ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Survey on Evil Twin Access Point Detection Technique

Vibhawari V. Nanavare, Prof. Dr. V. R. Ghorpade

ME Student, Dept. of CSE, D. Y. Patil College of Engineering & Technology, Kolhapur, India.

Professor, Dept. of CSE, D. Y. Patil College of Engineering & Technology, Kolhapur, India.

ABSTRACT- This paper considers problem of "evil twin" attacks in wireless local area networks. Evil twin is a term for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually it can be set up by attacker to eavesdrop on wireless communications. Evil twin is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of evil twin attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing. Mostly existing evil twin detection systems are administrator based like to check whether the access point present in authorized list or not. But this administrator based detection solutions are limited, expensive and not useful for all many scenarios. Again, existing detection systems are server side which need trained data (authorized AP/ host list) to detect and avoid evil twin attack. So, there is a need to implement a system which can be effective and detection can be at the user-side. For that it can calculate the interpacket arrival time among one hop and two hop systems.

KEYWORDS: wireless network, evil twin attack, rouge AP detection, packet arrival time

I. INTRODUCTION

Nowadays, wireless communication is becoming extremely popular as there is no need of any extra cables to connect with network and this networking devices can be used everywhere. Advantages of WLAN over wired network are its flexibility, portability and its inexpensiveness. But with this advantage, we have considered some security and performance issues related to WLAN. User can access the wireless Internet by connecting to any public Wi-Fi access point. But that access point can be more vulnerable to fraud. Evil twin is a term for a rogue Wi-Fi access point that appears to be legitimate one offered on the premises, but actually it can be set up by attacker to eavesdrop on wireless communication. Rogue wireless access points bypass physical endpoint security of local area networks and present significant security threats by creating network attack vectors behind firewalls, exposing confidential information, and allowing unauthorized utilization of network resources.

An Evil Twin attack is where attacker creates either a physical AP or evil AP that mimics the AP which a normal user will connect to. The idea is that either through user error or application design, you will trick a user into connecting to the fake AP instead of the original AP. The attack starts with the victim workstation connected to the legitimate AP. Either through knowledge or reconnaissance attacker find out the relevant information about a legitimate AP. Usually, the SSID is sufficient, but attacker may also want to imitate the user's channel as well. After obtaining this data on attacker workstation, attacker starts airbase-ng using the setting they have acquired from the legitimate AP. It is possible to set airbase-ng to respond to probe requests, however, attacker targeted its attack to the particular SSID in order not to attack any innocent workstations that were within transmission range. Once attackers have started airbase-ng, they must setup the client routing. The Fake AP will begin to constantly sendsdeauthentication packets to the victims pretending to be the Real AP. In addition, it will also start to send out Probe Responses for the Real AP's SSID, but with its own MAC. These packets are sent to victim in order to force him to disconnect from the legitimate AP and then connect to the Fake AP. After a few seconds, the victim will deautheticated from the legitimate AP and then authenticate with the Fake AP. In this case, the Victim receives it IP from the AP's DHCP server. The client will try to request its current IP from the new AP. In our case, the IP available on the Fake AP is in a different subnet. Therefore, the client temporarily loses higher level connectivity, and takes on an automatic private IP; however, eventually it will get a new DHCP address from the Fake AP. To the user on the Victim machine, it simply seems that

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

they have lost their connection temporarily; when they can continue browsing the web after a few seconds, they do not notice anything different about their connection. As a result, the attacker is now free to commit MitM attacks on the Victim.

