International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 12, December 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

A REVIEW PAPER ON WIRELESS NETWORK ATTACKS: WITH EXISTING METHODS TO LOCATE AND ERADICATE RAPS

Mr.Abhijit S.Bodhe[1] , Dr.A.S.Umesh[2] , Dr.Sanjay Thakur[3]

[1]*Asst.Prof. Computer Science & Engineering, SRES COE, Kopargaon, SPPU, Pune, (India)(M.S)*

[2]*Director & Prof. in Computer Science & Engg., SJVIT, VTU , Bangalore (KA),(India)*

[3]*Principal Lord Krishna College of Technology, RGPV university, Bhopal (MP), (India)*

ABSTRACT

This review paper mainly focuses on wireless communication, as it's become cheaper and more easily available, the day by day use of wireless technology is increasing with lots of risks involved in it. The wireless network can available easily but with that various attacks are imposed on network are discussed in detail. The paper mainly focused on Rouge Access Points(RAP) present in the network its detection methods with famous four elimination methods proposed by various authors, we discuss mainly general four methods with its possible pros and cons where traffic and other parameters like stats about network, client involvement plays vital role for detection and elimination of such RAPs.

Keywords: MAC spoofing, Rogue Access Points (RAPs), RAPD (RAP Detection), Traffic, Wireless Networks.

I INTRODUCTION

Wireless networking presents many advantages Productivity improves because of increased accessibility to information resources. Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, because communications takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can read it, thereby compromising confidentiality. Although wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems. The objective of this paper is to assist managers in making such decisions by providing them with a basic understanding of the nature of the various threats associated with wireless networking and available countermeasures.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The popularity of wireless Networks is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. The majority of computers sold to consumers today come pre-equipped with all necessary wireless Networks technology. The benefits of wireless Networks include: Convenience, Mobility, Productivity, Deployment, Expandability and Cost. Wireless Network technology, while replete with the conveniences and advantages described above has its share of downfalls. For a given networking situation, wireless Networks may not be desirable for a number of reasons. Most of these have to do with the inherent limitations of the technology.

The disadvantages of using a wireless network are: Security, Range, Reliability, and Speed. Wireless Networks present a host of issues for network managers. Unauthorized access points, broadcasted SSIDs, unknown stations, and spoofed MAC addresses are just a few of the problems addressed in WLAN troubleshooting. Most network analysis vendors, such as

Network Instruments, Network General, and Fluke, offer WLAN troubleshooting tools or functionalities as part of their product line.

1.1 Wireless Network Attacks and Types

- **Accidental Association**

  Unauthorized access to company wireless and wired networks can come from a number of different methods and intents. One of these methods is referred to as “accidental association”. When a user turns on a computer and it latches on to a wireless access point from a neighboring company’s overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network.

- **Malicious Association**

  “Malicious associations” are when wireless devices can be actively made by crackers to connect to a company network through their cracking laptop instead of a company access point (AP). These types of laptops are known as “soft APs” and are created when a cracker runs some software that makes his/her wireless network card look like a legitimate access point. Once the cracker has gained access, he/she can steal passwords, launch attacks on the wired network, or plant trojans. Since wireless networks operate at the Layer 2 level, Layer 3 protections such as network authentication and virtual private networks (VPNs) offer no barrier. Wireless 802.1x authentications do help with protection but are still vulnerable to cracking. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the cracker is just trying to take over the client at the Layer 2 level.

- **Ad-Hoc Networks**

  Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-topeer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

- **Non-Traditional Networks**

  Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. These nontraditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.

- **Identity Theft (MAC spoofing)**

  Identity theft (or MAC spoofing) occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to only allow authorized computers with specific MAC IDs to gain access and utilize the network. However, a number of programs exist that have network "sniffing" capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires, and the cracker can easily get around that hurdle.

- **Man-in-The-Middle Attacks**

  A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a "de-authentication attack". This attack forces APMan-in-the-middle attacks are enhanced by software such as LANjack and AirJack, which automate multiple steps of the process. What once required some skill can now be done by script kiddies. Hotspots are particularly vulnerable to any attack since there is little to no security on these networks.

