Abstract—Presence of rogue access points (APs) is becoming a major concern for the organizations. Administrators in organizations are worried because these rogue APs now introduce serious security threats. It is both simple and inexpensive to setup a rogue AP. Current approaches to rogue AP detection have high false positive and false negative rate. Moreover, some of them can be easily evaded by an attacker. We propose a Challenge-Response based solution to detecting rogue APs which requires no additional functionality from the existing APs and could be easily extended to detect rogue APs throughout the organization boundary. Moreover, the solution also handles the rogue APs that spoof identity of legitimate ones.

I. INTRODUCTION

Use of wireless routers is becoming common in home networks. The main reason behind this is that the prices of APs are dropping and it is trivial to setup an access point. User mobility and convenience are other reasons for increased usage of wireless APs. Almost all laptop computers and embedded devices have a facility to use wireless connection. Further, it is now possible to share a single internet connection with hundreds of devices without use of wires. However, the ease of setting up an access point has raised concerns among the system administrators. Employees in an organization can now run their access point using the network connection they are authorized to use. Often they do not enable strong security features on these APs due to lack of knowledge or negligence. The result could be disastrous. Everyone in the range of this AP is now able to access the internal network without requiring authentication. Thus, security imposed by the wired networks is lost. Even if there is no wireless network in the organization, the network is under threat.

Employees of the organizations are not the only ones responsible for setting up rogue APs. An attacker can setup a rogue AP on a compromised machine inside the network thus enabling him seamless access to the network. In fact, many organizations including small and large companies, Universities, Hotels etc. provide their users with an internet connection. Therefore presence of rogue APs has become a serious problem.

Existing solutions for rogue AP detection have a higher possibility of false alerts. Some of them are hard and some impractical to use. Some of them require enterprise wide scan of air waves to search rogue access points. We introduce a novel challenge-response based approach for rogue AP detection. Our approach allows to point out frames coming from the rogue AP even if the rogue AP is using same SSID and MAC as one of the legitimate APs. The remainder of the paper is organized as follows. Section II describes the current approaches. Section III describes background of our scheme and explains the challenge-response technique in details. Section IV describes the experimental setup. Section V describes the performance analysis of the results obtained. It also describes advantages and possible attacks on the proposed IDS and solutions to prevent those attacks. Section VI gives the conclusion and the final section VII recites future work and enhancements possible in the proposed system.

II. CURRENT APPROACHES

As discussed in [2], most of the current approaches are primitive, these are mainly classified as follows,

A. Wired Approaches

The usual approach queries routers and switches for the MAC address assignments of AP. This approach fails because MAC addresses can be spoofed easily by a rogue AP. The other approach makes use of httpd on the web server associated with AP. This assumes that the wireless router responds to the httpd queries. Some solutions follow LAN only approach in which they probe the network to identify the profile of wireless AP. It requires a workstation to sit on each segment of the network, and hence the approach proves not scalable.

B. Wireless Approaches

The schemes that use wireless approach enable scanning of frames. These use separate hardware devices like sensors or APs to detect beacon frames. These captured frames are analyzed at a central management system which follows various network policies. This technique is not useful for networks that do not have wireless APs. It has much dependency on multiple sensors or APs to monitor the air waves.

C. Hybrid Approaches

These systems listen at network layer 2 and 3 and query switches and routers to determine what devices are connected to them. These fail for the same reasons that the wired only solutions discussed above fail.

III. BACKGROUND ON OUR SCHEME

The goal of our solution is to detect rogue access points in the network. Our solution is independent of the make of the access points. It is designed to work with any access point without requiring any additional functionality from the
access point. Access point is expected to provide a Wired LAN interface. Following figure (Fig 1) shows the layout of our solution.

The Wireless Intrusion Detection System (WIDS) we propose consists of machines with two network interfaces. One interface connects the WIDS to the access point via ethernet network and the other interface which is a wireless interface, monitors the traffic near the IDS. Identification of a rogue access point from legitimate one is done based on the fact that only the legitimate access point is connected to the wired interface of the IDS. Potential rogue APs are detected using sequence number analysis proposed for MAC spoof detection in [1]. Next we describe various strategies used to implement the solution we propose.