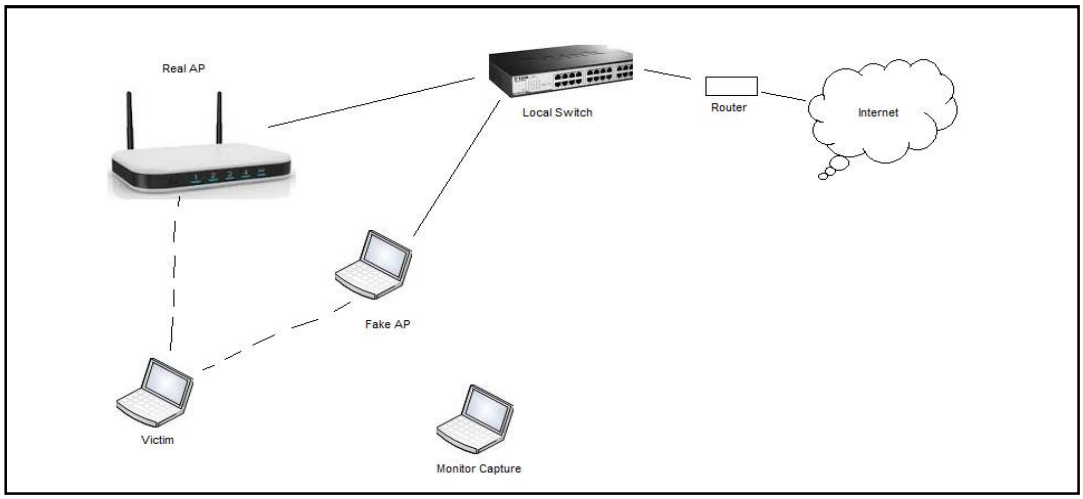

Figure 1. Existence of Evil Twin AP

Evil twin attack is very easy to set up. Without any need of extra hardware, attacker can easily launch the evil twin attack. The attacker can simply set up his rogue access point to create a fake access point which will mimic as the legal access point. Now rogue access point will attract user to connect. Vulnerable user easily connects with rogue access point.

Evil twin attack becomes successful very easily. Attacker can setup his laptop nearer to legitimate AP and mimic it as legitimate access point. Attacker can use the same SSID as the legitimate AP. User connects to access point which has highest signal strength. Now, client is connected to the legitimate access point via the evil twin attacker. Attacker can easily provides the Internet access to client plus it can access user's private information like user name, password. Most existing evil twin detection systems are administrator based systems. But this paper, focuses on implementation of evil twin access point detection system at the client side. For that purpose, it is necessary to check the time required to receive packets from normal access point and the evil twin access point.

II. LITERATURE SURVEY

Existing rouge AP detection solution can be mainly classified into two categories. The first category, monitors RF airwaves and additional information gathered at routers/switches and then compares with a known authorized list. The second category of rouge AP detection solution is to detect evil twins by differentiating whether clients come from wired networks or wireless networks, relying on the differences in diverse network protocols.

S. Jana and S. Kasera, explores the use of clock skew of WLAN access point as its fingerprint to detect unauthorized access point accurately [1]. The main goal of clock skew is to overcome the major limitation of existing solution, that is, inability to detect Medium Access Control address spoofing. In this it uses Time Synchronization Function to calculate clock skew of access point. TSF time stamps sent out in beacon/probe response frames. In this approach it uses two different methods, one is based on linear programming and other is on least-square fit. After that it collects TSF time stamp data from several APs in three different residential settings. Using measurement data as well as data obtained from a large conference setting, it can find that clock skews remain consistent over time for the same AP but vary significantly across APs. This work use a technique that different APs have different clock skew to detect unauthorized wireless AP. However, this work still uses the "fingerprint" technique, which needs a white list of authorized APs.

Utilization of time interval information to detect rouge APs have introduced by H. Han, B. Sheng, C. Tan, Q. Li [4], and S. Lu, and H. Han, B. Sheng, C. Tan, Q. Li, and S. Lu [6]. Specifically, it calculates the round trip time (RTT)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

between the user and the DNS server to independently determine whether the AP is legitimate or not without assistance from the WLAN operator. Since this work mainly utilizes the training detection technique and uses a relatively static threshold to differentiate normal and malicious scenarios, it needs to pre-collect the information of the target wireless network. Thus, such learning-based approaches highly depend on the knowledge of the target wireless network. They could not be effectively applied to those travelling users at the client side, since once the travelling users are in different areas, the network situation may have significantly changes.

Ankit Panch, Santosh Kumar Singh in [5], introduces a simple and easy approach, which uses, Wireless Connection Session Database[WCSD], where a system database file is configured on the client and server side, to maintain a track record of successful sessions between trusted systems to identify the credentials of the AP and hence makes it possible to identify the fake AP, with a very simple approach, without any modification at the infrastructure or the hardware. But this case, it need the creation of session in between the client and server. It requires the generation of a system file and an inclusion of a wireless connection session database, which can provides the historical evidences of the authenticity of the AP. Considering that the AP and the client were already connected one time and it stores entry in the database. This wireless session database need to be configured and stored in the configured system database file on both client and server sides.

In [3], authors W.Wei, K. Suh, B.Wang, Y. Gu, J. Kurose, and D. Towsley, differentiate clients according to its wired or wireless connection with AP. If client is from wireless network, and if it is not present in the authorized list then it consider it as a fake AP. In this detection scheme it use authorized list.

