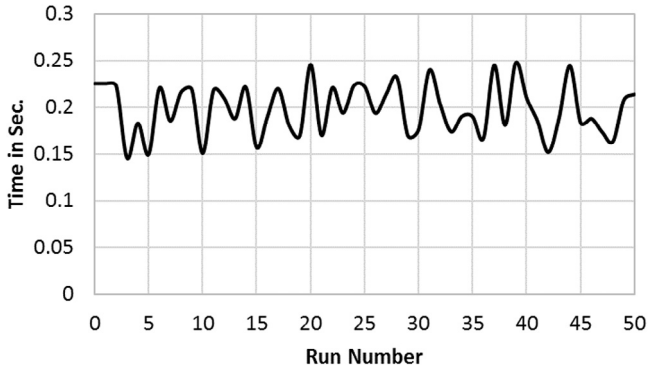


Fig. 11 – Time for WC to switch from RAP operating Wi-Fi channel to LAP Wi-Fi channel.

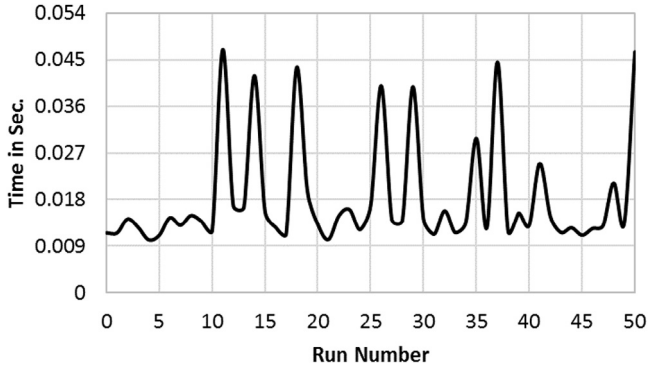


Fig. 12 – Time delay until VWC2 received heartbeats from PIS.

VWC1 has two active connections to the PIS through both the RAP and the LAP. Until now, the actual detection of ETA using single ISP gateway has not started yet.

Our ETA detection for the ETA using single ISP gateway starts when VWC1 sent "info start" packet to the PIS. "info start" packet was sent after VWC1 finished communicating with PIS which was around 0.035 seconds with variance of 0.0007 seconds as shown in Fig. 13. For comparison purposes, we used the same timing technique used in (Mónica and Ribeiro, 2011).

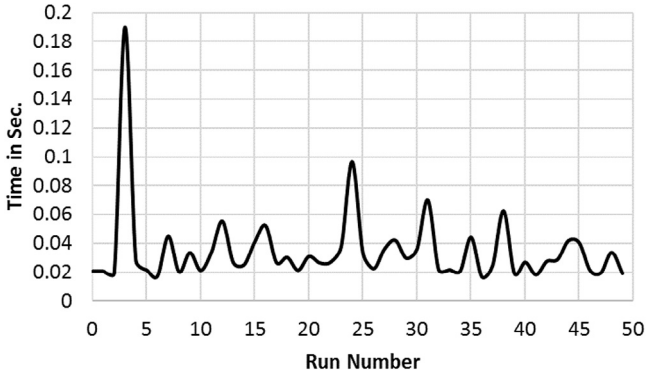


Fig. 13 – VWC1 communication time with PIS including sending "Info Start" frame.

The PIS started sending Info packets at an interval of D seconds each, where D is the time required for the VWC1 to switch from one AP to another. In our testbed, which was based on 50 runs, the average value of D was ≈ 0.2 seconds with standard deviation of 0.0008 seconds as shown in Fig. 11. Also, the VWC1 should spend longer than $(D + RTT)$ seconds to monitor each Wi-Fi channel (Mónica and Ribeiro, 2011), where RTT is the Round Trip Time between the VWC1 and the PIS. The RTT measured between the VWC1 and the PIS was ≈ 0.016 seconds with a standard deviation of 0.005 seconds. As a result, the VWC1 should monitor each Wi-Fi channel longer than (0.2 + 0.016) seconds. Based on that, we chose for the VWC1 to monitor each Wi-Fi channel for 0.4 seconds. Furthermore, to avoid being affected in case the info packets were lost/dropped along the route between the PIS and the VWC1, the PIS continuously sent info packets once every D seconds.