A. Sequence Number Analysis:

This technique makes use of the specification[3,4] that consecutive frames sent by an AP will have consecutive sequence numbers unless the frame is being retransmitted or it is a fragmented frame. For example, if we observe a frame with sequence number 1000, the next independent frame sent by the access point will have sequence number of 1001. If the frame was retransmitted, the only difference between that frame and its predecessor will be the retransmit flag and the CRC. In our solution, every frame within a predefined window of sequence numbers is preserved. Whenever another frame that has the same sequence number as one of the frames in the preserved frames is seen, the content of the new frame has to be exactly the same except for the retransmit flag and the CRC[4,5]. If it is not, then there is high possibility that the frame has been spoofed by an attacker. It should be noted that either the old frame or the new one could be an illegitimate frame. For example, the attacker could sniff the last frame sent by an AP. Before the AP sends out its next frame, the attacker will send out a new frame with the next sequence number.

Various attack scenarios to be considered are as follows:

B. Typical Attack Scenarios

In this context, the word 'Attack' implies introduction of a rogue AP in the network for either malicious or non malicious purpose. Various combinations of (MAC/BSSID, ESSID, channel) give rise to different kinds of rogue APs. We broadly classify them in following two classes.

1) In the first class, an attacker introduces the rogue AP with same ESSID, MAC and the same channel as that of legitimate AP. The attacker floods the legitimate access point with frames effectively ceasing its operation. Thus a legitimate AP now stops responding to the requests sent by its clients. The attacker then brings up his own AP and fools the clients into connecting to her rogue AP. The Attacker would start sending frames with next sequence number for the reasons evident from the above discussion on Sequence Number Analysis. After some time period the real AP will recover from the flood attack and start responding again. Typically this time period is 12 seconds for class 1 and class 2 access points[3]. The AP may continue transmitting frames with the next sequence number or it may reset its sequence number.

2) Other variants of rogue APs will have at least one of (MAC, ESSID, channel) different than that of the legitimate AP. If SSID and/or MAC used is the same as that of a legitimate AP, there is a high probability that the AP has been setup to fool the users into connecting to the SSID/MAC they are familiar with. In all other cases, the rogue AP is just any unwanted wireless access point in the network.

In either of the scenarios mentioned above, a client may be a victim of the MITM attack as the client is now connected to a rogue AP. Rogue AP may also enable the attacker to get unauthorized access to the network.

Main focus of our solution is locating the exact frames that came from the rogue AP in attack variant 1) even though this rogue AP has same characteristics as the legitimate AP. This is explained later in this section.

C. Challenge-Response Technique

This technique makes use of challenge response mechanism in order to identify a rogue AP. As shown in the figure 1, the IDS is connected to a legitimate access point via Ethernet LAN interface. However this connection does not directly enable us to identify the legitimate AP. This is because no special information about the AP will be communicated over Ethernet LAN interface to the WIDS.
In challenge response technique, we send a challenge request to the Ethernet LAN interface of the IDS. This request is sent by the wireless interface of the IDS. The AP will route this request to the LAN interface of the IDS. The process listening on the LAN interface will then send a challenge response destined for the sender. The AP will again route the response back to the wireless interface. Thus only the real AP will be able to send the challenge response in the air first.

For security reasons, encryption techniques are used for encrypting challenge and response messages. Challenge is encrypted with the key shared between the two interfaces of the IDS. Challenge is basically a random number that is encrypted. Response will contain a number one greater than the that in challenge.

Structure of challenge and response messages is shown in following figure.

![Message Formats](image)

The delimiter D1 is added in order to distinguish challenge/response message from other frames. We use Data Encryption Standard (DES) in order to encrypt the challenge and response nonce. The challenge message is not sent in clear text to prevent the attacker from getting encryption of any arbitrary number. In worst case, attacker may be able to replay the old challenge message but it is of no use to her. Moreover the key can be changed periodically in order to make it difficult to break the challenge response mechanism.

The message above is encapsulated inside a TCP packet. This packet does not need to have valid values for TCP sequence numbers and other fields, because it is both read and interpreted at MAC layer. TCP is not the only format one can use. The system could use any other protocol like UDP or even a totally new protocol. Our choice of TCP was just a matter of convenience in tracking the packets. Also if the challenge/response takes multiple hops on the LAN to reach the wired LAN interface, routing may be involved. Thus we may also need to include IP addresses in the message.

