The Enhancement of Intrusion Detection System Design in WLAN based on Rogue Access Point

S V Athawale[1] N S Sale[2]
[1,2]Department of Computer Engineering
[1,2]All India Shri Shivaji Memorial Society's College of Engineering Pune, India

Abstract— This write-up presents an analysis of the field of Wireless Intrusion Detection system (IDS). Wireless LAN users feel they have been connected to the wireless LAN through good signal, but not know they have been monitored by the hackers. IDS can help network system quickly identify attacks, which extends the system administrator's security management capabilities (including security audits, monitoring, attack recognition and response), improves the integrity of the information security infrastructure. Wireless intrusion detection system not only can detect the attacker's behavior, but also can detect rogue WAPS, identify non-encrypted 802.11 standard data stream.

Key words: Wireless Networks, Intrusion Detection, Rogue AP, Dos (Denial of Service) Attacks

I. INTRODUCTION

The growth of wireless networking has confused the conventional limitations between trusted and un trusted networks. First, wireless technology provides a expedient way of connecting various computers to a network with radio waves. Unhappily, from a security aspect , they also mean that you may become a network radio source to introduce new security threats. The threats from WLAN are many , such as spying , denial service attacks , monitoring to attack , intermediary (MITM) attacks , intrusion from client to the client , Rogue AP , flooding to attack , and so on , in this paper the unauthorized access is researched . Above mention attacks are the largest security risk to the current WLAN, hackers placed in the WLAN the unauthorized AP or client provided unlimited visitation to the network, to obtain be critical data through dishonesty. Rogue AP (referring to those AP directly access to the wired network without authorization) is the largest security threat to the current WLAN, hackers placed in the WLAN the unauthorized AP or client provided unlimited visitation to the network, to obtain be critical data through deception. In wireless network, the clear border of defense does not exist and the attack may come from all potential places. So at any time any nodes such as access points or client stations may be the victims. Wireless LAN users feel them have been connected to the wireless LAN through good signals, but not know they have been monitored by the other hackers. With the popularity of the current wireless LAN which because the low-cost and easy to configure , many users also can set up wireless base stations in their own traditional local area network , and the backdoor program some followed users installed on the network also caused the unfavorable environment of opening to unauthorized users. In fact, a new, specifically for wireless networks, prevention system are forcing on wireless local area network (WLAN) attacks vendors to add new detection and prevention service in their WLAN intrusion detection system products but existing does not scale well.

II. INTRUSION DETECTION

Wireless networks really increase fanatically day by day can provide customers around the world greatly improved mobility, flexibility and productivity over WLAN.

Wireless Intrusion Detection System can help network system quickly identify attacks. The traditional intrusion detection systems can only detect and respond to the destruction of the system. Now first Intrusion Detection System (IDS) is to judge the damage system and intrusion events by analyzing the transferred data on the network.

Wireless intrusion detection system is similar to the traditional intrusion detection systems, but is appends some detections for wireless local area network and the characteristics for damage system response. Today, intrusion detection systems have been used in wireless local area network, to monitor and analyze user's activities, determine the type of the invasion, detect illegal network behavior, and give an alarm for abnormal network flux. The wireless intrusion detection systems popular in the market are air defense rogue watch and air defense guard. Other some wireless intrusion detection systems have also been supported by Linux system, such as Snort-Wireless and WIDZ of free software open source organizations.

A. Architecture

Wireless intrusion detection system has centralized and decentralized two forms.

- Centralized wireless intrusion detection systems are usually used to connect a Separate sensor, collect data and transmit it to the central system which is responsible for data storage and processing.
- Decentralized wireless intrusion detection system typically includes a variety of devices to complete DS processing and reporting capabilities, it is more suitable for smaller-scale wireless LANs, because it is cheap and easy to manage.

B. Physical Response

Wireless LAN users feel they have been connected to the wireless LAN through good signal, but not know they have been monitored by the hackers. With the popularity of the current wireless LAN which because the low-cost and easy to configure, many users also can set up wireless base stations in their own traditional local area network.

Because of that Physical location is an important part of the wireless intrusion detection system. To block illegal IP, the intrusion detection systems need to deploy to find the intruder IP, and the deployment must be timely. Different with the traditional LAN, in which hackers can attack a remote network, the intruders of the LAN are in the local. Through wireless intrusion detection system the physical address of the intruder can be estimated. And through the 802.11sensor data analysis the victims can be

identified, thus the address of the intruder will be more easily located.

