Providing Data Security in WLAN

Sunil Shirsat
Research Scholar – Department Of Information Technology (M.E)
Smt. Kashibai Navale College of engineering, Pune-16, Maharashtra, India

Swapnil Sanap
Patent Analyst – Department Of Intellectual Property Rights
Legasis Services Pvt. Ltd, Pune-16, Maharashtra, India

ABSTRACT

Currently many organizations utilize the wireless LAN to provide the access channel to the Internet and Intranet enabling the flexible workforce. While doing so, communications with the Internet is continuously maintained. owever the wireless security is always a primary concern. So for securing data in WLAN it is necessary to detect unauthorized access points which are installed without explicit authorization from a local network management. Rogue APs potentially open up the network to unauthorized parties, who may utilize the resources of the network, steal sensitive information or even launch attacks to the network. This has forced the develop systems that will not only detect the unauthorized access points but also detect network attacks performed by authorized or unauthorized access points so that it protects data from external misuse. In network attacks, the hackers try to break the security of the network, by affecting host and then proceeding towards further damage. Due to the above security and performance threats, detecting unauthorized APs as well as detecting attacks performed by unauthorized or authorized AP'S is one of the most important tasks for a network manager.

Keywords:
Wireless network security, Rogue Access Point, Network attacks

1. INTRODUCTION:

1.1 Why security in WLAN?

Security is the key word for any kind of public, multi usage networking or interface. Security involves protection of data against malicious eyes and hands and transmitting confidential matters to the correct authorities.

- With a wireless LAN, transmitted data is broadcast over the air using radio waves, so it can be received by any wireless LAN client in the area served by the data transmitter. Because radio waves travel through ceilings, floors, and walls, transmitted data may reach unintended recipients on different floors and even outside the building of the transmitter. Installing a wireless LAN may seem like putting Ethernet ports everywhere, including in your parking lot.

Similarly, data privacy is a genuine concern with wireless LANs because there is no way to direct a wireless LAN transmission to only one recipient.

1.2 Need for rogue access point detection in IEEE 802.11

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in the- middle attack. Rogue access points can pose a security threat to large organizations with many employees, because anyone with access to the premises can ignorantly or maliciously install an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Within a properly secured WLAN, rogue access points are more damaging than rogue users.

Unauthorized users trying to access a WLAN likely will not be successful at reaching valuable corporate resources if effective authentication mechanisms are in place. Major issues arise, however, when an employee or hacker plugs in a rogue access point. The rogue access point helps an attacker in gaining access to sensitive information of an organization. Employees have relatively free access to a company's facilities, which makes it possible for them to mischievously install a rogue access point. An employee, for example, installs his personal access point without permission of network administrator in order to support wireless printing or access to the network from a conference room.

Software programmers working on wireless applications may connect an access point to the corporate network for testing purposes. In order to avoid this situation, it is necessary to implement security policies that mandate conformance with effective security controls and coordination with the network administrator before installing access points. This can only be effective, nonetheless, if you clearly inform employees of the policies. A hacker can install a rogue access point to provide an open, non-secure interface to a corporate network. In order to do this, the hacker must directly connect the access point to an active network port within the facility. This requires the hacker to pass through physical security. However, that's easy to do in most companies.

Therefore there is an urgent need of developing technology which will address problem of rogue access points. Although fair amount of work has been done in investigating efficient methods of detecting rogue access point in wireless LAN, but still this area offers plenty of opportunity for further investigation because most of the solutions available today are far from satisfactory.

1.3 Need for network attack detection

Network attack as the name suggests is the act of using a computer system or its resources without earning authorized privileges, with an intention to cause significant damage. Whereas Network attacks Detection is a process that performs the basic task of finding individuals or machines that attempt attack on a dedicated network. (NADS) Network Attack Detection Systems are nothing but software programs that perform detection activity by analyzing apparent behavior against mistrustful patterns, in real-time. It is basically a network based activity. With global network connectivity, which is continuously increasing the subject of network attacks has been successful to achieve prominence, encouraging active research in attempt towards building an efficient NADS.