**D. Putting these concepts together**

- Consider attack scenario a). Assume that the legitimate AP has been brought down by the attacker when it was at sequence number n. The attacker in order to look legitimate uses sequence numbers (n+1) onwards to transmit her frames. After certain period of time, the attacker will have reached sequence number (n+m). At this time the real AP recovers from the attack. It starts sending out its frames starting at sequence number (n+1) (because it had stopped at n) or 0 (if the sequence number was reset during recovery). The IDS detects inconsistency between the two sequence numbers (n+m and n+1). It will then send a challenge to both the APs. Note that since both the APs have identical characteristics, a single message will reach both of them. (Thus in this case, only one challenge message needs to be transmitted). The real AP will route this challenge message to the Ethernet LAN interface of IDS. Ethernet LAN interface will reply to this with response message which is again routed via real AP to wireless interface of IDS. Thus ideally this packet will be transmitted in the air with sequence number (n+2). Thus IDS will come to know that sequence number (n+2) belongs to legitimate AP and (n+m) is sent by a rogue AP. Note that in practice, the response message would be (n+k) where k > 2. This is because AP may be sending other packets before it routes the response message. Our experiments show that k will be typically in the range (2-10)[Refer Table 2]. Thus this approach has made it possible to identify exactly which sequence number is from the attacker.

- In all attack scenarios in b), detection of rogue AP is simpler. Our IDS system monitors all beacon frames in its range. It then issues challenges to those APs. If those APs are able to respond to the challenge successfully, they are considered legitimate. (Note that wired LAN interface of the IDS has to be connected to all real APs in order to achieve this). This case covers combinations like AP having same SSID different MAC, same SSID, same MAC but different channel etc. Multiple challenges may be required to be issued in some cases. For example, if there are two APs in the network with same SSID but different MACs, we send two different challenges to both of them and if both of them are able to respond, both of them are legitimate. Thus another thread will have to be spawned that tracks the other access point and the current thread no more tracks the other access point from here onwards.

Our experiments have shown that in order to be able to route a message to Ethernet LAN interface of the IDS through the access point, we need a legitimate MAC that is currently associated with that access point. System should know one MAC that is currently associated with AP. It can do such association if required.

**IV. Experimental Setup**

The base scenario of the experimental setup is depicted in Figure 1. It shows an access point, the laptop machine where IDS resides. It is connected to the access point through the Ethernet network as well as the wireless network. There will be other clients that are connected to AP over wireless.
network. The figure also shows a wireless card acting as a rogue access point that enters the wireless network. There are two processes in the IDS, first is the main process of IDS, and the other is challenge responder process. The main process of IDS performs the network traffic analysis, it detects the potential rogue AP based on the sequence number analysis. Further, it incorporates the logic to send challenge requests and to validate the challenge response.

Whenever it discovers any potential rogue AP, it sends the challenge request to the probable rogue APs and validates the response received from the access points. Both the challenge requester and challenge responder processes run on the same IDS machine. The main process that has challenge requester logic uses the wireless network interface and challenge responder process uses the Ethernet interface of IDS machine. The destination end of the challenge request message is the Ethernet interface on the IDS machine. Only the legitimate AP can route the challenge request to the Ethernet interface on IDS. If any new legitimate AP is added, it will still have the connectivity to the IDS through the Ethernet LAN. So when this AP is discovered by the IDS, it can be authenticated successfully.

V. PERFORMANCE ANALYSIS

A. Statistics:

Tables 1 and 2 show the data that was collected to judge the performance and effectiveness of our solution. The significance of each table is also described.

<table>
<thead>
<tr>
<th>Sequence Number at which inconsistency is detected</th>
<th>Timetaken of the packet in column 1</th>
<th>Timetaken of the challenge packet</th>
<th>Timetaken of response packet</th>
<th>Sequence number of response packet</th>
<th>Effective response time of IDS</th>
<th>Sequence number gap</th>
</tr>
</thead>
<tbody>
<tr>
<td>2246</td>
<td>32.871025</td>
<td>15.935997</td>
<td>16.97591</td>
<td>2257</td>
<td>0.208176</td>
<td>11</td>
</tr>
<tr>
<td>2391</td>
<td>24.11231</td>
<td>26.71225</td>
<td>26.23410</td>
<td>2399</td>
<td>0.103110</td>
<td>9</td>
</tr>
<tr>
<td>2551</td>
<td>35.041609</td>
<td>36.001437</td>
<td>36.045109</td>
<td>2562</td>
<td>0.105109</td>
<td>11</td>
</tr>
<tr>
<td>2710</td>
<td>46.881388</td>
<td>48.244933</td>
<td>48.04879</td>
<td>2717</td>
<td>0.103481</td>
<td>11</td>
</tr>
<tr>
<td>111</td>
<td>4.60558</td>
<td>4.75513</td>
<td>4.71052</td>
<td>115</td>
<td>0.103489</td>
<td>6</td>
</tr>
<tr>
<td>249</td>
<td>34.441466</td>
<td>34.545767</td>
<td>34.44552</td>
<td>249</td>
<td>0.103486</td>
<td>20</td>
</tr>
<tr>
<td>462</td>
<td>24.89229</td>
<td>24.740327</td>
<td>24.78046</td>
<td>462</td>
<td>0.103537</td>
<td>7</td>
</tr>
<tr>
<td>823</td>
<td>35.227490</td>
<td>35.388687</td>
<td>35.33028</td>
<td>823</td>
<td>0.103315</td>
<td>7</td>
</tr>
<tr>
<td>1138</td>
<td>45.027101</td>
<td>45.09595</td>
<td>45.17350</td>
<td>1141</td>
<td>0.146746</td>
<td>5</td>
</tr>
</tbody>
</table>

