ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Robust and Effective Evil Twin Access Point Detection Technique at End User Side

Vibhawari V. Nanavare[1], Prof. Dr. V. R. Ghorpade[2]

ME Student, Dept. of CSE, D. Y. Patil College of Engineering & Technology, Kolhapur, India. [1]

Professor, Dept. of CSE, D. Y. Patil College of Engineering & Technology, Kolhapur, India. [2]

ABSTRACT: Wireless LAN technology, despite the numerous advantages it has over competing technologies, has not seen widespread deployment. A primary reason for markets not adopting this technology is its failure to provide adequate security. Data that is sent over wireless links can be compromised with utmost ease. In this project, we propose a distributed agent based intrusion detection and response system for wireless LANs that can detect unauthorized wireless elements like access points, wireless clients that are in promiscuous mode etc. The system reacts to intrusions by either notifying the concerned personnel, in case of rogue access points and promiscuous nodes, or by blocking unauthorized users from accessing the network resources. Due to the prevalence of insecure open 802.11 access points, it is currently easy for a malicious party to launch a ariety of attacks such as eavesdropping and data injection. In this paper, we consider a particular threat called the evil twin attack, which occurs when an adversary clones an open access point and exploits common automatic access point selection techniques to trick a wireless client into associating with the malicious access point.

KEYWORDS: Wireless LAN, Evil Access Point, Network Security, Fake AP detection

I. INTRODUCTION

Wireless Networks like a Wi-Fi becoming very popular nowadays because of its easy connectivity between user and Wi-Fi Access point. User in public area like coffee shop, airport, mall can easily connects to freely available wi-fi. But connecting such available wi-fi networks is more vulnerable. An unauthorized user can access user's private information. That type unauthorized user we can consider as evil twin attacker. An evil twin, in security term, it is a rogue wireless access point that pretends as a legitimate Wi-Fi access point so that an attacker can gather user's personal or corporate information to which the end-user's are unaware. An attacker can easily create an evil twin with the help of Smartphone or other Internet-capable device and some easily-available software's. The attacker positions himself nearer to a legitimate hot spot and lets his device discover what service set identifier (name) and radio frequency the legitimate access point uses. Then an attacker sends out his own radio signal, using the same name as the legitimate access point. The end-user, suppose that the evil twin is a normal hot spot with a very strong signal; that's because the attacker not only uses the same network name and settings as the real access point, attacker impersonate, he also physically positioned himself nearer to end-user so that his signal is likely to be the strongest within range. If the end-user is strongly attracted by the strong signal and connects manually to the evil twin to access the Internet, or if the end-user's computer automatically selects that connection because it is running in promiscuous mode, the evil twin becomes the end-user's Internet access point, giving the attacker the ability to intercept with sensitive data like passwords or credit card information. Evil twin is not a new phenomenon in wireless transmission. Historically they have been recognized as base station clones or honeypots. Nowadays more businesses and consumers are using wireless devices in public places and it's easier than ever for someone who doesn't have any technical expertise to create an evil twin. To avoid evil twin connections, end users should use public hot spots for Web browsing only and avoid online shopping or banking. To protect corporate data, employees who use wireless devices should always connect to the Internet through private and secure network.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

