Volume 3, Issue 10, October 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Study of Different Rogue Access Point Detection and Prevention Techniques in WLAN

Sachin R. Sonawane *, **Sandeep P. Chavan**
MTECH COMPUTER,
BVDUCOE, Pune
Maharashtra, India

Ajeet A. Ghodeswar
MTECH I.T.,
BVDUCOE, Pune
Maharashtra, India

Abstract : WLAN security has demonstrated incredible favourable advantages in numerous fields, With adaptable and straightforward access, remote LAN systems administration has an extensive variety of requisition. Remote usage have expanded exponentially in venture situations, the security of the aforementioned mechanisms has come to be more of a concern Conveying Access Points, and limiting the utilization of the aforementioned Access Points to approved clients has been a test because of the powerless verification and encryption utilized within 802.11x guidelines. A fake AP might be set in any open spaces so as to imitate honest to goodness APs for adaptation. Existing fake AP detection methods analyze wireless traffic by using extra devices, and the data of traffic is collected by servers. The second type of rogue APs are set on a portable laptop with two wireless cards, one connected to a actual AP and the other configured as an AP to provide Internet access to WLAN stations. Rogue access point is one of the most serious threats in WLAN. In this paper we will study different RAP detection techniques with their pros and cons.

Keywords : WLAN,RAP

I. RAP Detection Scheme Using Statistical Techniques

A . 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.

This 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.

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

C. HDT Algorithm Description:

It now describe 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 compute 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).

D. 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.

E. 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) It is possible that if the workload of legitimate AP is extremely heavy, the time difference between one-hop server IAT under the normal AP scenario and two-hop server IAT under the evil twin AP scenario becomes less distinguishable. Thus, the accuracy of this TMM algorithm may be decreased. However, in this way, HDT algorithm can perform better. Particularly, HDT does not rely on any training data and relies on the server IAT to AP IAT ratio. Specifically, if it is under the evil twin AP scenario and the legitimate AP is busy, then the ratio of two-hop server IAT (between the client and the server) to one-hop AP IAT (between the client and the evil twin AP) will become even larger.

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. More further studies are needed in this area.

II. Detection of Rogue Access Point using Timing based Scheme

A.Working

In this method [3] it consider 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 propose 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 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.

B. Adversary Model

Here, it consider some defences 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.

C. Background

In this method the station contact a DNS server, and make use of the DNS lookup as the probe message. In addition, it uses two 802.11 management frames, probe request and probe response, to find the effects of network traffic.DNS server and lookup. [3] The basic function of DNS is to provide a distributed database that maps human-readable host names (such as www.cs.edu) to IP addresses (such as 128.239.28.68). The servers managing this distributed database are known as DNS servers. Current networks typically cache the queried records to achieve high performance. There are two typical types of DNS lookups, a recursive query, and a non recursive query. In a recursive DNS lookup, a station queries a local server for a host name. If this server cannot answer the query, it will contact the root DNS server which will then recursively ask other servers to determine the IP address. In a non recursive query, the local DNS server will only search the cached records locally without contacting the root DNS server. If no matches are found, the local server will send a "host not found" message back to the station.In this methods algorithm, it uses non recursive query as the probe message to measure the RTT between the user and the DNS server. The user will send a DNS request for a host name with the non recursive option. The user then waits for the response from the local DNS server and measures the RTT. The user repeats this process using a different host name each time. This scheme is efficient since most local networks may have a local DNS server or resolver for performance reasons .Therefore, a station can always send a request to the local DNS server and the time spent on the wired network is small due to the local communication.

Furthermore, since DNS lookup support is compulsory, all networks will have this function. At the end, since the DNS response changes for different queries, the adversary cannot guess in advance the user's query. The adversary also cannot guess whether a particular query can actually be satisfied by the real DNS server. Any fake AP that returns an wrong answer will be detected by the user. This cause a fake AP to forward the request to the real DNS server to ensure that the reply is correct.

D. 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 regular wireless drivers. 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.