C. Threat Detection

The detector which is distributed throughout the network has the ability of capture and analysis the data packet. Wireless intrusion detection system not only can detect the attacker's behavior, but also can detect rogue WAPS, identify non-encrypted 802.11 standard data stream. In order to better identify potential WAP (Wireless Application Protocol) targets, hackers often use scanning software, such as Nets tumbler and Kismet software use global satellite positioning system to record their location. These tools become popular just because the geographic support of many websites to the WAP. The detector which is distributed throughout the network has the ability of capture and analysis the data packet to find the AP (Access Point). For wireless networks, intrusion detection and denial of service (DoS) attacks are forcing wireless local area network (WLAN) vendors to add new detection and prevention service in their WLAN intrusion detection system. DoS attack, which is very common on the network. DoS attacks are caused by signal attenuation due to the building blocks. Hackers conduct DoS attacks on wireless LANs. Wireless intrusion detection system can detect such behaviors of the hackers, such as the forging legitimate users for flooding attacks.

D. Policy Execution

The popularity of the current wireless LAN which because the low-cost and easy to configure, many users also can set up wireless base stations in their own traditional local area network, and the backdoor program some followed users installed on the network also caused the unfavorable environment of opening to hackers.

- Wireless intrusion detection system can not only identify the invader, but also strengthen the policy. And the using of powerful strategy will make wireless LANs more secure.
- Physical location is an important part of the wireless intrusion detection system.

For example, to block illegal IP, the intrusion detection systems need to deploy to find the intruder IP, and the deployment must be timely. In addition to the above description, wireless intrusion detection system can also detect MAC address spoofing. It is to identify those wireless Internet users rogue WAP through a sequence analysis.

- Hackers are placed in network obtain data through rouging WAP and the who were using wireless LAN users think that they have been connected to wireless LAN, but do not know that they have been monitored by hackers.
- This is the causation that the organizations without configuring the intrusion detection system begin to think about the solution to configure IDS.
- Rogue AP (referring to those AP directly access to the wired network without authorization) is the largest security threat to the current WLAN, hackers placed in the WLAN the unauthorized AP or client provided unlimited visitation to the network, to obtain be critical data through deception.

III. ROGUE AP INTRUSION DETECTION STRATEGY AND RESULTS

Intrusion detection strategy and results which is achieved in WLAN based on Infrastructure are given in this paper by testing the counterfeit equipment detection technology (including AP and Client).

A. Rogue Device Detection

Rogue AP (referring to those AP directly access to the wired network without authorization) is the largest security threat to the current WLAN, hackers placed in the WLAN the unauthorized AP or client provided unlimited visitation to the network, to obtain be critical data through deception.

1) The AP's presence can be detected by listening to the packet of radio waves and these using AP, SSID and STA will also be got. These components should be placed in the network to achieve Rogue AP detection.
   - Detector Sensor / Probe, which is used to monitor wireless data timely; In order to avoid network conflicts, the wireless node scan send data in a certain time which determined in the frame. According to 802.11 formats, the time interval is designated in the frame head in order to keep the node channel.
   - Intrusion detection system IDS, which is used to collect the data came from detector and determine which is the rogue device; once the rogue device found we can secure wireless network from intrusion to hack data.
   - Network management software, which is used to communicate with the wired network, determines the switch port which meets the rogue device and disconnect the port.
2) The detector which is distributed throughout the network has the ability of capture and analysis the data packet to find the AP. They can quickly find all the wireless equipment operation and report to the administrator or DS system. This manner is called as RF scan. As some AP can find the neighbor regions ones, we only see the AP's adjacent ones. Certainly, the specific physical address of wireless network which was accessed by AP can be determined by the network management software, such as SNMP. Physical location is an important part of the wireless intrusion detection system. The AP's legality can be determined by using the legitimate AP list (ACL) after the AP found. If the new detected AP's relevant parameters were not found in the list, the Rogue AP will identify each AP's MAC address, SSID, Vendor (provider), wireless media types and channels. If they are abnormality, the AP will be considered as illegal one.

B. Rogue Client Detection

Once the rogue device detected the detector which is distributed throughout the network has the ability of capture and analysis the data packet to find the AP.