Chao Yang, Yimin Song, and GuofeiGu, authors have given the novel approach to detect the evil twin attack at the user side [7]. Existing evil twin access point detection solutions mostly needs network administrators to verify whether a given access point is in an authorized list or not, instead of for a wireless client to detect whether a given AP is authentic or evil. Such administrator side solutions are limited, costly, and not available to detect dynamic users. Thus, there is need to have a lightweight, effective, and user-side solution is highly desired. In this approach, they have proposed a novel user-side evil twin detection technique that outperforms traditional administrator-side detection methods in several aspects. Unlike previous approaches, it does not need a known authorized AP/host list, thus it is more efficient to identify and avoid evil twin attack.

III. SYSTEM ARCHITECTURE

Main goal of a system is to detect the evil twin access point. The evil twin attack detection system will be implemented on the client side to detect rogue access point. If user is connected to legitimate access point via the evil twin access point, then the time requires to receive packet form two hop access point is more than the one hop access point.

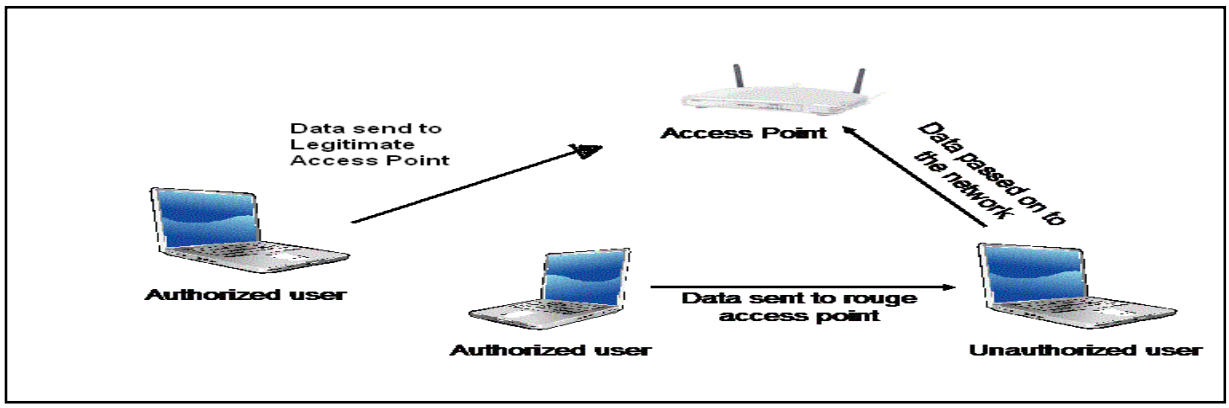

Figure 2. System Architecture

System includes three main factors that are as follows:
i) Legitimate access point: Legitimate Access Point is a device that allows wireless devices to connect to a wired network using Wi-Fi. The user can connect to the internet by using this legitimate access point. When user want to access the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

wireless Internet connection it must connect to the access point.
ii) Evil Twin Access point: Evil Twin access point is the access point which is rogue by attacker. It is illegal access point which acts as a legitimate access point. By setting Evil Twin access point in between the legitimate access point and user, it can access the user private information.
iii) User: User is the end user who accesses the wireless internet connection from any wireless hotspot. User always connects to the access point which gives the highest wireless signal strength.
In normal case, client can connect to the legitimate access point. The wireless internet access will be provided by legitimate AP. But evil twin attacker is unauthorized user who can set up his laptop in such a way that, it can connect to legitimate AP and he can mimic the legitimate AP. Normal client/user can connect with any available hotspot. Now, client may connect with evil twin attacker who just mimics it as the legal AP.
Technical contribution of this paper:

- To design effective user-side evil twin access point detection.
- It should not be administrator based. That is it should not use the trained data to detect and avoid evil twin attack.
- To design statistic method to effectively calculate intermediate time arrival packets.

IV. METHODOLOGY

To detect the Evil Twin attack the scenario like differentiating between normal AP connection and the Evil Twin AP connection can be used. As shown in Fig. 2 (a), in the normal AP communication, a user communicates with the remote server through the normal AP (a one-hop communication); on the other hand, in the evil twin AP scenario, the victim client communicates with the remote server through an evil twin AP and a normal AP (a two-hop communication) as in Figure 2 (b). Thus, compared with the normal AP scenario, the evil twin AP scenario has one more wireless hop. This observation gives the intuition to detect evil twin attacks by differentiating one-hop and two-hop wireless channels from the user-side to the remote server. To detect the two hop wireless channel the system calculates wireless IAT (Interpacket Arrival Time) network statistic.