- **Denial of Service**

  A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

- **Network Injection**

  In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as "Spanning Tree" (802.1D), OSPF, RIP, and HSRP. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.

- **Caffe Latte Attack**

  The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.

1.2 Brief History About WAN and Awareness

Wireless networking provides numerous opportunities to increase productivity and cut costs. It also alters an organization's overall computer security risk profile. Although it is impossible to totally eliminate all risks associated with wireless networking, it is possible to achieve a reasonable level of overall security by adopting a systematic approach to assessing and managing risk. This paper discussed the threats and vulnerabilities associated with each of the three basic technology components of wireless networks (clients, access points, and the transmission medium) and described various commonly available countermeasures that could be used to mitigate those risks. It also stressed the importance of training and educating users in safe wireless networking procedures.

- **Training and Educating Users**

  Notice that Figure 1 also includes users as the fourth basic component of wireless networking. As is the case with wired security, users are the key component to wireless networking security. Indeed, the importance of training and educating users about secure wireless behavior cannot be overstated. To be effective, user training and education needs to be repeated periodically

- **Network Auditing**

  Wireless network auditing is an important part of WLAN security policy. The network needs to be regularly audited for rouge hardware. In this method the network is scanned and mapped for all access points and WLAN nodes. Then this is compared with previous network map. Commonly available network mapping tools like netstumbler and wavelan-tool can be used to do this. Specialized tools such as Airsnort can be used for WEP cracking and auditing the network for weak keys, key reuse and WEP security settings.

- **Securing Wireless Client Devices**

  Two major threats to wireless client devices are (1) loss or theft, and (2) compromise. Loss or theft of laptops and PDAs is a serious problem. laptops and PDAs often store confidential and proprietary information. Consequently, loss or theft of the devices may cause the organization to be in violation of privacy regulations involving the disclosure of personal identifying information it has collected from third parties. Another threat to wireless client devices is that they can be compromised so that an attacker can access sensitive information stored on the device or use it to obtain unauthorized access to other system resources.

Securing Wireless Access Points

Insecure, poorly configured wireless access points can compromise confidentiality by allowing unauthorized access to the network.

- **Countermeasures to Secure Wireless Access Points**

  Organizations can reduce the risk of unauthorized access to wireless networks by taking these three steps:

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

1. Eliminating rogue access points;
2. Properly configuring all authorized access points

- **Eliminate Rogue Access Points**

  The best method for dealing with the threat of rogue access points is to use 802.1x on the wired network to authenticate all devices that are plugged into the network. Using 802.1x will prevent any unauthorized devices from connecting to the network.

- **Secure Configuration of Authorized Access Points**

  Organizations also need to ensure that all authorized wireless access points are securely configured. It is especially important to change all default settings because they are well known and can be exploited by attackers.

1.3 Existing Methodologies for Detecting & Eradicating Rogue Access Points with Pros &Cons

1.3.1. RAP Detection Scheme Using Statistical Techniques

- **Working**

First we will see method [4], RAP detection scheme using statistical techniques. The goal of this method is to detect evil twin attacks in real time under real wireless network environments. This targeted evil twin attacks, the evil twin AP pretends to be a legitimate one to allure victims to connect and utilizes the legitimate AP to relay users' network packets to the Internet. This approach is client-side one, second Secondly, unlike merely based on the learning knowledge; this method designs two different algorithms (a learning-free algorithm and a learning-free algorithm) to detect evil twin attacks.

For the learning-based algorithm, this method theoretically obtain the threshold from the intrinsic WLAN properties rather than using relatively static and empirical values, through exploiting fundamental communication structures and properties in the evil twin scenario. In addition, it also utilize SPRT technique to tolerate reasonable noise. However, this work designs two algorithms to detect evil twin attacks, based on two different wireless network statistics and analyses of intrinsic wireless network properties, with the considerations of dynamic changes of real-world wireless network parameters. Also, unlike designed as a server side approach, this work is a client-side approach suitable for traveling users.