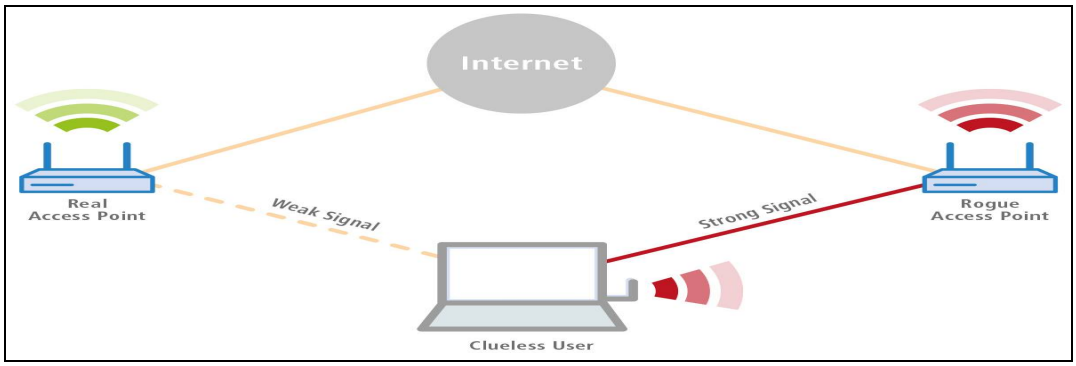

Figure 1. Existence of Evil Twin

The attacker uses a bogus wireless access point, purporting to provide wireless Internet services, but snooping on the traffic. When the users log into unprotected (non-HTTPS) bank or e-mail accounts, the attacker has access to the entire transaction, since it is sent through their equipment. He also is able to connect to other networks.

Unwitting web users are invited to log into the attacker's server with bogus login prompts, tempting them to give away sensitive information such as usernames and passwords. Often users are unaware they have been duped until well after the incident has occurred.

Users think they have logged on to a wireless hotspot connection when in fact they have been tricked into connecting to its evil twin by it sending a stronger signal within proximity to the wireless client. Rogue access points are easy to set up, for example using a laptop with a wireless card that acts as an access point (known as "host-ap"), but are hard to trace since they can suddenly be shut off. An attacker can make his own wireless networks that appear to be legitimate by simply giving their access point the same SSID and BSSID to the Wi-Fi network on the premises. The rogue access point can be configured to pass the traffic through to the legitimate access point while monitoring the victim's traffic, or it can simply say the system is temporarily unavailable after obtaining a username and password.

Our first task will be to creating an evil twin access point. Many new hackers are anxious to crack Wi-Fi passwords to gain some free bandwidth (don't worry, we'll get to that), but there are so many other Wi-Fi hacks that are far more powerful and put so much more at risk than a bit of bandwidth.

To accomplish this, hackers simply use a piece of software, or app, that is designed to capture data that is sent over a wireless connection. An example of software that is used during a fake Wi-Fi attack includes AirSSL, AirJack, Airsnarf, Dsniff, Cain, void11.

How is your data stolen during a fake wireless access point theft?

A large percentage to hack is take place with a fake wireless point which requires a login and password. Once that information puts into the login, a hackers will take it and use it to sign into popular websites, assuming that you use the same login and password for multiple sites.

When your online accounts start showing charges that you didn't initiate, or if your social media account is taken over, you could be the victim of a fake wireless access point data theft.

How to defend against an 'Evil Twin' attack?

There are a number of ways to defend against it, I'll look at some easy to understand examples:

- The best defence is to always verify with the wifi provider. Ask the Starbucks staff what their wi-fi is called, it can save you a massive headache. Always remember – if a deal seems too good to be true, like free wifi, it probably is.
- Use different login details and passwords for public wifi.

Disconnect auto-connect when you're in unfamiliar territory.

- Be cautious when connects suddenly disconnect, especially if it happens for everyone on the network. An app known as aireplay is capable of disconnecting users from wifi, hoping that they'll reconnect to their fake wifi.
- Be cautious of certificates. Good websites can occasionally send you one, but if this happens over a public wifi that you don't know, it is best to back off.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Evil Twin Methodology

Step 1: We will first scan the air for a target access point. Then create an access point using airbase-ng with the same name and channel of the target access point, hence Evil-TWIN.
Step 2:The client is now disconnected repeatedly from the original access point and as most modern system's setting says… "Connect back to same ESSID(AP name) if disconnects".
Step 3: Clients is now connected to the Fake WiFi access point and now client may start browsing Internet.
Step 4: Client will see a web administrator warning saying "Enter WPA password to download and upgrade the router firmware"
Step 5: The moment client enters the password, s/he will be redirected to a loading page and the password will be stored in the MySQL database of the attacker machine.

II. RELATED WORK

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.
Sweta Anmulwar; Shalvi Srivastava; Shrinivas P. Mahajan; Anil Kumar Gupta; Vinodh Kumar,[11], explores the different existing rogue access point detection system. There are different ways are present to detect rogue access point, like, administrator based, client-side detection, such different ways are reviewed here.
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.
To effective detection of evil twin access point detection, [8] explore the use of clock skew method. It also uses the TSF time stamp. It mainly focus on implementation of least-square fit method .From this the use of clock skews appears to be an effective and robust method for detecting fake AP's in wireless local area network

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) 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

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

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.