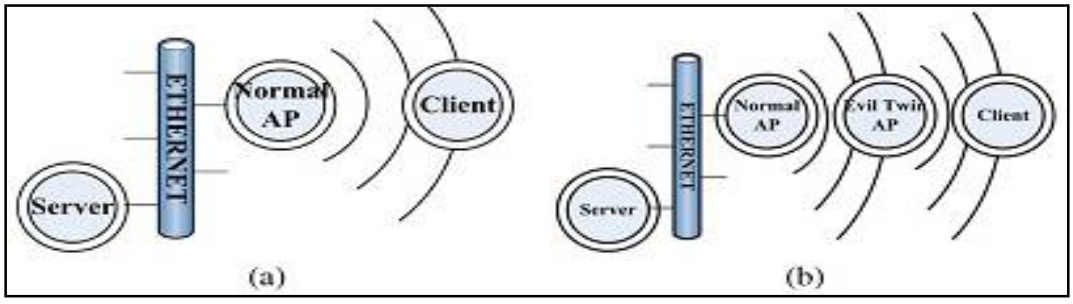

Figure 3. Illustration of a) Normal AP and b) Evil Twin AP

Interpacket Arrival Time is a time interval between two consecutive data packets sent from the same server to the client. To calculate more accurate and effective IAT, immediate acknowledgement for each and every packet is used. When any data packet P_1 receives from the server, client must send acknowledgement for that packet as A_1. When server receives this acknowledgement A_1 then and only then server can send the next data packet P_2. So, the sequence of packet transmission is like P_1 A_1 P_2 A_2. The IAT is the difference of time interval of two consecutive data packets T_{P2}- $T_{P1.}$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

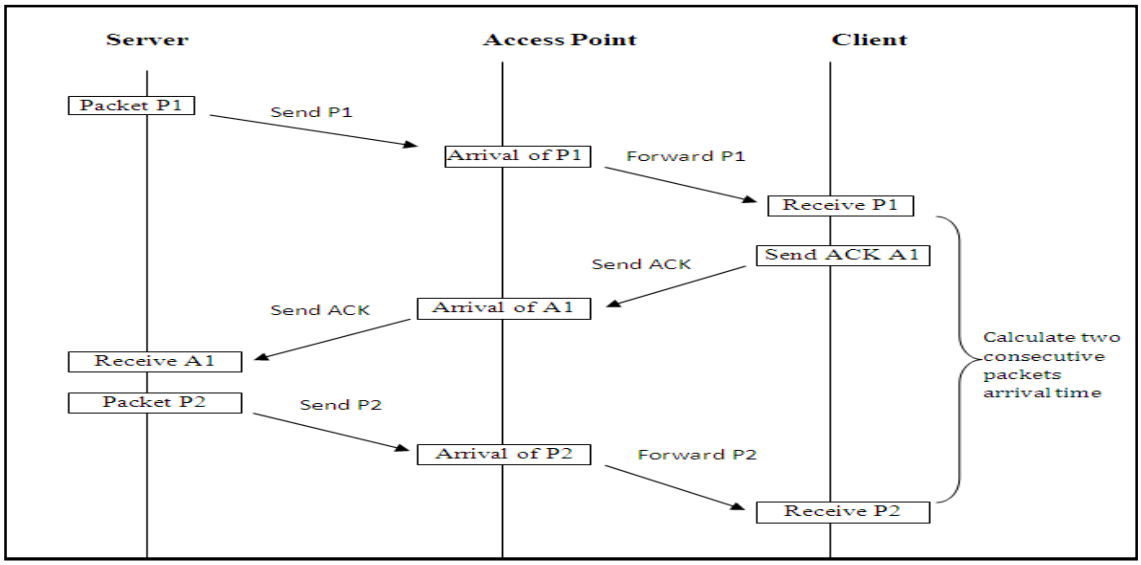

Figure 4. Calculation of IAT for one-hop wireless connection

At the client side evil twin detection system can be implemented. It can calculate the time interval of two consecutive packets. In case of one-hop wireless connection time interval between two consecutive received packets are less. When server sends any data packet to client it goes to AP.

