Defense against 802.11 Deauthentication and Disassociation Attacks

T6542

DATA ENTERED

Developed by:

Rehab Zafar
348-FBAS/MSCS/FO7

Supervised by:

Dr.Muhammad Sher
Muneera Bano

Department of Computer Science
Faculty of Basic and Applied Sciences
International Islamic University Islamabad
(2009)

MA/MSc
004. 67
RED

DATA ENTERED

1- Computer networks – management

2. Application software – Development

Department of Computer Science

International Islamic University Islamabad

Date: 2nd January 2010

Final Approval

This is to certify that we have read the thesis submitted by **Rehab Zafar,348-FBAS/MSCS/F07.**It is our judgment that this thesis is of sufficient standard to warrant its acceptance by International Islamic University, Islamabad for the degree of **Master of Science in Computer Science.**

Committee:

External Examiner:

Prof.Dr. Mahboob Yasin
Chairman
Department of Computer Science
Comsats Institute of Information Technology
Islamabad

Internal Examiner:

Mr.Mata-ur- Rehman
Assistant Professor
Department of Computer Science
Faculty of Basic and Applied Sciences
International Islamic University Islamabad

Supervisor:

Prof.Dr. Muhammad Sher
Chairman
Department of Computer Science
Faculty of Basic and Applied Sciences
International Islamic University Islamabad

Ms.Muneera Bano
Assistant Professor
Department of Computer Science
Faculty of Basic and Applied Sciences
International Islamic University Islamabad

بسم الله الرحمن الرحيم

Allah's Name I Begin With, the Most Compassionate, the Most Merciful

Dedication

Dedicated to **The Holy Prophet Muhammad** (Allah's grace and peace be upon him) Lord of the world and the hereafter. I offer my humblest thanks to Him, who made us aware of our creator and guided us to the right track, which leads to the success, who is a symbol of love and affection for all the creatures of Allah.

1

A dissertation Submitted To
Department of Computer Science,
Faculty of Basic and Applied Sciences,
International Islamic University, Islamabad
As a Partial Fulfillment of the Requirement for the Award of the
Degree of *Master of Science in Computer Science.*

Declaration

We hereby declare that this Thesis ***"Defense against 802.11 Deauthentication and Disassociation attacks"*** neither as a whole nor as a part has been copied out from any source. It is further declared that we have done this research with the accompanied report entirely on the basis of our personal efforts, under the proficient guidance of our teachers especially our supervisors Dr. Muhammad Sher and Muneera Bano. If any part of the system is proved to be copied out from any source or found to be reproduction of any project from any of the training institute or educational institutions, we shall stand by the consequences.

Rehab Zafar
348-FBAS/MSCS/F07

Acknowledgement

First of all we pay our humble thanks to **Almighty Allah** who knows all the things hidden or evident in this universe, even the things which pass through our hearts, who created us and gave us the courage to complete this project. It is said in the Holly Quran:

"Read! In the Name of your Lord, Who has created (all that exists), Has created man from a clot (a piece of thick coagulated blood), Read! And your Lord is the Most Generous, Who has taught (the writing) by the pen, Has taught man that which he knew not, Nay! Verily, man does transgress all bounds (in disbelief and evil deed, etc.), Because he considers himself self-sufficient, Surely! Unto your Lord is the return." [Surah al Alaq]

Without His help and blessings, I was unable to complete the project.

I also offer my humblest thanks to **The Holy Prophet Muhammad** (Allah's grace and peace be upon him), who made us aware of our creator and guided us to the track, which leads to the success, who is a symbol of love and affection for all the creatures of Allah.

I also express my cordial and humble thanks to all my friends especially Sadia Noreen and teachers for their untiring help and cooperation in completing this project especially Farrukh Shehzad Project Manager "NexGINRC" FAST-NU.

I cordially regard the inspiration, prays, encouragement and financial support of our loving and affectionate parents and family for their motivation in every aspect of our study enabling us to complete this project.

