Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 4 Issue 5, May - 2017

Evil Twin Detection by analysing the Network

Pratik Sarwade, Nagesh Puri
Dept. of Computer Science and Engineering
SIT, Lonavala
Pune, India

Arati Sabane, Monika Waghole
Dept. of Computer Science and Engineering
SIT, Lonavala
Pune, India

***Abstract*— Wireless technology has been widely spread all over the world. In the market places there is no war to provide the enough security. The data or the sensitive information sent over there is sometimes gets compromised or it may be insecure. There are the numbers of attacks eavesdropping and data injection etc. which attackers on the data transfer in the network. In this paper, we study the attack called the evil twin, it happen when the attacker clones the access points and which tricks the access and associate the connected client maliciously. As per the latest investigation on this, it is found that the near about 42% wireless 802.11 is not providing any security mechanism not even WEP or WPA is also.**

In the public Wi-Fi there are chances to attacker to evil twin attack on the Wi-Fi. Attacker creates the clone of the public Wi-Fi spot and an evil twin AP and the attacker can carry out frequent attacks to take improvement of the unacquainted victim. Data transferred to the Wi-Fi hacked by the attacker and it may be injurious to the innocent user. These type of attacks happen at bakery shop, bus station etc. In this paper we proposed the analyzing and recognition method that analyze the evil twin attacks. The proposed methodology as compare to the existing approaches recognize and detects the evil twin attacks, we are using the TMM and HDT algorithms to analysis.

Keywords— Closed Evil Twin Attack, Rogue access point, AWS' S3, Scale-out, workload executor.

I. INTRODUCTION

Wireless security has been inadequate in the todays in era of the wireless internet. There are the number of the service that currently provided by the franchisee. In those the consumer gets the easy access and use of the internet free of cost. Internet is accessed in the public places by the hotspot through the WIFI devices. This access of Wi-Fi sometimes susceptible and insecure to use that can cause the malicious attacks on the user device in turn important data steeled without user consent.

802.11 Wireless LAN's have developed and truly reshaped the network landscape. 802.11n is now quickly replacing Ethernet as the method of network access. These attacks are harmful to user and other credential is not able to provide full security to the entire device/system. Attacks like eavesdropping or data injection attacked by the attackers. Now days the evil twin attacks are used to steal the user information. In this paper we are studying the evil twin attack. What is evil twin attack- In the evil twin attack, attacker clones the Wi-Fi hotspot and makes new easy access and unauthenticated device, and user thought this is the access provided by the owner. If the user connects those types of hotspots access the service user doesn't know the attack was happen. While accessing services attacker get the user information to the attacker may harmful to user.

In this paper we are studying and analyzing the evil twin attacks which helpful to find malicious node and prevent getting user from connecting those type of devices. The new algorithms TMM and HDT are used in the detection phases. By using this approach the user will get to know the adversary has setup the evil twin attack and cloned the node.

.

II. EASE OF USE

The numerous amount usage of the internet has been grown last few decades. With the use of the internet need of the security in the internet and devices used for it increased called as the Rogue Access Points (RAP). A RAP is known as non-authenticated devices to accesses the network in the many premises. As the increased used if the smart phones the use of Wireless LANS has increased.

Users are started to use these type of device to use internet for there need it is the good side of the devices. If we see other side there has the chances of the data stolen or analyzed by the attackers are increased. Wireless broadcast employs microwave to extend data over the atmosphere. So within the collection of Access Point (AP) we can access the wireless signals. As the gesture can't be bound for to a particular recipient, it will be easy for cyber criminals to watch network traffic, disturb data flows and penetrate networks. These risks create wireless refuge to be more important.

The main approach is the providing easy and simple suitable functional technique to model the crisis created by the evil attacked the Access Points. Finally in the conclude twin recognition policy that contains access point hope by hope. In the methodology we are recognizing the access points in which we are checking originality of points to prevent the clients from getting malicious and provide security to data access.

A. Evil Twin Recognition

Evil twin attack is that listen the data delivery and access in the wireless LAN in the public places through the access points.

When users that access the twin access point they don't know about attack that. Access the email, secure site or any banking applications. While accessing these services user gives authentication credentials but while delivering data attacker theft the user information. The evil twin may be configured to pass Internet traffic during to the valid access point while monitoring the victim's association or it can only say the scheme is provisionally occupied after obtaining a username and password.

1. Recognition Techniques:

   In our proposed system, we implemented two recognition and detection techniques with the help of java technology using the packet transmission in the network. Wireshark tool used to get all information about the packet which are transferred through the access point and given as the input to the algorithms and stored in to the file for future use.

   1. Trained Mean Match:

      In our proposed system, we implemented two recognition and detection techniques with the help of java technology using the packet transmission in the network. Wireshark tool used to get all information about the packet which are transferred through the access point and given as the input to the algorithms and stored in to the file for future use.