Nazrul M. Ahmad; Anang Hudaya Muhamad Amin; Subarmaniam Kannan; Mohd Faizal Abdollah; Robiah Yusof authors give evil twin detection system at clent-side[9]. Existing most of detection system works at server or administrator side which will not be much effective. They uses a framework of client-centric RAP detection for Wi-Fi hotspots which exploits Received Signal Strength Indicator (RSSI) values measured over time between client and APs.

In approach [10],authors Bandar Alotaibi; Khaled Elleithy, to detect Rogue Access Points (RAPs) that clone some characteristics of nearby legitimate Access Points (APs). Passive approach that takes advantage of the first frame that the RAP sends (i.e, Beacon Frame (BF)) when it is planted in the Wireless Local Area Network (WLAN) is proposed. They proposed fingerprint to detect RAPs to evaluate the fingerprint effectiveness. The proposed framework examines every beacon frame size, and compares it with a threshold value. The technique is implemented on a commercially available Wireless Network Interface Controller (WNIC) to evaluate its accuracy. The detection algorithm achieves 100 percent accuracy to determine the RAPs in a lightly loaded traffic environment. The detection time can be taken in approximately 100 ms and is scanned in real-time setting. The robustness and the efficiency of the detection algorithm are examined in two different locations.

III. PROBLEM STATEMENT

Existing evil twin detection solutions are mostly for wireless network administrators to verify whether a given AP 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, expensive and not available for many scenarios. These approaches are limited because they all require the knowledge of an authorization list of APs and users. Thus, there is need to implement a lightweight, effective and user side detection system. Proposed system does not require any authorized AP list and it will detect evil twin attack at client side.

IV. OBJECTIVES

The main objective of this proposed system is to detect whether a user is connected to legitimate access point or evil twin access point. The detection system should not be administrator based. That is it should not use the trained data to detect and avoid evil twin attack. The detection system should be effectively implemented at the user side.

V. 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 require to receive packet from two hop access points is more than the one hop access point.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

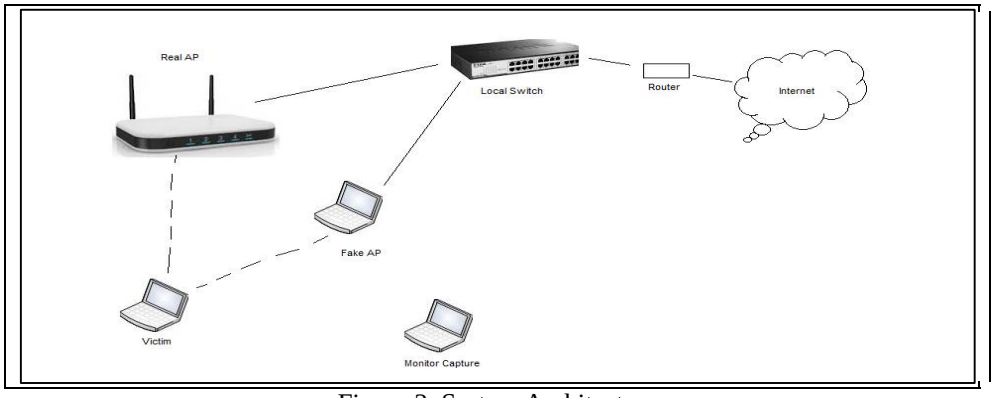

Figure 2. System Architecture

The evil twin AP is an access point that looks and acts just like a legitimate AP and entices the end-user to connect to fake access point. Aircrack-ng tool can be used to make the fake AP. This is a powerful client-side hack that will enable attacker to see all of the traffic from the client and conduct a man-in-the middle attack.

At the client side needs to use wireshark tool which is used to capture the packets from source to destination. The main goal is to detect the evil twin is completed by using IAT (Interval arrival time). Wireshark shows the packets and their time as well as generate the graph. The original AP sending packet time is less so our IAT is also less, on the other hand fake AP packet sending time is large then its IAT is bigger than this is called fake AP.