Rehab Zafar

348-FBAS/MSCS/F07

Project In Brief

Project Title:	Defense against 802.11 Deauthentication and Disassociation attacks
Undertaken By:	Rehab Zafar 348-FBAS/MSCS/F07
Supervised By:	Dr.Muhammad Sher Ms.Muneera Bano
Start Date:	27-10-09
Completion Date:	16-11-09
Tools & Technologies	C# Wireshark Aircrack-ng MDK3
Documentation Tools	Ms Office
Operating System:	Windows 2008 Linux BackTrack
System Used:	Pentium IV

Abstract

Wireless networks are becoming more common now-a-days and they are also more easy to be attacked. We have presented a BIO inspired technique to cater DOS attacks i.e. Deauthentication and Disassociation attacks. Artificial immune system mimics the natural immune system's characteristics of memory and learning to solve real world problems. Many sequence number based technique has been proposed to detect DOS attacks. But those techniques were not dealing with the lossy channels. We have used beacon frames for training instead of data packets. So we would be able to train our AIS before any data transfer get start. Results are almost better than the previous, and results will not deteriorate in lossy environment as this technique equally deals with both kinds of channels.

List of Figures

Fig 1.1 Wireless Infrastructure..2

Fig 1.2 IEEE 802.11 MAC Format...3

Fig 1.3 Basic IDS Structure..6

Fig 2.1 MMDS Security Agent Architecture.....................................16

Fig 3.1 WEP Encryption..22

Fig 4.1 Structure of an Antigen..30

Fig 4.2 Structure of an Antibody...30

Fig 5.1 Experimental Setup..33

Fig 5.2 D-Link Configuration Page...34

Fig 5.3 True Positives Rates...37

Fig 5.4 False positives Rates..38

Fig 5.5 True Negative Rates...39

Fig 5.6 False Negative Rates...40

Fig 5.7 Performance..42

Fig 5.8 Accuracy...43

List of Tables

Table 2.1. Comparison of different MAC adress Spoofing Detection Techniques...........18

Table of Contents

Chapter 1 1
1.1 Motivations and Challenges 1
1.2 Background 1
1.2.1 802.11 Wireless Networks 1
1.2.2 IEEE 802.11 2
1.2.3 Frame Format of Deauthentication and Disassociation Frames: 5
1.2.4 Intrusion Detection System 5
1.2.5 Efficiency of IDS 8
1.3 Research Domain/Problem Domain 9
1.3.1 Problem in Deauthentication and Disassociation Attack 9
1.4 Proposed Approach 10
1.4.1 Artificial Immune System: 10
Chapter 2 12
Literature Review 12
Chapter 3 21
Requirement Analysis 21
3.1 WEP setup 21
3.1.1 Problems 21
3.1.2 Passive Attack to Decrypt Traffic 23
3.1.3 Active Attack 23
3.1.4 Active Attack from Both Ends 23
3.1.5 Table-based Attack 24
3.2 WPA 24
3.2.1 WPA Problems 25
3.2.1.1 Cracking the Pre-shared password 25
3.2.1.2 MIC Denial of Service Attack 25
3.3 Problem Scenarios 25
3.3.1 802.11Authentication 25
3.3.2 802.11Association 26
Chapter 4 27
4.1 Introduction 27
4.2 Design Requirements 27
4.3 Methodology / Framework 28

4.3.1 Training Phase: 28
4.3.2 Detection Phase: 29
4.3.3 Structure of an Antigen: 30
4.3.4 Structure of an Antibody: 30
4.4 Deployment/Environment 30
Chapter 5....32
Results 32
5.2 Attack Scenario....34
5.3 Dataset Collection....35
5.4 Performance Metrics....35
Chapter 6....45
6.2 Achievements 45
6.3 Improvements 45
6.4 Future Recommendations....45
References: 46

Chapter 1
Introduction

Chapter 1

In this chapter we are discussing the motivations and challenges we faced in doing this thesis and also we are giving a brief overview of the important terms and technologies we came across during this thesis. In section 1.3 we are discussing the problem domain and in section 1.4 we are discussing a brief overview of the proposed solution.