2. RELATED WORK:

2.1 Literature survey:

It is really necessary for network administrator to detect Rogue Access Points. Wei Wei, Kyoungwon Suh, Bing Wang, [1] briefs us that most existing commercial products use following approaches. They either manually scan the RF waves using sniffers (e.g., AirMagnet, NetStumbler) or automate the process using sensors. This paper propose two online algorithms to detect rogue access points using sequential hypothesis tests applied to packet-header data collected passively at a monitoring point. Both algorithms extend TCP ACK-pair technique to differentiate wired and wireless LAN TCP traffic. The Algorithms make prompt decisions as TCP ACK-pairs are observed, and only incur minimum computation and storage overhead in paper Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with TCP ACK-Pairs.

Shetty, Sachin, Song, Min, Ma, Liran, [2] uses traffic characteristics of network for rogue access point detection. Here novel approach is proposed to detect RAP in a heterogeneous network comprised of wired and wireless subnets. The approach is implemented in two consecutive phases. The purpose of both the phases is traffic analysis performed at the gateway router by a network traffic analyzer (NTA). In the first phase, the NTA analyzes both inbound and outbound traffic and determines whether an end-host belongs to an Ethernet or WLAN.

In the second phase, the NTA analyzes the traffic from end-hosts on WLANs to compute the frequency of straight access and crossing-access attempts. If a WLAN end host generates traffic which causes the access point to access the port on the gateway router to which the access point is connected physically, then the access attempt is considered straight-access. If a WLAN end-host generates traffic which causes the access point to access the port on the gateway router to which the access point is not connected physically, then the access attempt is considered crossing-access. If the frequency values of these access attempts exceed a threshold, the NTA then alerts the network administrator that the end-host is connected to a RAP in paper Rogue Access Point Detection by analyzing Network Traffic Characteristics.

Srilasak, S. Wongthavarawat, K. Phonphoem, A [3] explains in paper Integrated Wireless Rogue Access Point Detection and Counterattack System how integrated approach can be used for rogue access point detection.

The algorithm is as follows:

- Compare the sniffing data (i.e., SSID, Wireless MAC) with the authorized AP information which is already stored.
- For Completely Matched, there are two possibilities of access points: *Trusted AP* or *Attacker Rogue AP*. The attacker rogue AP completely spoofs the authorized AP information (i.e., spoof MAC and spoof SSID).
- For Partially Matched, the result would be either Misconfiguration AP or Attacker's Rogue AP. The Misconfiguration AP is the access point with configuration that is not consistent to the registered AP.
- For Completely Unmatched, the result would be either Neighborhood AP or Employee rogue AP. Beyah, R. Kangude, S. Yu, G. Strickland, B. Copeland, [4] explains how temporal traffic characteristics are used to detect RAP. The primary goal of this research is to detect rogue APs from a central location with the detection independent of the wireless technology. The author shows a scalable solution, thus not attempting to reassemble data before analysis. Also, this solution will function independently of the signal range of the rogue APs. The research involves comparing traffic characteristics of flows from different sources in a LAN segment and detecting traffic coming from a wireless AP. The aim of this research is to experiment and derive such state representation and its derivation from the observed temporal characteristics of traffic. Here an additional PC was used to observe traffic traversing the link. The network sniffing software used was Ethereal in paper Rogue Access Point Detection using Temporal Traffic Characteristics.