1. Legitimate AP

Legitimate Access Point is the s a device that allows wireless devices to connect to a network using Wi-Fi. The user can connect to the internet by using this legitimate access point. When user want to access the wireless internet connection it must be connect to the access point using legitimate AP's ESSID name and password.

2. 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.

3. Evil Twin Attacker

Evil twin attacker is attacker, who interact in between legitimate AP and user. It can access user private information like password. Evil twin attacker can disconnect the user from internet access. For that it can use aircrack-ng tool.

The evil twin AP is an access point that looks and acts just like a legitimate AP and entices the end-user to connect to fake access point. Aircrack-ng tool can be used to make the fake AP which is first part of proposed system. This is a powerful client-side hack that will enable attacker to see all of the traffic from the client and conduct a man-in-the middle attack.

At the client side needs to use wireshark tool which is used to capture the packets from source to destination. The main goal is to detect the evil twin is completed by using IAT (Interval arrival time). Wireshark shows the packets and their time as well as generate the graph. The original AP sending packet time is less so our IAT is also less, on the other hand fake AP packet sending time is large then its IAT is bigger than this is called fake AP.

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.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

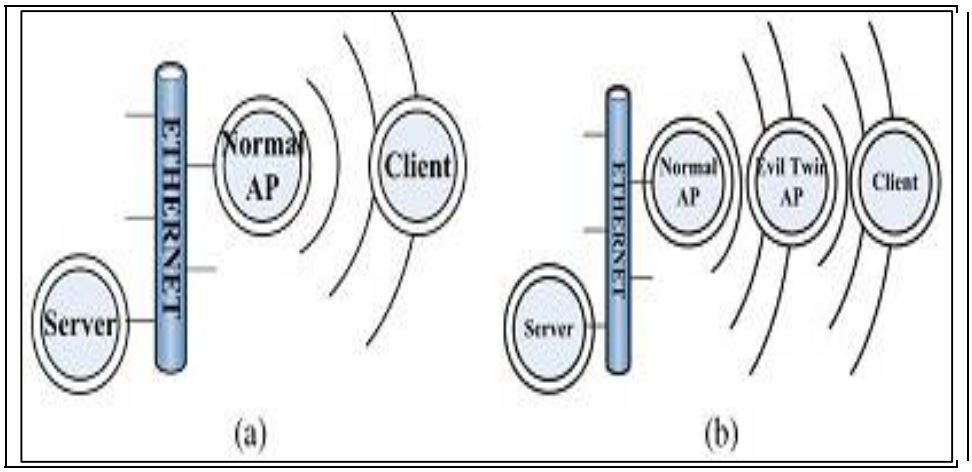

Figure 3. Illustration of a) Normal AP and b) Evil Twin AP

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}- $T_{P1.}$

1. TMM (Trained Mean Match)

The distributions of Server IAT in one-hop and two-hop wireless channels differs significantly. By using this statistics, a detection algorithm named Trained Mean Matching (TMM) is implemented. Specifically, given a sequence of observed Server IATs, if the mean of these Server IATs has a higher likelihood of matching the trained mean of two-hop wireless channels, the proposed system conclude that the client uses two wireless network hops to communicate with the remote server indicating a likely evil twin attack.

2. HDT (Hop Differentiating Technique)

In TMM it uses the trained threshold, but still computes a theoretical SAIR bound to distinguish these two scenarios. According to this observation, it develops a non-training based detection algorithm named Hop Differentiating Technique (HDT) algorithm. Different from the TMM algorithm, in the HDT algorithm can use a theoretical value for the threshold rather than a trained threshold to detect evil twin attacks. In the theoretical computation phase, compute a threshold as the SAIR boundary to differentiate one-hop SAIR and two-hop SAIR.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