Since each channel should be monitored four times to have ≈ 100 detection rate (Table 4), our ETA detection time based on the number of APs Wi-Fi channels available in the network can be calculated as:

$$DetectionTime = N * (2.4) \quad (3)$$

where N is the number of Wi-Fi channels to be tested, and 2.4 is the total time to monitor each Wi-Fi channel which came from calculating $4 \times (0.4 + 0.2)$. For example, based on Equation (3), VWC1 spend about half a minute to monitor all the 11 Wi-Fi channels in 802.11 b/g network.

Although VWC1 had to wait 0.4 seconds on each wireless channel, VWC1 was able to capture LAP, RAP and RWC info packets sent by PIS in average of ≈ 0.08 seconds with a standard deviation of 0.0001 seconds as shown in Fig. 14. This is due to the fact that PIS will keep sending multiple packets to the VWC1 every D time intervals which is equal to the switching time of the VWC1. By the time VWC1 switches from one AP to another, info packets should have already been sent by the PIS and on its way to VWC1.

6. Discussion, limitation and future work

Virtual Wireless Clients (VWCs) has been proposed previously to improve wireless performance and privacy (Zhang et al.,

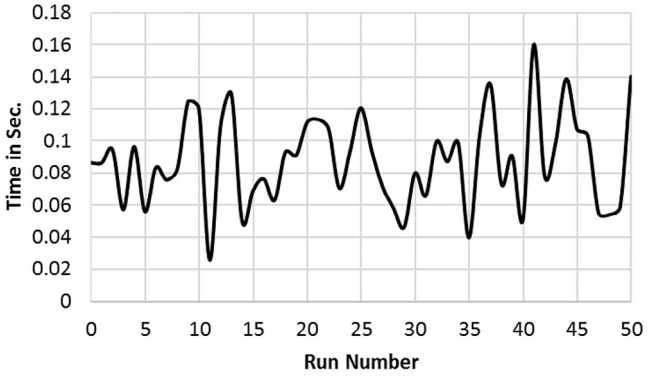


Fig. 14 – Average time delay before VWC1 capture Info frames from LAP, RAP and RWC.

2011), however, utilizing VWCs in securing wireless networks is unique. In this paper, we have presented a comprehensive ETA detection technique. The proposed detection can effectively detect ETA regardless of the gateway type used by the attacker. Both procedures of detecting ETA using single ISP gateway and ETA using different ISP gateways work in parallel using VWC technique.

6.1. *ETA detection using single ISP gateway*

Our ETA detection can monitor all the 11 802.11 b/g WiFi channels in less than half a minute with a detection rate close to 100%. Meanwhile, in Open WiFiHop (Mónica and Ribeiro, 2011), similar time period was spent to test only one AP. Furthermore, our proposed detection is more secure since it is not based on parameters that can be estimated by an attacker. For example, unlike Open WiFiHop (Mónica and Ribeiro, 2011), if the attacker has all the procedure timing information, our ETA detection efficiency will not be affected and is almost 100%.

The proposed ETA detection does not rely on training data and/or the Wi-Fi's network fingerprint, which makes it preferable for customers (such as travelers) who visit the Wi-Fi network for the first time. Furthermore, the WC will be the one who ensures her security. In addition, the PIS used in our ETA detection is simple to implement and maintain. No WC data will be saved on the PIS, which ensures user privacy in case the PIS is compromised.