1.1 Motivations and Challenges

Wireless 802.11 b is the most common wireless network architecture being used nowadays. It lacks behind only due to security issues. It is the cheapest set up of Wireless mostly used throughout the world and especially in the third world countries. If an organization or a company wants to change to another brand of wireless due to security issues than it has to change all its setup including hardware and all. Thus if we become able to tackle its security issues without having change in its hardware than it will be more beneficial and a cheap solution to the wireless customers. A simulation work has been done on this topic so in this thesis it was decided to make it implemented. An actual implementation and Simulation are very different from each other. In simulation we don't tackle many real time problems like packet capturing, packet injection etc. While implementing a project actually makes us know what will be its actual results while deploying it in a real environment.

1.2 Background

1.2.1 802.11 Wireless Networks

Wireless technologies are becoming increasingly popular in our everyday life and business. Many organizations are deploying Wireless technology for different purposes. Some are deploying to access calendars, internet etc and some are deploying it to locate the location of any wireless device in the world. So organizations and people should be aware of the security risks associated with it. As technology will change and improve so will be the security risks will increase and new risks will be faced. So organizations should keep itself up to date with the technological developments.

Wireless networks are divided into three groups on the basis of its coverage range:

- Wireless Wide Area Network
- Wireless Wide Personal Area Network
- Wireless Local Area Network

2G cellular, Cellular Digital Packet Data (CDPD), and Global System for Mobile Communications (GSM) are the etchnologies which comes in WWAN.In WLAN 802.11, HiperLAN etc are included and in WPAN Bluetooth and IR are included.

WLAN provides more flexibility than the wired LAN. More computers can communicate with one another or to the internet if it comes within the range of a Cell. Cell is the coverage area of a WLAN. Access Point is the managing device within a WLAN which covers a range of almost 300 feet. Client can freely move within this range.[21]

Wireless Networks are divided into two types:

- Ad-hoc Network
- Infrastructure Network

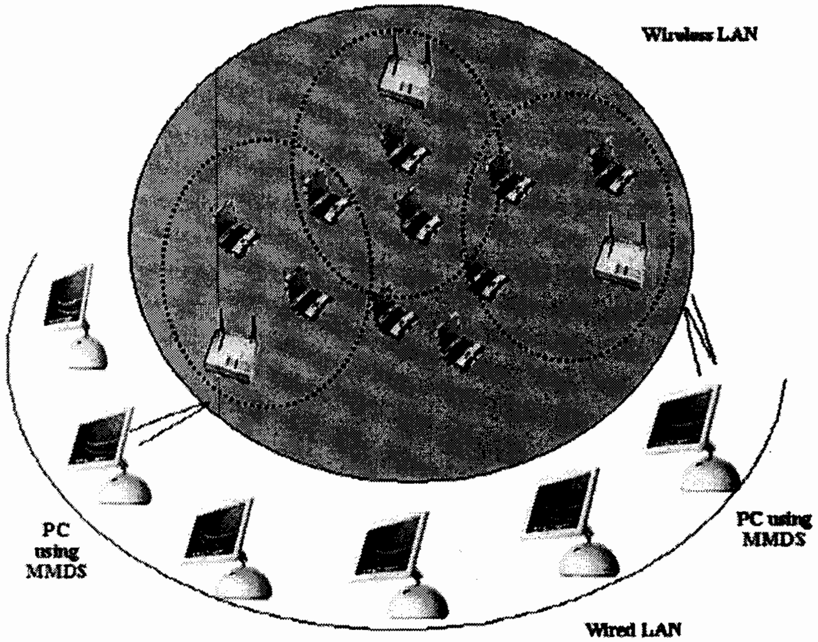


Fig 1.1: Wireless Infrastructure Network Structure [23]

1.2.2 IEEE 802.11

IEEE 802.11 is a set of standards for wireless local area network (WLAN) working in different frequency bands like 2.4, 3.6 and 5 GHz. They are implemented by the IEEE LAN/MAN Standards Committee. 802.11a works in 5 GHz band with a data rate of 54 Mbit/sec. 802.11b works in 2.4 GHz band with a data rate of 11 Mbit/sec. 802.11g is backward compatible with 802.11b and works in 2.4 GHz band with a data rate of 54Mbit/sec. 802.11n works in both 2.4 and 5GHz band with a data rate of 144 Mbit/sec.