E. DNS Operations

This scheme [3] has two DNS operations. The first is to determine a set of n different host names for measuring n samples of RTTs. The second operation is verifying DNS answers. Determining DNS queries. It generate DNS queries as follows: In a station, two pools are constructed. The first pool contains valid host names that can be extracted from local caches of web browsers (like Firefox and IE). The other pool contains some randomly generated host names. In this there is no knowledge whether they are valid or not. Once the two pools have been constructed, it will randomly select a pool to pick a host name to test. Then, delete that host name from the pool to avoid using it again. This prevents a rogue AP from remembering the corresponding answers. Note that if it need a lot of samples, it assign a smaller weight to the first pool to prevent it from exhausting too fast. Verifying DNS answers. Suppose that a station hears m þ 1 ðm _ 1Þ APs composed of m legitimate APs and one rogue AP. The station will first randomly select one AP and send a recursive DNS query to it. Assuming this selected AP is not a rogue AP, it will execute this recursive query. This forces the local DNS server to provide an answer to the query by querying other name servers on the Internet and cache the response. The station then uses the same host name and queries all other APs in non recursive queries. Now the answer to the query should be cached on the DNS server. it then execute Algorithm 1 on the remaining APs.

The legitimate APs will respond accordingly with a reasonably short RTT. For the rogue AP, if it chooses to forward the query, the rogue AP will be detected by this algorithm. If the rogue AP does not forward the query, the rogue AP does not know the correct answer and can only return a "host not found" message. The station can thus determine that AP is a rogue AP. If the selected AP is a rogue AP, it must forward the recursive DNS query to the real AP. This is because if the rogue AP does not forward the query, the DNS server would not contain the correct answer. When the station runs this algorithm, all the other APs will reply with a "host not found" message. When this happens the rogue AP will be detected, since a legitimate AP will always execute the recursive DNS query. then repeat the process for the remaining APs to detect the rogue AP.

F. Pros of the Method

i)This method, present a practical, timing-based scheme for the end user to avoid connecting to rogue APs. This is done without any assistance from the network administrator.

ii) This timing-based rogue AP detection algorithm is compatible with the existing networking protocols, and can be applied to 802.11 network (including both 802.11b and 802.11g) without further modifications by network administrators.

iii)This method can detect powerful rogue APs that actively try to avoid detections as opposed to an "accidental" rogue AP deployed, for example, by an innocent employee in an office.

G. 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 have 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.

Wireless traffic :Wireless traffic may incur large variance of RTT. That is because some packets may be sent immediately with no contention, but some packets may be deferred for a long time due to collision or interference with others. The variance may hide rogue AP's additional wireless link, and make the detection hard.

III. Detection of RAP using Received Signal Strengths

A.Working

This method [1] propose a novel fake AP detection method in the client-side. To overcome the limitations of the client-side, This method is designed to be a lightweight solution. The key process of this method is to find highly correlated RSS sequences that can be collected in any wireless devices. If a similarity of RSS sequences is less than a threshold value, it define the RSS sequences as fake signals. This method divide work into two categories s: Server-Side and Client-Side. This method,[1] focus on the fake AP scenario because there are some reasons that the rogue AP scenario is unsuitable in the real-world . The first reason is of the limited number of Ethernet ports. Also, when the rogue AP is successfully connected to the ethernet network, it cannot move closer to clients for inducement. Finally, network managers can disable unknown devices connected to the Ethernet network.

B. FAKE AP DETECTION USING RECEIVED SIGNAL STRENGTHS :

In this it describe the fake AP detection method in order to measure the optimal threshold value.

Fake AP detection 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 $\sim$ 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 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.

C. 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.

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

D .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.

IV . A Novel Approach for RAP detection on Client Side

A.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 are 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 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.

B. The Proposed Method

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. 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 lure 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 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.

C. Pros of the Method

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

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.

D.Cons of the Method :

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

V. 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.

REFERENCES

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

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

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

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

[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.