Rogue client is the wireless clients who attempt to illegally enter the WLAN or disrupting the normal wireless communication. If the administrator pays more attention to abnormal action, these fake clients can be identified easily. Main features of the abnormal action are: (1) send a long

duration frame; (2) duration attacks; (3) detect "any SSID" equipment; (4) non-certified customers.

- If the client sends a long duration of the frame, the other customers must wait a specified duration when they use the wireless media. In this case, other users cannot use the wireless medium and they must have been in the wait state. Network Allocation Vector (NAV) stores the time interval value and tracks each node. Other nodes can use the channel when the duration value is become to 0. That forced other nodes cannot use the channel in the duration. If the attacker successfully sends long duration packets continuously, other nodes should wait a long time and cannot receive services. It causes that other nodes meet the situation of denial service.
- In order to avoid network conflicts, the wireless nodes can send data in a certain time which determined in the frame. According to 802.11 formats, the time interval is designated in the frame head in order to keep the node channel.
- It will give attackers great convenience when the AP allows customers connect the network with any SSID manners. It may be the attacker when the customer connects the network with any SSID manners. So the AP setting should be changed to prohibit connection with any SSID manners. It can use the client MAC addresses and equipment supplier's logo to judge the fake clients when they are in the legitimate client authentication list. It the MAC address of NIC or the Vendor ID is not in the access control list, it may be an illegal customer.

C. Wireless Network Attack Defense

The AP's legality can be determined by using the legitimate AP list (ACL) after the AP found. When the fake AP has been identified, it should be immediately taken measure to block the AP's connection. The ways to block the AP's connect are shown as follow:

1) Using DoS attack methods, which can force wireless services unavailable for all customers; DoS attacks are caused by signal attenuation due to the building blocks.
2) Network administrators using the network management software determine the illegal AP's physical connection location and cut the connection in physical; Physical location is an important part of the wireless intrusion detection system.
3) Detecting the switch port which illegal AP connection used and prohibiting the port. This task can be achieved by using the wireless network management software. When the fake AP has been identified, the management software can find the AP's MAC address and find the switch port which was connected by AP. It will disconnect or block all traffics which were sent from this port. It can automatically stop the client to connect to the fake AP and connect to other adjacent AP. It is one of the most ways to solve this problem.

For Rogue client is the wireless clients who attempt to illegally enter the WLAN or disrupting the normal wireless communication. The Rogue clients, when it identified as illegal one, the network administrator can disconnect their network connection. The common method to solve this problem is that removing the illegal customer's MAC address from the AP's access control list (ACL). ACL can determine that which MAC addresses can connect with the network and which one cannot do.

D. IDS Application

The traditional intrusion detection systems can only detect and respond to the destruction of the system. Today, intrusion detection systems have been used in wireless local area network, to monitor and analyze user's activities, determine the type of the invasion, detect illegal network behavior, and give an alarm for abnormal network flux. Intrusion Detection System (IDS) is to judge the damage system and intrusion events by analyzing the transferred data on the network.

Intrusion detection using this technology can do the respond for unauthorized connection attempting and even against some possible invasions. Intrusion detection system can be divided into four components by the IETF ID-WG. These components are including of event generator, event analyzer, response unit, and event database. IDS basic frame in the traditional cable network is shown as figure 1.

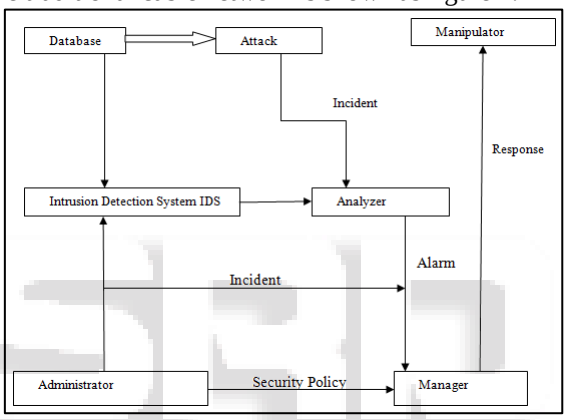

Fig. 1: IDS basic frame in traditional cable network

Above shown IDS Intrusion detection system basic frame in traditional cable network. When the detector placed in the network detected anomalies, it will result in an incident to report to the analyzer, resulting in alarm information by analyzing and report to the manager. The administrator will decide how to operate and respond to the incident. We use the IDS technology in traditional network for wireless networks to improve the capacity of wireless networks against attacks.