   2. Hop Differentiating Technique

      The distributions of Server IAT in one-hop and two-hop wireless channels differs significantly. By use this figures, a recognition algorithm named Trained Mean Matching (TMM) is implemented. Specifically, specified a sequence of experiential Server IATs, if the mean of these Server IATs has a higher possibility of corresponding the trained mean of two-hop wireless channels, the projected method finish that the client uses two wireless network hops to commune with the remote server signifying a possible evil twin attack.

3. Comparison

   This is the module which compares the both algorithm used in the detection. Both algorithm able to detect the attack in the different environment and different based on the average packet ratio and the execution time.

III. PROPOSED SYSTEM

Attacked access point by evil twin is just as same as the original Access point and looks same. This results user can connect to the malicious node. In the implemented system back track 5 r3 as the main stream of the project.

By using the proposed system user able watch the all traffic which is going from the client side to the server side and conduct the man in the middle attack. By using the wireshark tools analyze the packets travelling from the source to destination. The time between the packets transmissions such as interval arrival time (IAT) on that basis recognize the attack or evil twin. IAT is extracted from the wireshark tool which on the other hand fake AP packet sending time is large then its IAT is bigger than this is called fake AP. We implemented the Two-Hop wireless connection means evil-twin and their IAT is larger than one-Hop.

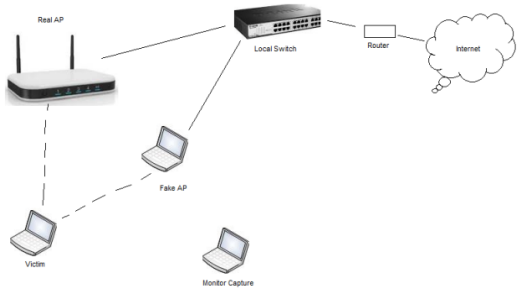

Fig. sWireless Network

A. Block Digram

In the proposed system we have implemented the two techniques train mean match and hop different technique called TMM and HDT respectively. In the block diagram both one and two hop fingers are shown in the above figure. With the help of packets we calculate IAT and Average. Then we derive the second mean .Standard deviation is find out with the help of standard deviation formula. Then probability find out which is similar to TΘ values. We assign

probability to approximately TΘ value. And then TΘ value decides which is evil tween or normal access point scenario. Both the algorithm needs the input files and the trained file. The work flow of the both of algorithms are different with some steps are similar.

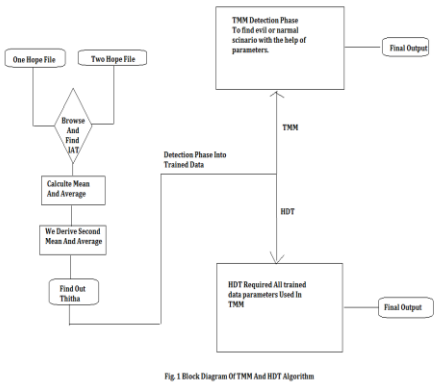

Fig. 1 Block Diagram Of TMM And HDT Algorithm

Fig.Block Diagram of TMM and HDT Algorithm

B. *Mathematical Equations*

Our proposed approach is implemented using the java technology which is platform independent and portable. In which there are authorized clients are generated and there network ids such as IP address SSID and MAC address are used to analyzed the unauthorized users with help of wireshark and using the formulas.

We collect Server IAT in both one-hop and two-hop wireless channels. Then, we compute the mean and the standard deviation of Server IAT collected in the one-hop (normal AP) scenario, with different variables. We are calculating the range with the help of range formula. Then we derive the second mean and calculate average of derive mean called as TΘ. We 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.

IAT is the intermediate packet arrival time of two consecutive packets. In this scenario, we have calculated IAT for one minute's packets and also calculate their average it is related to two hopes.

$$f(IAT)_{NAP} = \int_0^{\mathrm{n}} (\mathrm{Packets})_{\mathrm{NAP}} \quad (1)$$

Then IAT find out for two hope i.e evil tween access point is,

$$f(IAT)_{EAP} = \int_0^{\mathrm{n}} (\mathrm{Packets})_{\mathrm{EAP}} \quad (2)$$

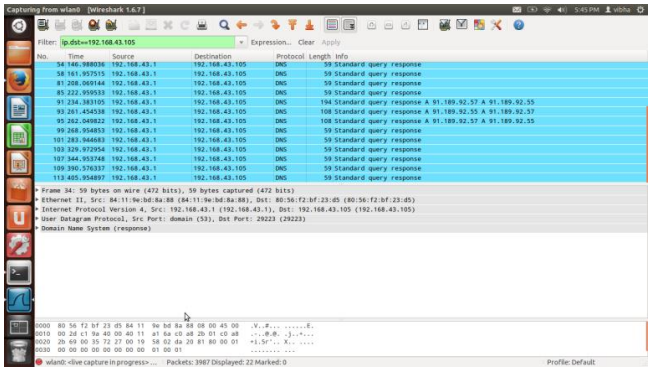

Fig. Packet Capturing

We are finding 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.Whchi is normal and evil scenario. Then we are taken a one random variable which is 1 then we are says that evil tween scenario if random variable is 0 then normal access scenario.

$$f(T\square) = \frac{1}{2} \sum_{n=1}^{\infty} (f(IAT)_{NAP} + f(IAT)_{EAP}) \quad (3)$$

Where $f(T\square)$ the set of average of IAT come from our equation (1) and (2).

