International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

Detection of Rogue Access Point to Prevent Evil Twin Attack in Wireless Network

Vishwa Modi
M.Tech Cyber Security
Raksha Shakti University
Ahmedabad, India

Asst. Prof. Chandresh Parekh
M.Tech Cyber Security
Raksha Shakti University
Ahmedabad, India

***Abstract* - From last few years open wireless network commonly available in cafe shop, shopping malls, multiplexes restaurants and other public places to provide free internet service. This open accessible wireless network is vulnerable to different types of threats like eavesdropping, man in the middle attack, evil twin attack, etc. In this paper we consider the problem of open Wi-Fi which is susceptible to Evil Twin Attack created using Rogue Access Point. Evil twin attack is phishing scam in wireless network. Attacker creates rogue access point by spoofing the parameters of legitimate access point to steal confidential information of client and for other malicious activity. We proposed solution to detect Evil Twin Attack dependent on different MAC address and same MAC address as well as same external IP addresses and different external IP address of Access points. Our detection method doesn't rely on network administrator's action. It can easily detect evil twin access point and warns client to disconnect from evil twin access point or alert about existence of evil twin access point if available in wireless network.**

Keywords* - *Access Point, BSSID, Deauthentication frames, External IP address, Evil Twin Attack, Security Threats, SSID, Rogue Access Point, Wi-Fi network

I. INTRODUCTION

Nowadays wireless communication is rapidly growing because large numbers of mobile devices are available in market. Wireless network provides flexibility, portability and it is expensive. To meet the large number of demand for accessing wireless network requirement more and more number of wireless access points are used to provide wireless internet access and various security mechanisms are added to provide secure internet service [1].

Large numbers of businesses such as restaurants, cafe, stores, and shopping malls have setup open Wi-Fi access point to provide free wireless internet service. So that people can use internet by connecting to any public Wi-Fi access point. This public Wi-Fi is more vulnerable to security threats. Attacker uses this public Wi-Fi to perform various malicious activity such as intercepting, collecting data such as user's user name, password and other confidential information. As such security threats and vulnerabilities related with the protocol layers are typically protected separately at each one layer to meet the security requirements of wireless network such as authenticity, confidentiality, integrity and availability. But still attackers are targeting the Wi-Fi networks in different ways to capture the network traffic [1].

In Evil Twin attack, attacker creates either a physical AP or evil AP that resemble the original AP so that user will connect to it. Attacker tricks a user into connecting to the Rogue AP instead of the original AP. The attacker spoofs the SSID (name of AP) and BSSID (MAC of AP) of legitimate access point. Victim unknowingly gets connected to this access point which has same SSID. Once victim gets connected to the Evil Twin Access Point or Rogue Access Point, he inadvertently creates a playground for various attacks such as man-in-the-middle attack [8].

In this paper we have considered two scenarios of Evil Twin Attack and proposed solution for that. In one case attacker spoofs SSID as well as BSSID of legitimate access point and connect to legitimate Access Points to provide Internet Service to clients. In another case attacker spoofs only SSID and disconnects all the clients who are connected to legitimate access point. So that users can only get connected to attackers rogue access point [9].

In this paper we improved Open or Public Wi-Fi security by:

Presenting novel detection method for the above discussed two scenarios. As far as we know if rogue access point of evil twin attack connected to the legitimate access point and provide internet service to the client through it then it forwards the packet from client to legitimate access point. So it creates extra hop from source to destination and RTT (Round Trip Time) between source and destination is also increased. Also if rogue access point provides internet service to client through other internet service provider than the legitimate one then their external IP address of ISPs are not same. If two access point with same SSIDs used for load balancing then their BSSIDs are not same and any one of them don't launch deauthentication frame to disconnects clients from access point. So we concluded that if continuous deauthentication frame broadcasted from any one of the access point then it may be under the attack of evil twin access point which is forcefully disconnecting the client connected to legitimate access point.

II. EVIL TWIN ATTACK

The attacker gathers parameters of legitimate access point such as SSID, BSSID, Channel, etc to setup rogue access point to perform Evil Twin Attack. Every access point continuously broadcasts beacon frames to notify the wireless client about the existence of access point. This beacon frames contains SSID, BSSID, Timestamp, channel and many more

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

fields. Every wireless device receives this beacon frame and notify client about existence of wireless access point with SSID. So that client can connect that access point. Now attacker also sniffs this beacon frame to make rogue access point using same SSID and BSSID of legitimate access point. Normally wireless device automatically get connected to open Wi-Fi with higher signal strength. So the attacker also increases the signal strength of rogue access point. Therefore wireless client automatically connect with the attacker's access point without knowing that he is connected to malicious access point [8].