These method present two algorithms to detect evil twin attacks: Trained Mean Matching (TMM) and Hop Differentiating Technique (HDT). Both algorithms utilize the Sequential Probability Ratio Test (SPRT) technique .TMM algorithm requires knowing the distribution of Server IAT as a priori (trained) knowledge. However, the HDT algorithm does not have such a requirement. Instead, it is directly based on theoretical analysis. so it is more appropriate for scenarios where the distribution of IAT is either unknown, instable, or unable to be (perfectly) trained.

- **TMM Algorithm**

Based on the training technique [4], the TMM algorithm affords an effective approach to detect evil twin attacks. However, in some cases, it is too time-consuming or impractical for a normal user to acquire a priori knowledge, particularly the training data for two-hop Wireless channels. In addition, the trained knowledge in one wireless network can be hardly directly applicable to another network. These limitations motivate to design

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

an effective and practical non-training-based algorithm to detect evil twin attacks – Hop Differentiating Technique (HDT).

- **HDT Algorithm Description:**

It now describes the HDT algorithm [4] in detail. Different from the TMM algorithm, in the HDT algorithm, it use a theoretical value for the threshold rather than a trained threshold to detect evil twin attacks. In the theoretical computation phase, it computes a threshold as the SAIR boundary to differentiate one-hop SAIR and two-hop SAIR. In order to use the SPRT technique, it also compute the upper bound for the probability of the SAIR exceeding the threshold in the normal AP scenario, and the lower bound for the probability of the SAIR exceeding the threshold in the evil twin AP scenario. This method acknowledge that once an attacker knows about HDT algorithm, he may attempt to evade it by making the server IAT similar to AP IAT under the evil twin scenario (e.g, maintaining different bandwidth for the first wireless hop and second wireless hop).

- **Pros of the Method**

i)This method provide a novel lightweight user-side evil twin attack detection technique. ii) It present two algorithms, TMM and HDT. That implement this methods prototype system and evaluate it in several real-world wireless networks, and evaluation results proved its effective and efficient.

- **Cons Of the Method**

i) It is possible that attackers may attempt to evade detection scheme, because attackers, between the victims and normal AP, can manipulate the traffic to affect IAT. However, by doing this, attackers need to exactly know how HDT work. Also, a low practical bandwidth between the attackers to victims may decrease attackers' attractions to victims. In addition, designed TMM algorithm can be combined with HDT and be used to detect such anomaly.

ii) Finally, In this method timing-based detection techniques may not perform well once attackers pretend to be the users to get the next data packet and send it back to the users, which is also a challenge to most of current timing based evil twin detection approaches. Further studies are needed in this area

1.3.2. Detection of Rogue Access Point using Timing based Scheme

- **Working**

In this method [3], it considers a scenario when a wireless station tries to join a WLAN to access the Internet. Later scanning the channels, the station will discover multiple APs within its communication area. Some of these APs are authorize and some might be rogue APs. Objective of this method is to design an algorithm that helps the station to detect the rogue AP. The detection algorithm should work in all IEEE 802.11 wireless networks without need additional modifications from the network administrator. This method proposes a scheme uses a client-oriented approach, where a user can avoid connecting to a fake AP. This can be combined with administrator-oriented approaches where the system administrators actively detect and disable rogue APs. It assume that the rogue AP will be launched using a mobile device with two wireless interfaces. The first interface connects the fake AP to the legitimate AP. The second interface pretends to be a legal AP to induce users to connect to it. When a user connected to the fake AP, the fake AP will forward packets from the second

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

interface to the first interface, and then toward the legal AP. This way, the user will still be able to use the Internet as if connected to a legal AP[4].