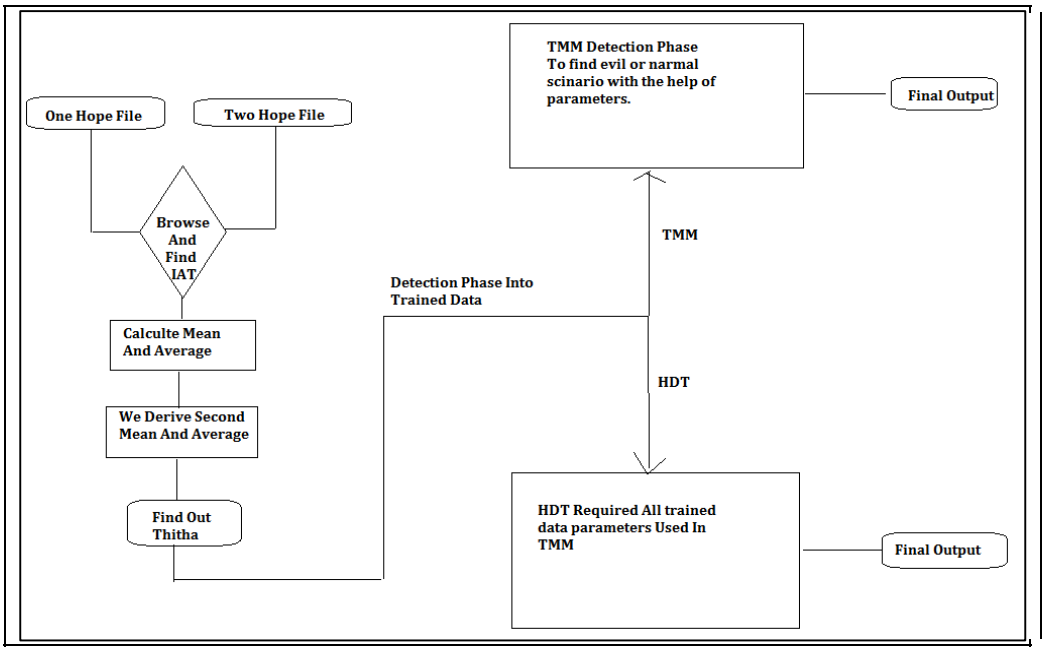

Figure 4 Block Diagram of TMM and HDT Algorithm

Above Block diagram shows that how to go TMM and HDT for detection of Evil and Normal Scenario. Which is requiring to both one and two hope files which includes packets and time related to scenario. With the help of packets we calculate IAT and Average. Then system derive the second mean. Standard deviation is find out with the help of standard deviation formula. Then find out probability which is similar to TΘ values. Assigning probability to approximately TΘ value. And then TΘ value decides which is evil twin or normal access point scenario.

The working of TMM and HDT algorithm is different but required input files and trained data is similar just some steps are different of HDT and TMM algorithm. First, system collects Server IAT in both one-hop and two-hop wireless channels. Then, compute the mean and the standard deviation of Server IAT collected in the one-hop (normal AP) scenario, with different variables. Next it calculates the range with the help of range formula. Then derive the second mean and calculate average of derive mean called as TΘ.

Proposed module obtain two probabilities of one Server IAT in these two scenarios exceeding the trained threshold, denoted as P1 and P2 , by computing the percentage of collected Server IATs deviating from in the normal and evil twin AP scenario, respectively.

In the detection phase, given a sequence of Server IAT observations, represented by Delta and use random binary variable to denote whether the 'i'th observed Server IAT belongs to evil twin AP scenario or not. Here it also needs to calculate Hypothesis 0 and 1.

Next part is to find out delta and random variables from trained data which is derived from one and two hope files. Then Θ1 and Θ2 find out and P1 and P2 probability assign to Θ1 and Θ2 which is normal and evil scenario respectively. Then take a one random variable which is 1 then we are says that evil twin scenario if random variable is 0 then normal access scenario.

HDT detection technique uses same above trained data, only detection phase is different that is all parameters like random variable or hypothesis, probability and delta are same like a TMM. The HDT detection is depend on average. Then check trained data average and decide scenario is evil or not.