Once the client is connected to this access point this creates playground for attacker where attacker can intercept personal information of client such username, password, unencrypted credential of bank transaction and other critical data by monitoring and capturing the network traffic generated through wireless client's device. Attacker also manages to make fake access point having same MAC and IP of the legitimate AP. So that it's becoming very tedious job to detect the Evil Twin Attack. There are many ways to launch Evil Twin Attack. Different types of tools are available for performing evil twin attack [12]. So that attackers can easily create attack using such tools.

Following figure shows two scenarios of performing evil twin attack for which we have proposed detection method.

In figure 1 attacker spoofs SSID and BSSID of legitimate access point (LAP) and uses them to create evil twin access point. Evil twin access point provides internet service to the client by connecting his access point with the legitimate access point. So that evil twin AP working as man in the middle by forwarding network traffic between client and legitimate access point. Therefore attacker is able to capture all the traffic of client who is connected to him [10].

In figure 2 attacker spoofs only SSID of legitimate access point and uses it to create evil twin AP. In this case attacker provides internet service to client from different access point or from own 3G/4G mobile network. Attacker sends deauth frame using BSSID(MAC address) of legitimate access point to all the clients to disconnect them from legitimate access point. So that clients can only connect with the evil twin AP [11].

III. RELATED WORK

Somayeh Nikbakhsh, Azizah Bt Abdul Manaf, Mazdak Zamani, Maziar Janbeglou [5] performed the detection of Rogue Access Point by comparing the gateways and the routes of a packet that travels through the AP to destination. If two access points of same SSID having different IP and Same Net ID then by monitoring the trace routes of them decide which one has extra hop and notify the client to don't connect to it.If two access point of same SSID having different IP and

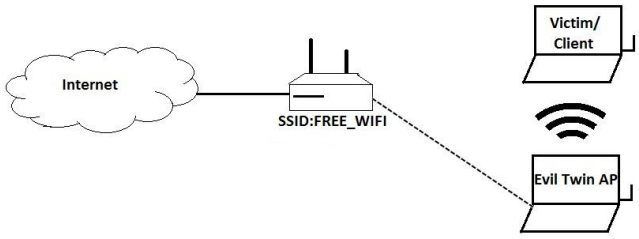

Fig. 1 Evil Twin AP with same SSID, BSSID and uses LAP for internet service

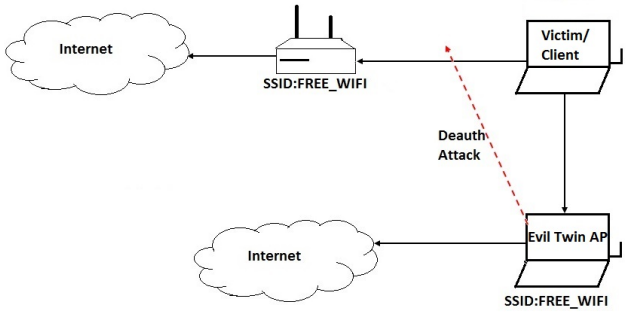

Fig. 2 Evil Twin AP with same SSID, different BSSID and Deauth client from LAP

different Net ID then it monitors the trace route which indicates different route to the same destination. So it warns the client existence of rogue access point.

Anil Kumar, Partha Paul [4] proposed solution works when client has been connected to the AP earlier. They maintained table of SSID, MAC address and Count on AP as well as on client's operating system. AP checks the count value for every connection requesting device in table after matching SSID and MAC address and sends response frame to client with count value. After sending association frame AP increased count value by one. On receiving the Association frame operating system increases the count value and matches with AP's count value. If it is different then frame is dropped and warning message of "Rogue Access Point Detected" is generated.

Hossen Mustafa, Wenyuan Xu [6] proposed client-side CETAD mechanism for detecting the Evil Twin Attack in which they have created one Android Application. They used RTT and ISP information for detection. If attacker uses own network then ISP of legitimate AP and Evil Twin AP is different and RTT value also differs. If attacker uses access network of legitimate AP then RTT values are compared for detection. They used a timing based scheme utilizing the RTT value to detect both Si-Fi attack and Du-Fi attack. RTT time for Evil Twin Access Point is much larger than the legitimate access point.