Here, it considers some defenses that can be circumvented by a sophisticated adversary [3] Identity & verification. Users can run programs like trace route to determine whether the connected AP is a rogue AP. trace route will gave the number of intermediate hops to a host site. From the output, the station will gain knowledge that a suspicious AP exists in the route. However, the rogue AP can evade this detection by monitoring the wireless channel to learn the SSID and MAC address of a legitimate AP, and then set up the fake AP to have the identical parameters. The rogue can then, will not forward the real AP's reply to the user, thus giving the thought that it is connected to the same gateway as a legitimate AP. Traffic monitoring. Traffic monitoring is a technique to distinguish between wireless and wired traffic. A longer interval indicates that the TCP packets are travelling over a wireless connection. However, since the user connecting to a legitimate or rogue AP must use a wireless link, the resulting time slice between TCP ACKs will experience high variance due to fluctuating channel conditions. This made looks like the traffic monitoring technique unsuitable for rogue AP detection. The station may use the timing information such as the round trip time (RTT) to detect a fake AP.

Since the fake AP consists of an additional wireless link to the legitimate AP, this may cause a delay when transmitting data. The station can find the RTT by sending a message such as a ping request or TCP data packets and wait for a reply. However, the rogue AP can simply forge a response to the client, thus avoiding the time penalty of the additional wireless link. For example, the fake AP can generate a ping response to return to the user without forwarding the request to the real AP. In the same manner when the user sends a TCP packet, the fake AP can return the ACK to the user directly.

This methods rogue AP detection [3] protocol uses timing information based on the round trip time. The idea is to let the user probe a server in the local network and then measure the RTT from the response. The user repeats this process for many times and records all the RTTs. suppose the mean value of RTTs is statistically larger than a certain threshold, we regard the associated AP as a rogue AP. This method propose a protocol and show how to determine the parameters[5]

- **Network Traffic Conditions**

To determine the wireless traffic conditions, we compute another RTT using probe request and probe response messages. [3] These messages are generally used when a station is scanning for APs. There are two advantages of using probe request and response. First, by calculating the durations between these two packets, it can estimate the channel traffic and the AP's workload. The reason is that in a busy channel, both the probe request and response will take a long time to transmit due to channel contention and retransmission after signal collisions. Similarly, when the AP has a heavy workload, i.e., the AP is sending many packets for other associated stations, the probe response message has to wait in the AP's transmission queue for a long time before being sent out. Second, it is difficult for a rogue AP to replicate a busy channel by intentionally delaying the probe response because commercial wireless card drivers do not dispatch this kind of low level management frames to OS. Furthermore, it is difficult to delay a probe response since this function is not supported by

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

regular wireless drivers[6].

However, a regular probe request has a drawback in that it is a broadcast message and every AP that overhears this request will respond. This leads to multiple responses, which will create unnecessary channel contention and lead to biased RTT measurements. Furthermore, a broadcast message will not be retransmitted if lost. The associated AP that does not receive the probe request correctly will never reply. This may affect the RTT values. Therefore, it modify the probe request packet to be a unicast message. This is done by putting the MAC address of the target AP into the destination field in the probe request. This will ensure that only the target AP will respond and other APs will not. Also, the station will automatically retransmit the probe request if needed.

- **Cons of the Method**

In this method following factors that have influence on timing RTT, which may lead to false results.

Data transmission rate: RTT is inversely proportional to data transmission rate. High transmission rate usually leads to small RTT.

Location of DNS server: In some small hotspots (e.g., coffee shops, restaurants), APs are usually connected to a close DNS server or resolver provided by ISP. This server may be located some hops away from APs.

In this case, it has possibility to falsely identify a legitimate AP as a rogue AP due to large RTT. AP's workload : AP's workload is related to the utilization of AP's queue.

1.3.3 Detection of RAP Using Received Signal Strengths

- **Method**

In the detection method,[1] which consists of three phases.

1) Collection of RSSs: the first phase measures the RSSs from nearby APs.

2) Normalization of collected RSSs: for accurate measurement, the second phase estimates some missed RSSs, caused by air conditions, such as interference, home appliance, noise or, etc., and normalizes the estimated RSSs for generalization of a variety of wireless environments.

3) Classification of RSSs: Finally, this method determines which RSSs are highly correlated to others based on empirical threshold value Δ. It define that the highly correlated RSS sequences as fake signals from a single device.