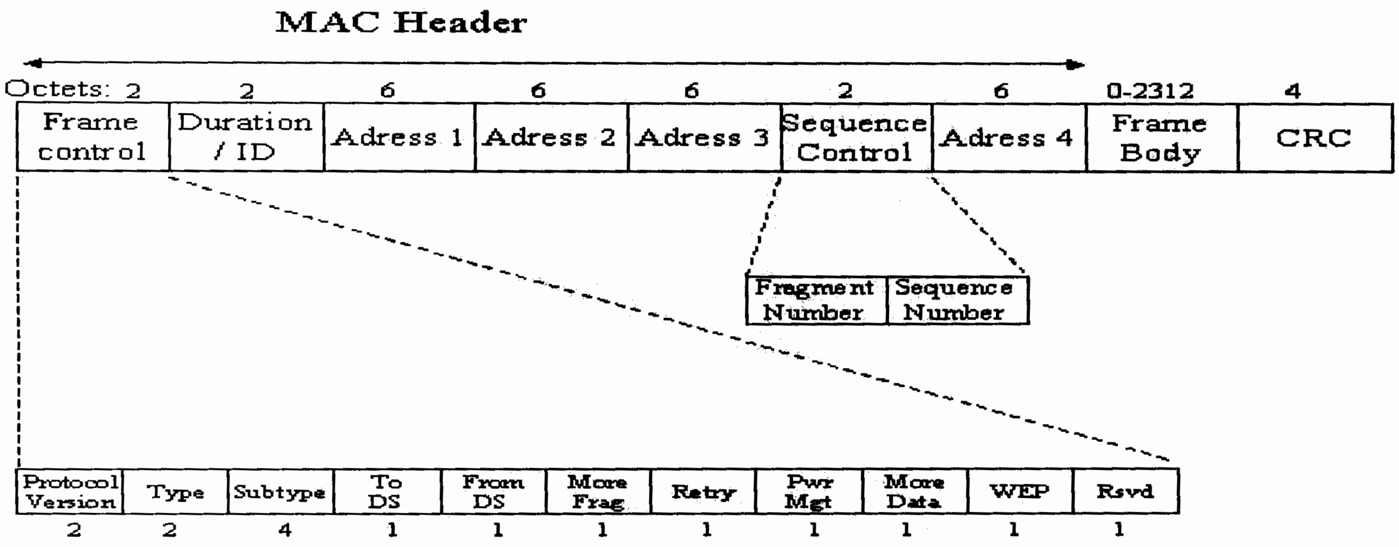


Fig 1.2: IEEE 802.11 MAC Format [22]

Frame Control:

It includes all these fields.

Protocol Version:

This field is normally set to zero which is of 2 bits. It has been kept to accommodate future versions.

Type and SubType:

This is a 6 bit fied.2 bits for Type and 4 bits for SubType.

- 00 in Type is for Management Frame.
- 01 in Type is for Control Frame.
- 10 in Type is for Data Frame.
- 11 in Type is for Reserved Frame.

To DS

This one bit field is set to 1 when the frame is addressed to AP for forwarding to the Distributed System otherwise it is set to zero.

From DS

This one bit field is set to one when the frame is coming from the Distributed System.

More Fragments

When there are more fragments related to one frame to be sent than this bit is set to one.

Retry

When retransmission of a frame is done than this bit is set to one.

Power Management

This bit is used by the stations to indicate when to go to the power save mode from normal active state and vice versa.

More Data

This bit is used to indicate to the power mode station that more frames are buffered for it. The stations decide that whether it wants to change itself to the active mode or wants to remain in the power mode.

WEP

This bit shows encryption with WEP.

Reserved

This bit field indicates that the frame is sent by the users that cannot accept change of ordering in unicast and multicast frames.

Duration/ID:

In Power save mode this is the station ID otherwise it is the duration value for NAV calculation.

Address 1:

It is the source which is sending the frame. If ToDS is set than it's the AP address.

Address 2:

It is the destination address to which the frame is addressed. If FromDS is set than it's the AP address.

Address 3:

It consists of the missing or remaining address. The field contains Sender address if From DS is set and contains Destination address if To DS is set.