Nazrul M. Ahmad, Anang Hudaya Muhamad Amin, Subarmaniam Kannan, Mohd Faizal Abdollah, Robiah Yusof [7] discussed client centric RSSI based detection. RSSI value is bounded to the cluster and associated with the distance between AP and client. RSSI value is extracted from wireless frame. RSSI values have rapid fluctuation if RSSI sequences are coming from LAP and Evil Twin. If the distance between the centroid of clusters for two access points is larger than threshold then AP spoofing is detected. For legitimacy of AP estimated distance between client and target AP is calculated and actual distance between client and target AP is calculated from client position. If the different between actual distance and estimated distance is less than certain level then the target AP is RAP. Otherwise target AP is LAP.

Omar Nakhilaab, Erich Dondykc, Muhammad Faisal Amjadd and Cliff Zoue [3] proposed a method for detecting Evil Twin Attack where attacker has different gateway of rogue access point than the legitimate access point having. They used SSL/TCP protocol. For detection client initiates TCP 3-way handshake with arbitrary remote web server which supports HTTPS connection through AP1. Then client

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

switches the internet connection through AP2 which having different gateway. When client try to retrieve web page content from previously connected web server then web server sent RST/ACK packet for rejection of connection. Because gateway of AP is changed and can't able to retrieve web page before again initiating TCP 3-way handshake through AP2. Wireless client is notified abot ETA by warning message.

IV. PROBLEM STATEMENT

In RSSI based detection method if the client is not stationary then it gives false positives. In SMC based detection method if an attacker manages to spoof count value of the number of times connections between the access point and client then attack can be executed. There is no encryption in ICMP packet so that trace route of packets travelling through the rogue access point can be changed to the trace route of the legitimate access point. SSL/TCP based detection method will not work if gateway of rogue access point is same as the legitimate

V. PROPOSED METHOD

A. *Design Assumption*

The proposed detection technique is based on the following assumption of attack: There are different scenarios to make rogue access point to perform Evil Twin Attack in Wireless network. In certain case attacker only spoofs SSID of legitimate access point and use different internet service from the legitimate one to provide internet service to victim whereas in other case attacker spoofs SSID as well as MAC address of legitimate access point and connected to the legitimate access point to use and provide internet service to victim.

B. *Proposed Detection Design*

The detection depends on MAC address and external IP address of AP or ISP. When client start detection process first client connects to any one of the access point to get external IP address of AP1, RTT and number hop counts between client and server. Then client switches connection to another access point AP2 having same SSID as of AP1 to get external IP address of AP2, RTT and number hop counts between client and server.

The fingerprint of access point or any white list of access points is not needed for detection. The detection mechanism can be used by client as well as administrator. Administrator also knows the basic configuration of AP. So this method is very helpful to decide which access point is Evil Twin AP. For client also this detection method is useful to decide to which access point connection is safe and to which access point not to connect or disconnect if connected when there is two access points with same name.

Our proposed detection method will make a distinction that two access point with the same SSID have same BSSID or not also both have same external IP (IP address of ISP) or not. If SSIDs are same and BSSIDs are not same then it will check for continuous deauthentication frames broadcasted by legitimate AP due to attacker wanted to get disconnect clients from legitimate access point. Detecting such deauthentication frames from particular BSSID and alert client that other AP with different BSSID is Rogue Access point which is performing Evil Twin Attack.

If SSIDs and BSSIDs are same then compare external IP addresses of both APs. If external IP addresses are not same then warn client about possibility of Evil Twin Attack. If external IP addresses are same then find RTT value and compare with the value of previous obtained RTT value if any one of the AP having greater value than the other one and then it may be Rogue access point [10]. For confirmation comparing number hop counts. If any of the access point having extra hop count then it will be Rogue Access Point and alert will be generated that ETA detected.