So by using trained data average we find out which file is normal access scenario or evil scenario. Using TMM and HDT algorithm as a base paper mention that TMM performance is low compared to HDT which is shows by graphically as well as with the help of execution time. In graphical representation we present time execution for TMM and HDT. In red part show time execution for TMM in MS and green part shoes HDT execution time. Shows graphs also shows the HDT time excitation is less than TMM and its better than TMM.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

VI. RESULT ANALYSIS

1. Execution Time Require to TMM and HDT

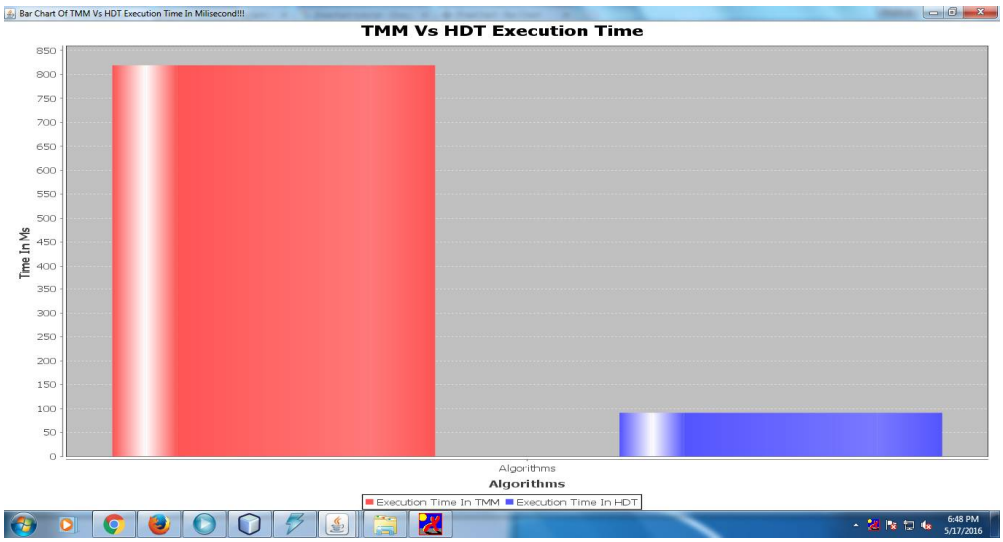

Figure 4 Execution Time for TMM and HDT

Above graph shows TMM Vs. HDT algorithm Execution time. The X-axis represents algorithm and Y-axis represents time in MS. Here it clearly show that time execution of TMM is always high compare to HDT. Because our base paper mention that HDT is better than TMM. And its clearly that as execution time HDT is better.

2. IAT Average of two Algorithm

Then below graph shows the average of two algorithms which is in %.

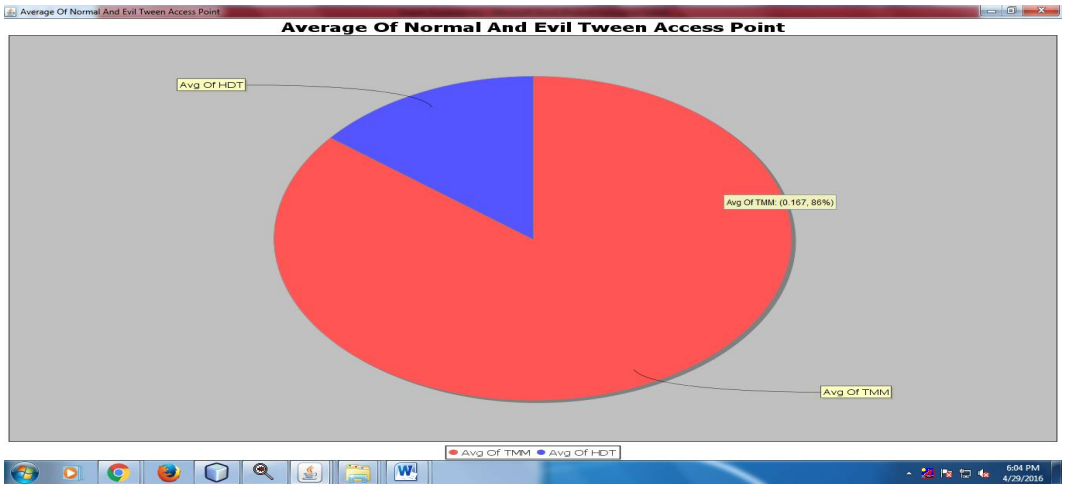

Figure 5 IAT Average of One-hop and two-hop

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

TMM Algorithm:

// Training Phase

1) Calculate One Hope average $\mu_{1,NAP}$ and delta $\sigma_{1,NAP}$.