The detection system is a network-based intrusion detection system (NIDS), as shown in figure 2.

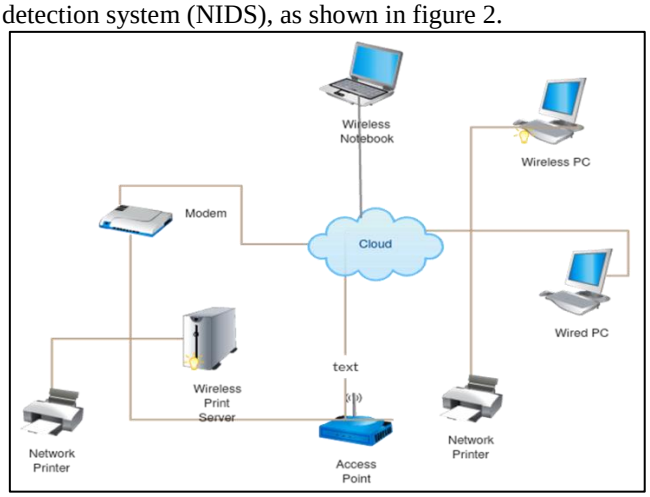

Fig. 2: The detection system framework

The center console of network administrators is to configure the detecting agent and browse the detecting results, and conduct association analysis. The monitoring agent is to monitor the data packets, use detecting engines for testing, record warning messages and send them to the center console. Probe is to capture the wireless data packet and send to the monitoring agent.

IV. TESTING RESULTS

We use free software open source organization IDS systems WIDZ to conduct intrusion detection, use non-authorized users to conduct attacks (rogue MAC address), the detection alarm message recorded as follows:

- Alert NON white list Mac essid Wireless_packet_type Beacon macl fffffffffff
- mac2 0030ablb9bcc mac3 0030ablb9bcc mac4 000000000000
- Alert NON white list mac essid Wireless}acket_type Probe Request macl
- fffffffffff mac2 00904b063d74 mac3 fffffffffff mac4 000000000000
- Alert NON white list mac essid Wireless_packet_type Probe Response macl
- 00904b063d74 mac2 0030ablb9bcc mac3 0030ablb9bcc mac4 000000000000

The AP's legality can be determined by using the legitimate AP list (ACL) after the AP found. If the new detected AP's relevant parameters were not found in the list, the Rogue AP will identify each AP's MAC address, SSID, Vendor (provider), wireless media types and channels. If they are abnormality, the AP will be considered as illegal one. It is obvious that the identified MAC address of the legitimate device which is not listed in the ACL table may be counterfeit equipment. The next thing is to find the device and disconnect it.

V. CONCLUSION

Wireless Intrusion detection systems (WIDS) are vital to WLAN security. In this paper, we first analyze the threats to wireless LANs, then introduce an overview of intrusion detection system in WLANs. To detect and response these wireless attacks, we design the detection system framework and specific intrusion detection systems and control solution system. It imports the network, expands the detection rules based on device information and uses policy based recognition to identify the real intention of the attacker. In future work we are interested in more advanced forms of a single technology cannot solve the security problem, so we must combine a variety of measures and technologies to establish multi-level security architecture.

REFERENCES

[1] IEEE Std 802. 11-1999:Wireless LAN Medium Access Control. (MAC) and Physi.ca.l Layer (PI-IY) Specifications[S].USA:I EEE, 1999
[2] Stubblefield, A., J. Ioannidis, and A. D. Rubin. Using the fluhrer, Mantin, and Shamir attack to break WEP. In Network and Distributed System Security Symposium (NDSS), 2002, 1250: 373-389
[3] Bernard Aboba, Tim. Moore, John Roese. IEEE 802. lx For Wireless LANs IEEE 802. 11-00/035, 2001, 22D:187-204.
[4] Walker, JUnsafe at any key size; an analysis of the WEP encapsulation. IEEE 802.11-00/362, 2000
[5] Tim Moore. Suggested Changes to Robust Security Network (RSN) for IEEE 802.11IEEE 802. 11-02/298r4.2002:343-354