C. *Proposed Flow Diagram*

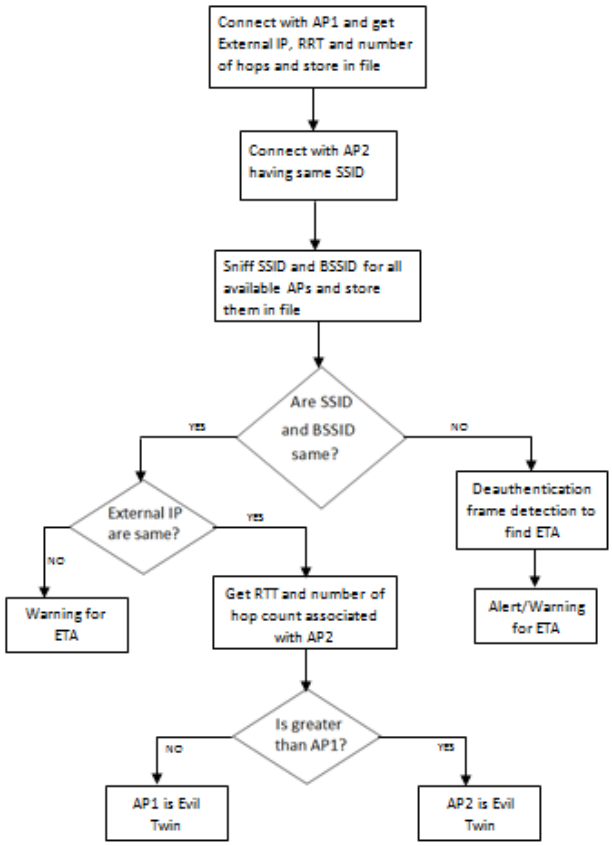

Fig. 3 Flow Diagram of Proposed Detection Method

VI. CONCLUSION

Wireless networks are increasingly being used in commercial applications, public and private sectors. We understood various ways of creating "Evil Twin Attack" in Wi-Fi network. Among which we discussed the particular scenario of evil twin attack for which we have proposed detection method. The proposed method does not need to modify infrastructure of network and it can give effective and efficient result.

REFERENCES

[1] Yulong Zou, Senior Member IEEE, Jia Zhu, Xianbin Wang, Senior Member IEEE, and Lajos Hanzo, Fellow IEEE, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination, Pg. 1727-1765.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

[2] Akhil Gupta, Rakesh Kumar Jha, "Security Threats of Wireless Networks: A Survey", 2015 IEEE International Conference on Computing, Communication and Automation (ICCCA2015), Pg. 389-395.

[3] Omar Nakhilaab, Erich Dondykc, Muhammad Faisal Amjadd and Cliff Zoue, "User- Side Wi-Fi Evil Twin Attack Detection Using SSL/TCP Protocols", 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Pg. 239-244.

[4] Anil Kumar, Partha Paul, "Security Analysis and Implementation of a Simple Method for Prevention and Detection against Evil Twin Attack in IEEE 802.11 Wireless LAN", 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), Pg. 176-181.

[5] Somayeh Nikbakhsh, Azizah Bt Abdul Manaf, Mazdak Zamani, Maziar Janbeglou, "A Novel Approach for Rogue Access Point Detection on the Client-Side", 2012 26th International Conference on Advanced Information Networking and Applications Workshops, Pg. 684-687.

[6] Hossen Mustafa, Wenyuan Xu, "CETAD: Detecting Evil Twin Access Point Attacks in Wireless Hotspots", 2014 IEEE Conference on Communications and Network Security, Pg. 238-246.

[7] 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", 2014 IEEE 2nd International Symposium on Telecommunication Technologies (ISTT), Langkawi, Malaysia (24-26 Nov 2014), Pg.104-109.

[8] Volker Roth, Wolfgang Polak and Eleanor Rieffel, "Simple and Effective Defense Against Evil Twin Access Points", 2008 ACM conference on Wireless network security, Pg. 220-235.

[9] Yang, Chao, Yimin Song, and Guofei Gu. "Active User-Side Evil Twin Access Point Detection Using Statistical Techniques." Information Forensics and Security, IEEE Transactions on 7.5 (2012), Pg. 1638-1651

[10] Omar Nakhila, Cliff Zou, "User-Side Wi-Fi Evil Twin Attack Detection Using Random Wireless Channel Monitoring", IEEE Milcom 2016 Track 3 - Cyber Security and Trusted Computing, Pg. 1243-1248.

[11] Hao Han, Bo Sheng, Member, IEEE, Chiu C. Tan,Member, IEEE,Qun Li,Member, IEEE, and Sanglu Lu,Member, IEEE "A Timing-Based Scheme for Rogue AP Detection" IEEE Transactions On Parallel And Distributed System (2011), Pg. 1912-1925.

[12] Fabian Lanze, Andriy Panchenko, Ignacio Ponce-Alcaidey, Thomas Engel, Hacker's Toolbox: Detecting Software-Based 802.11 Evil Twin Access Points, 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Pg 225-232.