Han, H., Lu, Lu, X.L., and Ren, L.Y. [12] explains scanning and searching the signature in database is really time consuming so data mining concept is used to discover signatures in network based intrusion (Network attack) detection in paper "Using Data Mining to Discover Signatures in Network-Based intrusion detection"

One of the approaches of designing a network security is to define network behavior patterns that indicate improper use of the network and also look for the occurrence of those patterns. While such an approach may be capable of detecting varieties of known intrusive behavior, it would allow new or undocumented types of attacks to go undetected. As a result, this leads to a system which monitors and learns normal network behavior and then detects deviations from the normal network behavior. An NADS (Network Attack Detection System) may use anomaly based techniques, signatures, or both. Alerts are any sort of user notification for an intruder activity. When NADS detects an intruder, it informs the security administrator about this by using alerts. These alerts may be in the form of logging to a console, pop-up windows, sending e-mail and so on. It is an unrelenting active attempt in discovering or detecting the presence of network attack activities. As Network attacks Detection (ID) relates to computers and network infrastructure it encompasses a far broader scope. It refers to all processes that are used in discovering or detecting unauthorized uses of network or computer devices.

2.2 Problems in existing methodologies

2.2.1 Brute force approach:

- This approach, however, is ineffective and time-consuming.
- Scans are not effective as a RAP can easily be unplugged when the scan takes place.
- In addition, IT personnel must upgrade their detection devices to accommodate multiple frequencies.

2.2.2 Enterprise-wide scan from a central location:

- This approach is expensive as one must place sensors or access points throughout the entire enterprise to monitor the air waves.
- Also this approach can be ineffective if a malicious employee uses a directional antenna, or reduces the signal strength to cover the small range within his/her office.

2.2.3 RF monitoring:

• This approach has a limitation as that it heavily relies on certain specific features of IEEE 802.11, which can be easily turned off or violated.

2.2.4 Network attack detection using concept of data mining:

• If Apriori algorithm is used for mining data then it become very time consuming to scan and search a signature in database. So this solution is not a much effective.

3. PROPOSED SYSTEM:

In this project we have developed two different modules. First module is used for detection of unauthorized access points. Second module is used for detection of network attacks performed by authorized as well as unauthorized access points, It also drops all the packets come from unauthorized access point so that it don't achieve the purpose for which it is connected.

3.1 Module 1: System architecture of unauthorized access point detection in WLAN:

Here we have considered three types of access points 1. Authorized 2. Unauthorized and 3. External. Authorized APs are the AP configured by network administrator. So these are the actual APs of network. External APs are the AP whose signal can be reachable to my laptop. But these AP are of external network. So we should not connect to this network and discard such AP from rogue AP detection. Some APs are harmful to our network as they are set to steal our data. They can use the SSID of our network or MAC and can divert network traffic through that access point. So we want to detect such access points for that purpose we will use different filters. The first filter we will use is to check SSID or MAC. If SSID is of different network that might be the AP of external network so we will not apply any other filter on that. But if SSID or MAC is of same network then we apply another filter. Another filter is applied using IP and MAC.IP and MAC is compared with stored database if match is found then access point is authorized otherwise it is unauthorized. Then next filter is applied for MAC spoofing if anybody is try to use MAC of authorized AP still that rogue AP is detected through our system. One more advantage of our system is for not to spoof MAC it is possible to change MAC address through our software. So using these entire parameters rogue AP is detected.

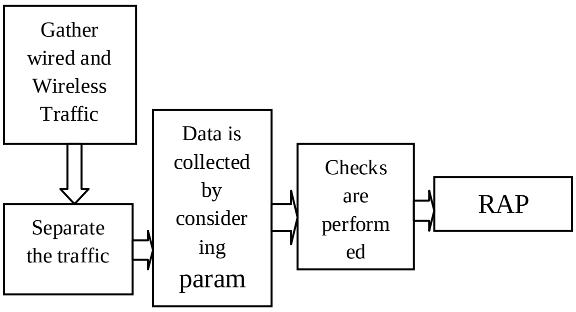

Gather wired and Wireless Traffic
Separate the traffic
Data is collected by consider ing param
Checks are perform ed
RAP

Fig. 1 System Architecture of Unauthorized Access Point Detection in WLAN

As shown in Fig. 1 first we capture packets then we separate the traffic and consider wireless packets. Packets are collected by considering 1. Unregistered MAC, Duplicate MAC and Unregistered IP. Then checks are performed with stored database and Rogue Access Point is detected.