- **Collection of received signal strengths**

In the first phase, this method [1] collects the RSSs from nearby APs. In IEEE 802.11 infrastructure, the received signal strength indicator (RSSI) is a measurement of the power present in a received radio signal using beacons from nearby APs. There are two techniques to read beacons in WLANs. The first is an active scanning that sends a probe request message from a client to nearby APs. The AP's response is a probe response message to the client. The second technique is passive scanning, which involves listening for beacons from nearby APs. The APs typically send 10 ~ 100 times per second.

- **Normalization of signal strengths**

After the collection of received signal strengths, it estimate and normalize the vectors S for suitability to detecting fake APs. When it collect signals, some low signals or intermittent appearing signals can be collected

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

from nearby APs due to some characteristics of WLANs, such as distance of APs, reflection, etc. The phenomenon of wrongly collected signals causes the received signal strength to become zero; this is termed missing data. Missing data can be a consequence of a failure result.

- **Classification of RSSs:**

The last step classifies [1] whether a RSS is multiple-signal or not. The classification process measures a distance of two randomly selected signal sequences. If the distance is above the Δ,it will cluster the two signal sequences that are highly correlated with each other. The highly correlated signals are classified into multiple signals generated from a fake AP.

- **Pros of the Method**

i) This method is designed to be Lightweight solution on the client side.

ii) To guarantee availability to the client, this method discovers fake APs without extra monitoring devices or network manager privilege in WLANs [7].

iii) This method does not require modification of the AP device, and it can detect the fake APs even if their traffic encrypted.

- **Cons of the method**

i) To guarantee the mobility of a client, this method considered developing the fake AP detection method on a limited platform such as a Smartphone

1.3.4 A Novel Approach for RAP detection on Client Side

- **Working**

Existing rogue access point detection methods [2] are mostly for wireless network administrators. These administrator-side solutions are expensive, limited and not available in many cases. For example, mobile users, who use public Wi-Fi at airports, hotels, or cafes, need to protect themselves from rogue access points. As we cannot stop Wi-Fi popularity, it is necessary to protect Wi-Fi users by offering them a lightweight rogue access point detection system on their devices. When a general user wants to use a public Wi-Fi, there are many access point SSID to choose from. Some of them have similar SSIDs and pretend they provide same network. The main question is how to differentiate between a rogue access point and a legitimate one. How the average computer user, who does not have any information about wireless networks and authorized list of Access points, is able to use their own mobile device (laptop, cell phone) as a detection instrument is the main concern of this technique.

The main problem here is, while a user enjoys public wireless network, they cannot be sure that they are connected to the legitimate wireless access point or an unauthorized one. The second problem is many common methods of client-side rogue access point detection are only limited to the MITM scenarios. For instance, those methods would not cover the state when a hacker shares their own broadband internet connection with the same SSID as public Wi-Fi. In general the rogue access point threat can be classified in two different categories. The first category of rogue access points is those which threaten user by Man-In-The-Middle attack. An attacker can simply implement this attack by configuring a rogue access point which imitates an authorized one. Then they

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

just forward packets to the legitimate access point. Man-In-The-Middle attack inserts the attacker between client and authorized access point. The attacker is able to sniff all the packets. The second category of rogue access points are those which presents threats to user by evil twin attack. In this kind of attack, an attacker spoofs the MAC address of the legitimate access point. In the second step they begin to broadcast the same SSID as genuine access point. When user connects to the evil twin AP an attacker can easily access user's traffic.

- **Method/Working of Technique**

Detecting rogue access point is a challenging task.[2] The main difference between proposed model and the current methods is the steps and the way we apply to detect rogue access points for different type of rogue access points. Current solutions are just available for MITM scenario or evil twin scenario. Because all rogue access points are not behaving in the same way, there is a necessity to have one comprehensive solution that is able to work in different scenarios. Our proposed solution detects both MITM attack and evil twin attacks. There are three states according to the information it collects; this method is able to determine if there is a definite rogue access point (MITM scenario), possibility of being tricked by a rogue AP (evil twin scenario), or if it is a safe network[8]. It consider two public APs broadcasting the same SSIDs and MAC addresses. In the first step, two IPs are compared. There are two possible results for this comparison. If they are equal, the trace routes will be compared. The first situation could not happen, because both access points have same SSIDs, MAC and IP addresses and packet travels exactly the same route. According to network logic, it could not have two same IP addresses in one network simultaneously. If this situation happens it will cause IP address conflict and both devices will stop working.