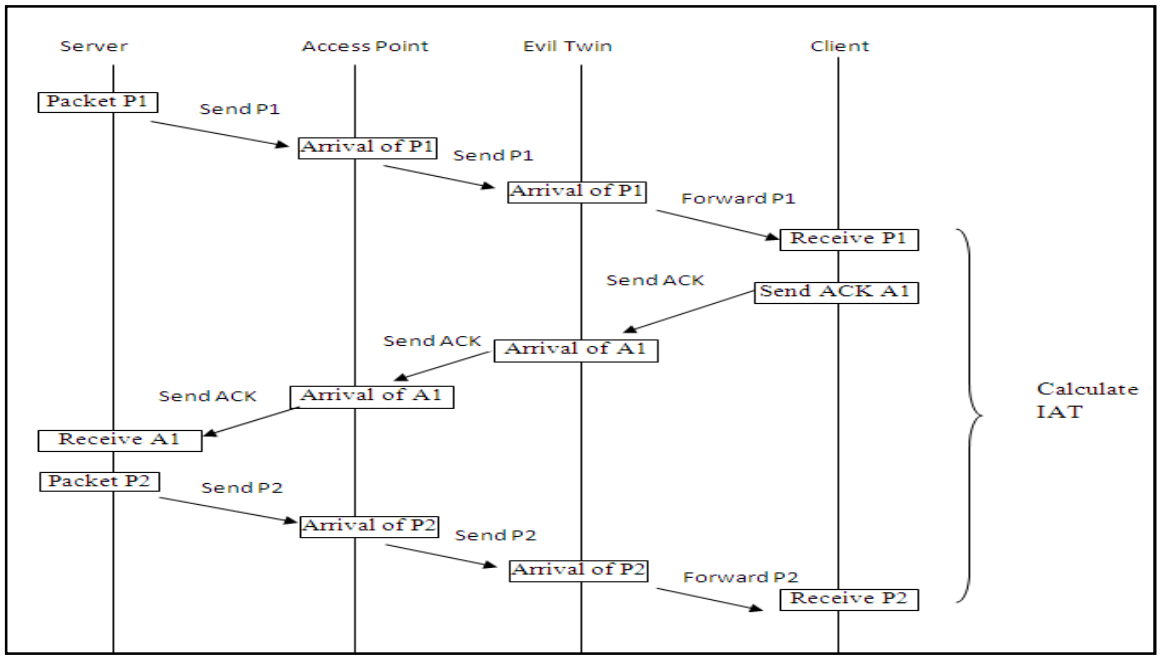

Figure 5. Calculation of IAT for Two-hop wireless connection

If client is connected to normal access point then the time interval of two consecutive received packets is less. And if client is connected to the evil twin access point then the time interval of two consecutive data packets are more.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

V. CONCLUSION

This paper focuses on the interactive detection of the evil twin access point at the client side which does not require any authorised access point list or administrator solution. The calculation of the IAT (Interpacket Arrival Time) effectively identifies the difference between normal access point connection and evil twin access point detection. In evil twin access point connection the time interval in two consecutive packets (IAT) is more than the normal access point connection. So this approach can easily find out the existence of evil twin access point.

REFERENCES

[1] S. Jana and S. Kasera. "On fast and accurate detection of unauthorized wireless access points using clock skews" *IEEE Trans. Mobile Comput., vol. 9, no. 3, pp.449-462, Mar. 2010.*
[2] Evil Twin in Wikipedia [Online]. Available: http://en.wikipedia.org/wiki/ Evil_twin_(wireless_networks)
[3] 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 *Proc. 7th ACM SIGCOMM Conf. InternetMeasurement (IMC'07)*, San Diego, CA, 2007.
[4] H. Han, B. Sheng, C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue AP detection," *IEEE Trans. Parallel Distrib. Syst., vol. 22,* no. 11, pp. 1912–1925, Nov. 2011
[5] Ankit Panch, Santosh Kumar Singh, "A Novel approach for Evil Twin or Rouge AP mitigation in wireless environment", Internationl Journal of Security and Its Applications Vol. 4, No. 4, Oct, 2004
[6] H. Han, B. Sheng, C. Tan, Q. Li, and S. Lu, "A measurement based rouge AP detection scheme," in Proc. IEEE Int. Conf. Computer Communications (Infocom 09), 2009.
[7] Chao Yang, Yimin Song, and GuofeiGu, *Member, IEEE,* "Active User-Side Evil Twin Access Point Detection Using Statistical Techniques", IEEE Transactions On Information Forensics And Security, Vol. 7, No. 5, October 2012
[8] Cracking WPA & WPA2 with Aircrack-ng [Online]. Available:http://www.youtube.com/watch?v = GLO9HGDwOY0
[9] Cracking WPA & WPA2 key with Aircrack-ng on Kali Linux [Online]. Available:http://www.youtube.com /watch?v=93AEREX5w0I