3.2 Module 2: System Architecture of network attack detection:

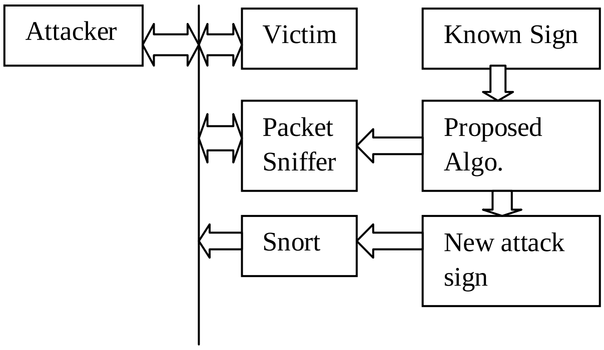


Fig.2 System architecture of Network Attack Dktection

By the observation of the attach signatures, we find that there are some attack signatures which are similar to attack signatures generated previously. This mainly happens, because the new attack which gets generated is a derivative of the previous known attack. For e.g. worms. All worms are similar because the main task of any worm is to consume network resources by propagating itself in the network and eventually force the system to halt. There are several examples which show that there is some kind of similarity between many different attacks and the existing ones. Therefore our plan is to use some part of the known signature to find out the new attacking signature. For this we can use the Traditional Apriori Algorithm, but it takes much time to generate candidate item sets and scan the database. Therefore, we suggest an algorithm to identify intrusions by making use of old signatures, which will save a lot of processing time.

As shown in Fig.2 Attacker gets an attacking tool to attack victim. Our algorithm takes two kinds of data one comes from packet sniffer and other comes from the known signature. Our algorithm outputs the new attack signatures derived from known signatures. Snort is used to check signature accuracy we find out.

3.2.1 Algorithm for network attack detection:

Parameters used in the Algorithm:

The following parameters will be used in our algorithm.

D: A set of transactions where every transaction is a packet.

1. C: The candidate itemset.
2. S(c) The support of the candidate c is the percentage of transactions that contain c.
3. min_sup: Minimum support meets the threshold.
4. Known_signature :The part of signature we have known.
5. Max_len : Maximum length of frequent itemset that contains the known signature.
6. N : Length of known signature + 1.
7. k–itemsets : An item set having k items.
8. Sig: Current frequent- item set in Lk.

9. Lk: A set of frequent k-itemsets (with minimum support: The set has two fields: item set and support count).
10. Ck A set of candidate k-itemsets (potentially frequent itemsets). The set has two fields: item set and support count.

Finding out Frequent K item sets

In the first step, all of the frequent items will be found. And then we use a simple way to scan the database in order to find the frequency of occurrence of each item, and decide which one meets the minimum support. Secondly, we generate the candidate n-itemsets by checking all of the possible combinations of the frequent items with already known signatures, if they meet the minimum support requirement. Then, append this n-itemsets from right. Finally, the maximum length of frequent-item set can be mined by our method.

ALGORITHM STEPS

```
Input: D, min _sup.
Output: Lk
STEPS
Step 1: L1= find_frequent_1_itemsets(D, min_sup);
Step 2: Ln= find_frequent_n_itemsets(D, L1, min_sup,known_signature);
Step 3: for k=n+ 1 to max_len do
Step 4: Ck= candidates_gen (D,L1,Lk-1, min_sup);
Step 5: Answer=Lk
```

There are three procedures used in above algorithm which are explained below. The first is find_frequent_1-itemsets,and the second is find_frequent_n-itemsets. The third is candidates_gen. In find_frequent_1-itemsets we read one transaction each time from database and then count the support of each different item. If an item occurs twice in the same transaction, the support count of this item will increase once. Repeat until no transactions available in database. Finally, we will check all items in candidate 1-itemset and append the item that meet the minimum support into L1 .