Wi-Fi network coverage maybe extended by setting up relays such as repeaters or creating wireless distribution system (WDS). This type of wireless coverage extension is avoided by Network administrators due to the lack of standardization (Chandra, 2009; Chwan, 2013; Coleman, 2006; Holt, 2010; Olenewa, 2014). However, our proposed detection can detect whether a specific AP is a relay or an AP by checking the wireless frame headers. In IEEE 802.11, Wi-Fi relay traffic uses all the four address fields in the wireless frame; however, LAP, WC and RAP use only three address fields (Miller et al., 2011).

The WC should be within the wireless coverage area of both the LAP and RAP to detect the ETA. We assumed the network administrators wirelessly covered the designated network area (such as coffee shops, etc) by using LAPs. When the attacker sets up her RAP, she will be within that designated wireless network area. The same assumption applies to the WC.

All time measurements in our testbed may vary from one wireless network to another. For example, the RTT is based on the Internet speed between the WC and the PIS. Also, different DHCP servers vary in their response time. Some DHCP servers wait longer time to test if the IP is already in use before leasing it the WC (Droms, 2013).

Attacker can hide the info packets by setting up a VPN tunnel between the RWC and a VPN proxy server on the Internet. In this case all data traffic between the RWC and the VPN proxy server will be encrypted. VWC1 will be unable to decrypt info packet anymore. However, using VPN proxy will modify the public IP address of VWC1 on the Internet. This behavior will be detected by VWC2.

Another tactics an attacker may undergo on our proposed ETA detection is to exhaust all the available association identifiers AID on each LAP to prevent the VWCs from connecting to it. Each AP can have up to 2007 AIDs (Ieee standard for information technology, 2007). Each AID is given to a WC. In this case, the RWC must generate many VWCs and connect to the LAP all at the same. The RWC must maintain all these connections since the LAP timeout and drops idle connection for certain amount of time. To alert the WC of such condition, our proposed ETA detection could count the number of connections to each LAP by monitoring the wireless traffic.

6.2. *ETA detection using different ISP gateways*

The proposed ETA detection using different ISP gateways is light, fast and effective. However, after detecting the existence of ETA, VWC2 can not tell which AP is LAP and which AP is RAP. Since both the LAP and the RAP provide Internet access that could have the same specifications, it is very challenging to distinguish them with only client-side actions.

If the client receives only RAP(s) signals without any LAP, 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. VWC2 cannot detect ETA since all the AP(s) give the consistent fake results without any ground-truth feedback from a LAP.

Finally, having PIS server in our detection design is vital. An attacker may initiate a Denial of service attack (DoS) to block all the connection from the wireless clients to the PIS server. To overcome this scenario, multiple PIS servers can be created and installed in different locations. Since the design and implementation of PIS server is simple, no synchronization between the servers is needed. The wireless client randomly select any available PIS server to start our proposed ETA detection technique.

6.3. *Future work*

In our ETA detection proposal, it is important for the WC to be able to monitor wireless traffic (WiFi in promiscuous mode). Such a condition depends on the WC OS, wireless interface card driver and chipset. In our experiments, we used Linux OS and LORCON2 driver with Atheros based WiFi USB interface card. As future work, our proposed system can be ported to mobile O.S, e.g., Android, or in a Windows system using different wireless interface card drivers and chipsets. For example, Windows

O.S users can use Winpcap driver with supported interface cards (WinPcap Team, 2017). Android O.S users can use PCAP library (Kershaw, 2017) on RTL8187 chipset based wireless interface card.

7. Conclusion

In this paper, a comprehensive real-time client side ETA detection was proposed. Both, ETA using different and single ISP gateways can be detected in parallel. The wireless client can scan the whole 11 Wi-Fi channels of the 802.11 b/g network for ETA in about half a minute. No training data and/or network fingerprint was used in the detection. The efficiency of our proposed detection mechanism was mathematical modeled and implemented in real life scenario with a detection rate close to 100%.