2) Filter one hope server IATs beyond the range.

3) Compute second mean for One Hope $\mu_{2,NAP}$.

4) Calculate Two Hope average $\mu_{1,EAP}$ and delta $\sigma_{1,EAP}$.

5) Filter Two hope server IATs beyond the range.

6) Compute second mean for Two Hope $\mu_{2,EAP}$.

7) Find T-thitha and check scenario.

$$T_\theta = (1/2)(\mu_{2,NAP} + \mu_{2,EAP})$$

8)In detection Phase,

/* Detection Phase: */
$\Lambda = 0, \theta_0 = P_1, \theta_1 = P_2$
for $i = 0$ **do**
  Compute δ_i
  if $\delta_i \geq T_\theta$ **then**
    $\Lambda = \Lambda + \ln\theta_1 - \ln\theta_0$
  else
    $\Lambda = \Lambda - \ln(1-\theta_1) - \ln(1-\theta_0)$
  end if
  if $\Lambda \geq B$ **then**
    return evil twin AP scenario
  else if $\Lambda \leq A$ **then**
    return normal AP scenario
  end if
end for

HDT Algorithm:

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

1) Same Trained Data Is Used i.e Above All parameters are used as it is.But Only Detection Phase Is different.

$\Lambda = 0, \theta_0 = P_1, \theta_1 = P_2$
for $i = 0$ **do**
  Compute α_i
  if $\alpha_i \geq \alpha_\theta$ **then**
    $\Lambda = \Lambda + \ln \theta_1 - \ln \theta_0$
  else
    $\Lambda = \Lambda - \ln(1 - \theta_1) - \ln(1 - \theta_0)$
  end if
  if $\Lambda \geq B$ **then**
    return evil twin AP scenario
  else if $\Lambda \leq A$ **then**
    return normal AP scenario
  end if
end for

VII. CONCLUSION AND FUTURE WORK

Proposed system implements a novel lightweight user-side evil twin attack detection technique. For that system presents two algorithms, TMM and HDT. Proposed System implements prototype system and evaluate it in several real-world wireless networks, and our evaluation results proved its effectiveness and efficiency.

TMM and HDT algorithms used to conclude either the AP is Normal AP or Evil AP. Both algorithms need Packet arrival time IAT to check normal or evil scenario. The TMM algorithm affords an effective approach to detect evil twin attacks. It requires a priori knowledge of IAT. Uses Threshold value to detect NAP an EAP. However, in some cases, it's too time-consuming for a normal user to network can be hardly directly applicable to another network.

These limitations motivate us to design an effective and practical nontraining-based algorithm to detect evil twin attacks (HDT). HDT doesn't need trained data, it can directly work on real data. So it requires less time as compared to TMM.

If there are multi-hop present in the network, which is legitimate one, then also this proposed system detect is as an evil twin scenario. So in future system can be implementing to detect multi-hop connection in network.

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. Internet Measurement (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.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

[7] Chao Yang, Yimin Song, and Guofei Gu, *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] Swati Jadhav; S. B. Vanjale; P. B. Mane, "Illegal Access Point detection using clock skews method in wireless LAN", Computing for Sustainable Global Development (INDIACom), 2014 International Conference on Year: 2014
[9] Nazrul M. Ahmad; Anang Hudaya Muhamad Amin; Subarmaniam Kannan; Mohd Faizal Abdollah; Robiah Yusof , "A RSSI-based rogue access point detection framework for Wi-Fi hotspots", Telecommunication Technologies (ISTT), 2014 IEEE 2nd International Symposium on Year: 2014
[10] Bandar Alotaibi; Khaled Elleithy , "An empirical fingerprint framework to detect Rogue Access Points Systems", Applications and Technology Conference (LISAT), 2015 IEEE Long Island Year: 2015
[11] Sweta Anmulwar; Shalvi Srivastava; Shrinivas P. Mahajan; Anil Kumar Gupta; Vinodh Kumar, "Rogue access point detection methods: A review" Information Communication and Embedded Systems (ICICES), 2014 International Conference on Year: 2014