![Fig. 4. Table 1 - Timing Characteristics](image)

Table 1 shows how a client responds when it finds an AP to be unresponsive. For this experiment, we simulated the Denial Of Service (DOS) on AP by switching it off. Our reasoning behind doing this is that when a real AP will be brought down by an attacker, it will be as good as switching the AP off. We calculated the number of seconds a typical Windows Vista machine takes to realize that the AP is down. This is when it will typically try to (automatically) reconnect to some different access point. This is significant because when attacker brings the real AP down, the clients will not connect (automatically) to the rogue AP till 24.628 seconds have passed on average.

We observed an important phenomenon here. During our experiment, the AP was switched off, a rogue AP was set up that sent just the beacon frames and probe response frames to clients. We noticed that in this case the client never realized that it has lost the connection with the real AP. Thus we concluded that the test of whether an AP is alive is completely based on presence of beacon frames and not on the actual data being exchanged.

The second row of table 2 shows the amount of time a client machine takes to realize that the AP is back up again. Once the AP recovers from the attack, client will take this much time to connect (automatically) to real AP.

Table 2 gives us the performance of our solution. For this experiment we had setup the IDS so that it detects a gap of two between the sequence numbers as an inconsistency (In practice this gap can frequently occur due to packet loss in the pcap library). It then raised an alert and sent the challenge request and received challenge response.

As can be seen from the table, in normal scenario, the IDS is able to verify the authenticity of an AP in 0.1 second after the inconsistency between sequence numbers is detected. Thus the response time seems fairly quick. In few rare cases however we observed that the response time was about 7.5 seconds.

The last column shows the difference between sequence numbers of the response frame and the frame where inconsistency was observed. Average value is 10. It is useful in following way. Consider that an attacker has brought down the AP when it was at sequence number 1000. The attacker then starts a rogue AP at sequence number 1001 and continues. The rogue AP comes up when the attacker is at
sequence number 1100. Now AP sends frame with sequence number 1001 and an inconsistency is detected. IDS now sends a challenge to both the attacker and the real AP. Real AP will respond to this challenge with a frame having sequence number 1011 (1001+10). Attacker will either not respond or will respond with a fake message with frame having sequence number of minimum 1101. Thus this field tells us that in order to successfully identify sequence number of rogue AP from that of the real AP, the difference between their sequence numbers has to be at least 10. (Note: According to [3] when a class 3 AP is flooded, it takes 12 seconds to respond to client authentication requests. Thus we expect to get a frame from the real AP again after 12 seconds. Thus attacker has to have incremented its sequence number by 10 during this 12 second period in order for our detection mechanism to work. As the last column of the table shows, the real AP incremented the sequence number by 7 each 0.1 seconds. So this assumption seems reasonable.)

Another important observation is that the packet capture library was observed to drop one frame per 140 frames it captured. This can be seen from the first column of the above table. Thus in practice we can not expect to see packets with consecutive sequence numbers consistently. We have to keep a tolerance of some value which should be computed statistically. The invasive challenge-response approach is considered active. It can alert the firewall at advanced router, and might drop the packet, before it reaches the challenge responder end. In such case, firewall should be configured to allow traffic flow to the IDS interfaces.

B. Possible attacks against IDS and proposed solutions:

1) Hidden Terminal Problem: Consider the situation depicted in figure 6. An attacker is able to sniff the packets sent by an AP but the wireless interface of the IDS can not. Attacker can execute man in the middle attack as follows. The Attacker claims to be a real access point. The IDS challenges it because it saw this AP for the first time (See future enhancements section). Attacker just forwards this challenge to a real AP and relays its response back to the IDS. Thus successfully fooling the IDS. If the SSID used by the attacker is different, then adding ssid to the challenge response message would help. For the other case, we are still in the process of finding a solution.