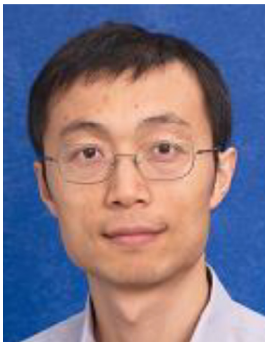
Acknowledgment

This work was supported by the National Science Foundation (DGE-1723587).

REFERENCES

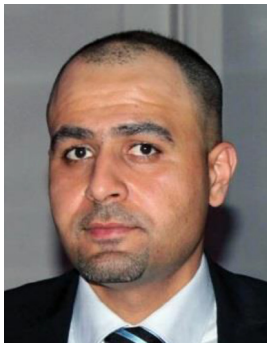
Albert R, Jeong H, Barabási A-L. Internet: diameter of the world-wide web. Nature 1999;401(6749):130–1.
Bahl P, Chandra R, Padhye J, Ravindranath L, Singh M, Wolman A, et al. Enhancing the security of corporate Wi-Fi networks using DAIR. In Proceedings of the 4th International Conference on Mobile Systems, Applications and Services, MobiSys '06, pages 1–14, New York, NY, USA, ACM. 2006.
Chandra P. Wireless security. Amsterdam Boston: Newnes/Elsevier; 2009.
Chwan. Introduction to computer networks and cybersecurity. Boca Raton, FL: CRC Press; 2013.
Coleman D. CWNA certified wireless network administrator study guide: (exam PWO-100. Hoboken, N.J. Chichester: Wiley John Wiley distributor; 2006.
Droms R. Dynamic Host Configuration Protocol. RFC 2131, 2013.
Ericsson. Mobility report. Tech Rep NAVTRADEVCEN. 2015.
Holt A. 802.11 wireless networks: security and analysis. London: Springer; 2010.
IEEE standard for information technology telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Std 802.11–2007 (Revision of IEEE Std 802.11–1999), pages 1–1076, June 2007.
Intel. What is Wi-Fi roaming aggressiveness. 2014.
Internet Engineering Task Force. RFC 791 Internet Protocol – DARPA Inernet Programm, Protocol Specification, 1981.
Jana S, Kasera SK. On fast and accurate detection of unauthorized wireless access points using clock skews. IEEE Trans Mobile Comput 2010;9(3):449–62.
Kershaw M. Kismet project, 2017.
Lanze F, Panchenko A, Braatz B, Engel T. 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 '14, pages 3–14, New York, NY, USA, ACM. 2014.
Lanze F, Panchenko A, Ponce-Alcaide I, Engel T. Hacker's toolbox: Detecting software-based 802.11 evil twin access points. In 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), pages 225–232, Jan 2015.
Marlinspike M. More tricks for defeating SSL in practice. Black Hat USA, 2009.
Miller B, Mackenzie P, Westcott DA, Coleman DD. CWAP certified wireless analysis professional official study guide: Exam pw0-270l. In John Wiley & Sons, March 2011.
Mónica D, Ribeiro C. WiFiHop – mitigating the evil twin attack through multi-hop detection. Berlin, Heidelberg: Springer Berlin Heidelberg; 2011. p. 21–39.
Mustafa H, Xu W. CETAD: Detecting evil twin access point attacks in wireless hotspots. In Communications and Network Security (CNS), 2014 IEEE Conference on, pages 238–246, Oct 2014.
Nakhila O, Zou C. User-side Wi-Fi evil twin attack detection using random wireless channel monitoring. In MILCOM 2016 - 2016 IEEE Military Communications Conference, pages 1243–1248, Nov 2016a.
Nakhila O, Zou C. Parallel active dictionary attack on IEEE 802.11 enterprise networks. In MILCOM 2016 - 2016 IEEE Military Communications Conference, pages 265–270, Nov 2016b.
Nakhila O, Dondyk E, Amjad MF, Zou C. User-side Wi-Fi evil twin attack detection using SSL/TCP protocols. In 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), pages 239–244, Jan 2015a.
Nakhila O, Attiah A, Jinz Y, Zou C. Parallel active dictionary attack on WPA2-PSK Wi-Fi networks. In Military Communications Conference, MILCOM 2015 - 2015 IEEE, pages 665–670, Oct 2015b.
Nikbakhsh S, Manaf ABA, Zamani M, Janbeglou M. A novel approach for rogue access point detection on the client-side. In Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on, pages 684–687, March 2012.
Olenewa J. Guide to wireless communications. Boston, MA: Course Technology/Cengage Learning; 2014.
Panch A, Kumar Singh S. A novel approach for evil twin or rogue AP mitigation in wireless environment. Int J Secur Appl 2010;4(4):33–8.
Rayanchu S, Mishra A, Agrawal D, Saha S, Banerjee S. Diagnosing wireless packet losses in 802.11: Separating collision from weak signal. In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, April 2008.
Scott C, Wolfe P, Erwin M. Virtual private networks. Sebastopol, CA, USA: O'Reilly & Associates, Inc.; 1998.
Seufert M, Griepentrog T, Burger V, Hofeld T. A simple WiFi hotspot model for cities. IEEE Commun Lett 2016;20(2):384–7.
Sherwood R. Discovering and Securing Shared Resources on the Internet. Univ. of Maryland, 2008.
SMC Network. Wireless Hotspot Solutions. 2008.
Song Y, Yang C, Gu G. Who is peeping at your passwords at Starbucks? To catch an evil twin access point. In 2010 IEEE/IFIP International Conference on Dependable Systems Networks (DSN), pages 323–332, June 2010.
van Rijswijk-Deij R, Sperotto A, Pras A. DNSSEC and its potential for DDoS attacks: A comprehensive measurement study. In Proceedings of the 2014 Conference on Internet Measurement Conference, IMC '14, pages 449–460, New York, NY, USA, ACM. 2014.
Wang SC, Helmy A. Beware: background traffic-aware rate adaptation for IEEE 802.11. IEEE/ACM Trans Netw 2011;19(4):1164–77.
WinPcap Team. WinPcap project 4.1.3, 2017.