In find_frequent_n-itemsets all frequent items have been mined, we will stop generating all possible candidate 2-itemsets just like the Signature Apriori algorithm. We generate the candidate itemsets only related the known signatures. Then, all of the frequent items will be concatenated to the known signature and put them into candidate n-itemsets. After that, check all item sets in the candidate n-item set. Then, add the itemsets that meet the minimum support into L1 , assume that A, B, C and D are frequent items. {B C} are the part of known signature. We will check whether {B C A}, {B C B}, {B C C} and {B C D} meet the minimum support and determine the frequent itemsets. In candidates_gen first append all frequent items to sign until no any s(sign + item) meet the minimum support. Repeat this until no any s (item+sign) meets the minimum support.

Working of the algorithm

We assume that the transactions in the database are {{A B C D E F G Q},{M N A B C D E F G},{ J A B C D E F G},{P Q I}}. The attack signature we have already known is {C D E}. Let the minimum support be 0.7. Applying the proposed algorithm, we can firstly get the frequent items L1={A B C D E F G}. In order to find out the derived attack signature we expanded the known signature by each frequent item, and we then we have Cn={ {C D E A},{C D E B},{C D E C},{C D E D},{C D E E},{C D E F}, {C D E G}} at the first stage. After we have Cn candidate itemsets, we scan the database to find out the Ln={C D E F}. Then we let the Ln be the new attack signature that we have already known. Repeating the step until the minimal support is no longer satisfied We win get the Ln ={ C D E F G} in this example. Next, we expand the Ln in the inversed direction. Finally, we will get the possibility attack signature Ln ={A B C D E F G}

3.3 Features of the system:

- This software is enhancing the network security by solving two different problems. It is detecting rogue access points as well as network attacks performed.
- Our system detects Rogue access point but along with it drop all the packet send by RAP so the task of RAP is not achieved.
- Technique used here is cost effective. We do not require any extra sensors and hardware.
- No need to have knowledge of the attacks.
- Able to detect & prevent any type of malicious flag combination.
- No need for user to take any kind of action on the attacks.
- Display continuous notification about the attacks which have been prevented.
- Allows the network administrator to view existing signatures.
- Provides a log file about all the attacks prevented.

3.4 Why our software is better than other existing software's:

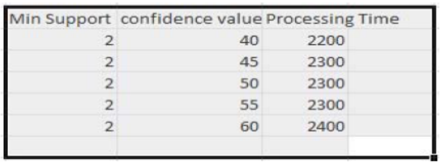
- Existing software's are used for detecting Rogue access point. But through our software we are not only detecting RAP but also detect and prevent attacks performed on our network.
- We are not allowing to pass the packets send by RAP on network so RAP is not achieving the purpose for which it is connected on network.
- We are detecting RAP using MAC spoofing, but not to spoof the MAC easily we are also providing facility of changing MAC through our software.

3.5 Experimental analysis for network attack detection:

Lot of analysis is done. And following are the actual results of our software. Processing Time is the time taken by the compiler to generate no of iterations.

3.5.1 Following is the graph of minimum support count and processing time.

Here, minimum support is 2.Processing time is almost constant as confidence value increases.



Min Support	confidence value	Processing Time
2	40	2200
2	45	2300
2	50	2300
2	55	2300
2	60	2400

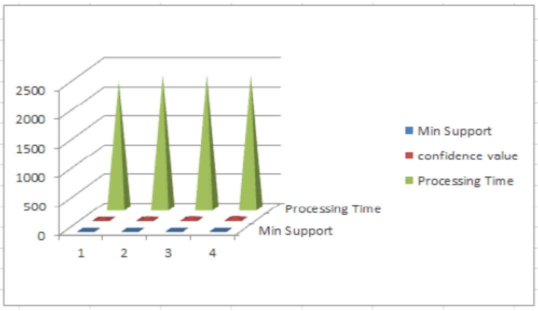
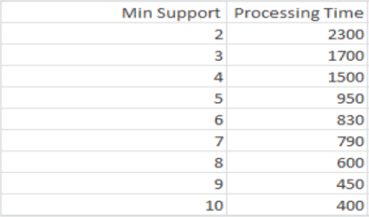


Fig. 3 Graph showing processing time

3.5.2 The graph of minimum support count and processing time.

Here, we prove that as minimum support count increases processing time also decreases.