2) Loss of packets and noise: There can be possibility of loss of packets when challenge response is sent out. Further, it is possible that the response packet reaches the attacker, but IDS fails to capture it due to noise. In such case attacker can resend the intercepted packet after replacing the sequence number with its next sequence number. This could lead to failure of authentication of legitimate AP or MITM attack from the attacker. To reduce the frequency of this situation, challenge-response procedure can be repeated more than once. For every further retrieval, IDS should be able to validate the response from the AP successfully.

3) Beacon flood attacks: Attacker can send beacon frames with spoofed random legitimate looking source MAC, SSID and channel information and random sequence numbers. This will enforce the IDS to send challenge requests to every potential rogue AP and which can make the IDS busy, can result into denial of service for further rogue AP identification requests. There is no clear solution for such situation. However, presence of such large number of beacons could itself be a valid reason to raise an alert and notify the administrator.

C. Advantages over existing solutions

As mentioned in various white papers[6, 7, 8], existing solution providers claim to detect rogue access points. However, the techniques incorporated by most of the existing solutions could not be analyzed as we did not get chance to experiment with those. Considering the strategies followed by our solution, we see following advantages:

1) Less false positives: The proposed scheme uses two step mechanism to detect the rogue AP. The first step makes use of the sequence number analysis mechanism to detect the potential rogue AP and then uses the challenge response mechanism to confirm the rogue AP. With this design of the system, the number of false positives are expected to be significantly less. With our setup, no false positives were found. However, in rare situations it is possible that the access point or the wired interface of IDS may drop the challenge packet. In the current implementation, this has been taken care of by resending the challenge request. The probability of challenge packet getting dropped over multiple number of trials becomes less. Considering this, we perform the challenge request-response activity for multiple repetitions to reduce overall probability of getting false results.

2) no configuration changes to IDS or AP: In the proposed scheme, IDS does not require any configuration changes to the AP. Also, IDS does not require any extra logic implemented in the AP, as part of the IDS. The IDS machine is connected to the AP over the wired network and can be routed to AP over wired network itself. So any further addition of AP to the local wired network is possible. There is no need to change...
the configuration and execution environment of the IDS, to protect the newly added AP. Whenever a new legitimate AP is added to the network dynamically, it will be authenticated by IDS successfully, and will be tracked separately for further possible attacks on it.

VI. CONCLUSION

In this paper, we presented a technique to identify rogue APs using sequence number analysis and the challenge-response based authentication approach. It provides a solution which does not require any configuration changes in the AP.

VII. FUTURE WORK AND ENHANCEMENTS

The challenge-response mechanism can be enhanced to support the secure wireless network. The frames that are sent across and received as challenge request and challenge response will need to follow the security settings of the network like WEP, WPA, WPA2, 802.11x etc. The frames need to be encrypted and decrypted as per the encryption type specified, and using the keys specified for the technique. Typically networks with large geographical area coverage like university network, will have multiple APs to provide wireless connectivity over the large area. These access points can have different or same essids and can be set on multiple channels. In such case, IDS is still connected to all the access points over wired LAN, and can be extended to protect each of these access points. The IDS can track these multiple essids separately and follow the same challenge-response based authentication approach to detect rogue APs. So whenever a new AP is discovered, it can be authenticated by sending the challenge request and verifying the response to it, if authenticated successfully it will be tracked separately. This approach can be applied to multiple APs with same essid as well in the similar way.

The proposed scheme can be extended to incorporate active intrusion prevention. The IDS can counter attack the rogue AP with de-auth floods. It can disconnect all the clients of the rogue AP by sending those de-auth frames. The reason code in these de-auth frames can be set appropriately to indicate the rogue AP intrusion in the network. Further, IDS can follow the ARP cache poisoning to disassociate the clients. Key that is used to encrypt the challenge request data and challenge response data can be renewed periodically. Since both challenge requester and responder process run on the same IDS machine, periodic distribution of new key is not difficult.

Currently, IDS uses the sequence number analysis technique to detect the potential rogue AP. It can be enhanced to track the fragment numbers as well. The analysis would require additional observations in various cases when rogue AP is found.

REFERENCES

1) Sequence Number-Based MAC Address Spoof Detection, Fanglu Guo and Tzi-cker Chiueh
2) Rogue Access Point Detection using Temporal Traffic Characteristics, Raheem Beyah, Shantanu Kangude, George Yu, Brian Strickland, and John Copeland
3) Phishing in the Wireless: Implementation and Analysis, Ivan Martinovic, Frank A. Zdarasky, Adam Bachorek, Christian Jung, and Jens B. Schmitt
6) Countering Rogues in Wireless Networks, Austin Godber and Partha Dasgupta