Wright J, Kershaw M. Lorcon2 project, 2016.
Yang C, Song Y, Gu G. Active user-side evil twin access point detection using statistical techniques. IEEE Trans Inform Forensics Secur 2012;7(5):1638–51.
Zhang F, He W, Liu X. Defending against traffic analysis in wireless networks through traffic reshaping. In 2011 31st International Conference on Distributed Computing Systems, pages 593–602, June 2011.



Cliff C. Zou is an associate professor in the Department of Computer Science, University of Central Florida. He received the PhD degree in the Department of Electrical and Computer Engineering from the University of Massachusetts, Amherst, MA, in 2005. His research interests include computer and network security, computer networking, and performance evaluation. He is a senior member of The Institute of Electrical and Electronics Engineers (IEEE).

Muhammad Faisal Amjad is a senior member of the IEEE and an Assistant Professor in the Department of Electrical Engineering, National University of Sciences and Technology Pakistan. He received his PhD degree in Computer Science from the University of Central Florida USA in 2015. His current research focusses on network security, digital forensics and malware analysis. He specializes in dynamic spectrum access and defense against security vulnerabilities in Cognitive Radio Networks as well as wireless sensor and ad hoc networks, game theory and multi-agent systems.



Omar Nakhila is a PhD Candidate in the Department of Electrical and Computer Engineering, University of Central Florida. He received his M.Sc. degree in Computer Engineering from the University of Mosul, Mosul, Iraq, in 2007. His research focuses on the network privacy and security of computers, mobiles and Internet of things.

Erich Dondyk is a Software Developer Engineer at Amazon Web Services. He graduated from the University of Central Florida with a Bachelor degree in Computer Engineering and Electrical Engineering in 2012 and a Master degree in Computer Engineering in 2014. His interest includes distributed systems, cloud computing, and mobile device security.