Therefore the only answer would be the same IP addresses with different trace routes. This condition is the result of IP spoofing. This method does not have any references to check which one is the authorized access point, so it just warns the user about evil twin attack. If network IDs are the same, it indicates that both APs are in the same network. This situation is the result of load balancing in the network. The network administrator may use two access points (with same network ID) for load balancing purpose. Therefore, IPs are different but Net IDs are the same, it is safe to connect to either of them. In this state, the green light will ensure the user that they could connect securely to both of them.

Another possible [2] result is different IPs and different network IDs. In this situation, the algorithm executes a trace route on both access points and compares the results. If there is any extra hop in the result, which is the proof of man in the middle, the red light will notify the user it is not safe to connect to this access point. In this state, the hacker had set up an access point to broadcast the same SSID as the public access point. The IP address of this network is different from the genuine one. The attacker lures users to connect to the rogue access point and after capturing packets they may pass them to the authorized access point.

This will cause the extra hop in trace route result. The last condition is when both access points' IP addresses and network IDs are different, and the trace-route result indicates different routes to the same destination. In this state, the attacker rings his own access point to the public place and broadcast the same SSID. This state will cause some experienced users connect to the rogue one. In this state, the yellow light will be switched on. As it mentioned before, this technique could not decide which access point is the authorized one, because this

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

technique works on client-side and there is not any previous knowledge about the network that could be used as the reference. Therefore, the yellow light just warns the user that this network is not safe.

In summary,[2] In this method SSID comparison result is used as a traffic light by this method. If the comparison result shows the same route, it means using both networks are safe. If the result of comparison is different then there is an indication of warning by yellow light, which says using this network is not safe. and if the comparison states any additional hop in the trace route, it means there is possibility of Man in the Middle attack so in such a case red light will indicate states that connecting to such a network is not at all safe.

- **Pros of the Method**

i) It can detect Man in the middle and evil twin attack efficiently[9].

ii)There is no need to modify network architecture if you are using this method, as it works on client side.

iii) Any Client side device can serve as detection mechanism, no special device needed for detection.

- **Cons of the Method :**

i)This method only notify user about rogue access point.

II CONCLUSION

The Study shows that we are still away from a technique that will clearly identify rogue access point. Such a technique will collect constructive or precise information from network to determine whether a device is rogue or not. This is quite challenging as network traffic is penetrate through multiple devices. so there is need to discover technique that will be hybrid i.e. for wired and wireless. This will minimize the weaknesses of both wired and wireless techniques while maximizing their strengths.

ACKNOWLEDGEMENTS

I thank all who supports for writing this paper including college staff and Principal also my family members, Special thanks to my current PhD guide Dr.Umesh And M.Tech guide Dr.Thakur for his valuable & quality time spend and making this paper in reality.

REFERENCES

[1] Taebeom Kim, Haemin Park, Hyunchul Jung, and Heejo Lee,Online Detection of Fake Access Points using Received Signal Strengths.

[2] Somayeh Nikbakhsh, Azizah Bt Abdul Manaf, Mazdak Zamani, Maziar Janbeglou, A Novel Approach for Rogue Access Point Detection on the Client-Side.

[3] Hao Han, Bo Sheng,, Chiu C. Tan, Qun Li, and Sanglu ,A Timing-Based Scheme for Rogue AP Detection.

[4] Chao Yang, Yimin Song and Guofei Gu, Active User-side Evil Twin Access Point Detection Using Statistical Techniques

[5] http://compnetworking.about.com/cs/wireless/g/bldef_ap.html.

[6]http://www.computer-network-security-training.com/how-to-detect-a-rouge-access-point.

[7]http://www.smallbusinesscomputing.com/webmaster/article.php/3590656.

[8] http://www.trainsignal.com/blog/rogue-access-points-still-here-and-still-a-threat.

[9] Graham, E., Steinbart, P.J. *Wireless Security(2006)*