IV. RESULTS

This command can be used to enable monitor mode on wireless interfaces.

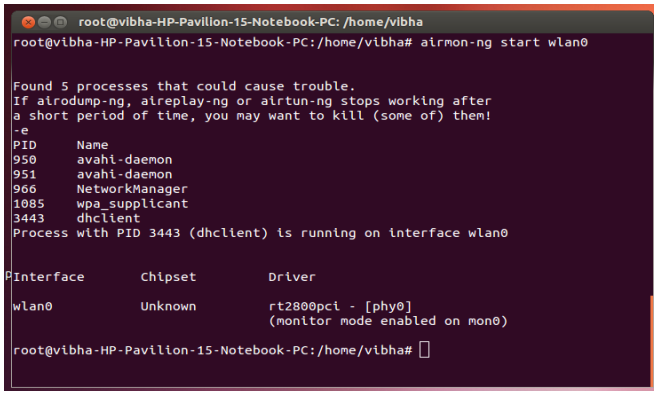

Fig. Command Prompt for create a Evil

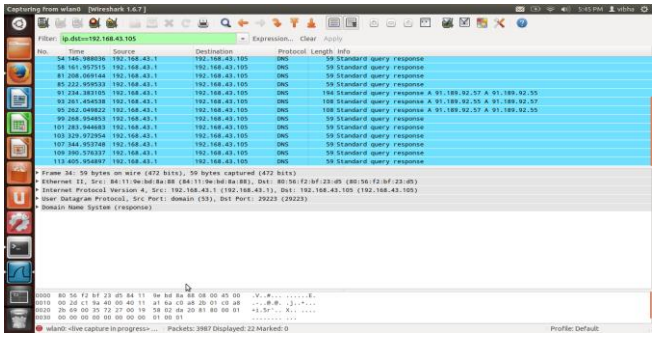

Fig. Wireshark Tool

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

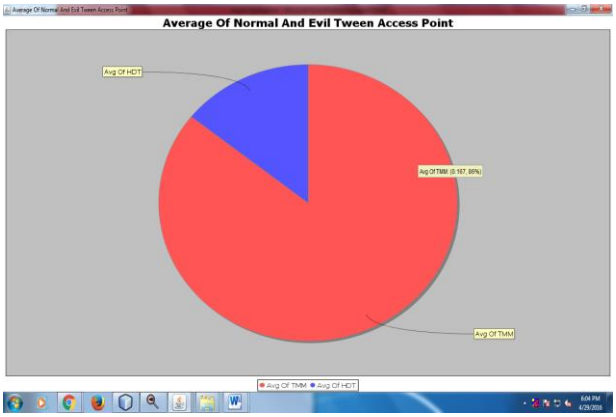

Fig. Graphical Representation

V. CONCLUSION

We studied the evil twin attack and wireless LAN related issues. The proposed system is well defined and able to find the evil twin attack on the access point. The recognition algorithm TMM and HDT performs well. The IAT is the main attendant such as one hop and two hope to train the wireless packet transmission. Analyzed all trained data to find threats. The experimented results shows proposed system prevents and analyze the evil twin attack successfully.

REFERENCES

[1] 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

[2] 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..

[3] M. Bellare, Namprempre, D. Pointcheval, and M. Semanko, “The one-more-rsa-inversion problems and the security of chaum’s blind signature scheme,” Journal of Cryptology, vol. 16, no. 3, pp. 185–215,2003

[4] Public wi-fi useage survey, Identity Theft Resource Center, 2012.

[5] A. Lamaraca, Y, chawathe, s. consolvo, J.Hightower, I smith, J. scoot, T. sohn, J. horward, Jhughes, R, Potter, J. Tabert, P. Powedge, G. Borriello and R Schilit, “Place Lab: Device posiyioning using radion beacons in the wild”, in pervasive, 2005

[6] C. van Rijsbergen, Information Retrieval. 2nd ed. Butterworths, 1979.

[7] How to create an evil twin access point

[8] Fake wireless access point creation-Rouge AP

[9] Evil Twin in Wikipedia

[10] Ter Kah Leng, —Wireless Internet regulation: Wireless Internet access and potential liabilitiesǁ, Computer law & Security Report, Vol. 23 (2007), pp: 550 – 554

[11] P.G.Sasane and S. K. Pathan, “Detection and Elimination of Fake Access Points in WLAN using Multi Agents and Clock Skew Methodology”, International