Min Support	Processing Time
2	2300
3	1700
4	1500
5	950
6	830
7	790
8	600
9	450
10	400

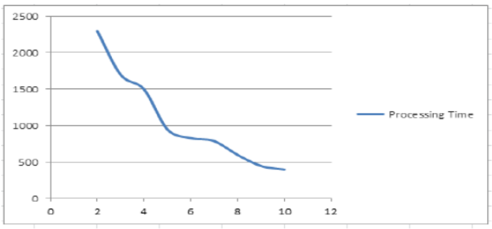


Fig 4. Graph showing changed processing time

4. CONCLUSION:

In our project, we have implemented the Rogue access point detection and network attack detection System. Our Project can be used in the organization level to provide security because it is used for dual purpose like detection of Rogue access point as well as detection of network attacks. It also drops all the packets which are send from rogue access point.

Thus in this research work we have successfully achieved our aim of detecting Rogue AP and network attacks by using the attack information from the attack definition datasets. For achieving we have employed the technique of detecting new attacks based on the information of known attacks. We have used the KDD dataset for the same, and applied the signature Apriori algorithm which is well known and widely used network attack detection algorithm our results illustrate that our system effectively detects attacks as compared to other systems.

Our system exhibits consistent results with minimum overheads. Our solution is effective and low cost. It is designed to utilize the existing wireless LAN infrastructure. There is no need to acquire the new RF devices or dedicated wireless detection sensors.

5. REFERENCES:

[1] Wei Wei, Kyoungwon Suh, Bing Wang, "Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with TCP

ACK-Pairs" ,IMC'07, October 24-26, 2007,IEEE CNF, San Diego, California, USA.

[2] Shetty, Sachin ,Song, Min ,Ma, Liran, "Rogue Access Point Detection by Analyzing Network Traffic Characteristics" Military Communications Conference, 2007. MILCOM 2007, IEEE, Orlando, FL, USA,

[3] Srilasak, S. Wongthavarawat, K. Phonphoem, A,"Integrated Wireless Rogue Access Point Detection and Counterattack System", Information Security and Assurance, IEEE CNF April 24-28, 2008,Pathumthani,Thailand.

[4] Beyah, R. Kangude, S. Yu, G. Strickland, B. Copeland, J., "Rogue access point detection using temporal traffic characteristics" Global Telecommunications Conference, GLOBECOM '04,IEEE CNF, Atlanta, GA, USA.

[5] Raheem Beyah, Shantanu Kangude, George Yu,Brian Strickland, and John Copeland, "Rogue Access Point Detection using Temporal Traffic Characteristics," in Proc. of IEEE GLOBECOM, Dec. 2004.

[6] Hu Zhengbing, Li Zhitang, Wu Junqi , "A Novel Intrusion Detection (NIDS) Based on Sinatures Search of Data Mining" in 2008 IEEE workshop on knowledge Discovery and Data Mining.

[7] Lee,W.,Stolfo, S.J. and Mok,K.W. "A Data Mining Framework For Building Intrusion Detection Model", in Proceeding of the IEEE Symposium on Security andPrivacy,1999. pp.153-157.

[8] Yang,X.R.,Song,Q.B.and Shen, J.Y.,"Implementation Of Sequence Patterns Patterns Mining In Network Intrusion Detection System", in Proceeding of ICII,2001. pp.323-326.

[9] Hu Zhengbing, Ma Ping. Data Mining Approaches to Signatures Search in Network Intrusion Detection. Control Systems and Computers (USiM). №.1, 2005.pp:83-91. ISBN:0130-5395.

[10] Hu Zhengbing,Shirochin V.P., Su Jun, An Intelligent Lightweight Intrusion Detection System(IDS), Proceedings of IEEE Tencon'2005, Melbourne, Australia, 21-24