Address 4:

It is used in when one AP communicates with another AP and wants to sends frames for distribution.

Sequence Control:

It contains two other fields Fragment no and Sequence no. Fragment no tells that the how many fragments belong to the same frame and Sequence no tells that in which sequence frames are received.

Frame Body:

It contains the data.

CRC:
It is a 32 bit field containing 32 bit cyclic redundancy check for security and integrity of data.

Kinds of Frames:

There are 3 kinds of 802.11 frames:

1) Management Frames
2) Control Frames
3) Data Frames

Beacon frames, Association Request and Response, Deauthenticate, Disassociate, Reassociation request, Reassociation response, Probe request and Response all are included in Management frames whereas Control frames include RTS and CTS frames etc used for controlling.

1.2.3 Frame Format of Deauthentication and Disassociation Frames:

Deauthentication frame

1) type = 0x00 (Management), subtype = 1100
2) It de-authenticates the authenticated clients
3) By sending spoofed DEAUTH frame with BSSID of the AP valid users of the network could be de-authenticated.

Disassociation frame

1) type = 0x00 (Management), subtype = 1010
2) It disassociates the associated clients

1.2.4 Intrusion Detection System

This section gives us a brief overview of IDS .For detail discussion of IDS the readers should consult [15].IDS are system software's designed to recognize attacks against a computer or an information system and to prevent such attacks from destructions. Intrusion detection systems check the usage of systems to detect any appearance of insecure states either by the legal users or any intruders. It is difficult to ensure that a network system could be without any flaws and the security implemented over it could be without any holes. Thus the need of IDS is important for a secure and robust Computer Network system.

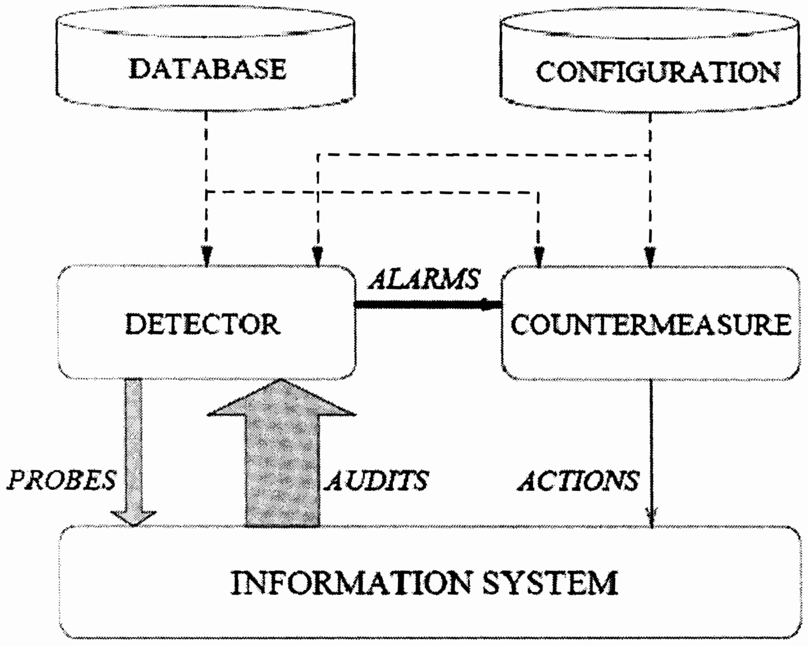


Fig 1.3: Basic IDS Structure [19]

This is a basic structure of IDS taken from [19].IDS basically act as a detector which protects the information being exchanged between the systems. This design contains a database which contains the information related to attacks and the configuration contains information related to the states of the system .Countermeasure contains the actions which will be performed against any attack at a specific state of the system. Probe Requests are given to the Information system to initiate the audit process which describes the events taken place on the information system.

Intrusion Detection System is a system used to monitor and check the whole network to insure the confidentiality and integrity of the network. They are a need of now a days Security infrastructure. They are the burglar alarms of the of the Security field [15]. Whenever an intrusion or an attack takes place it just informs like a burglar alarm and the appropriate step has to be taken. The real aim is just to avoid or tackle with these intrusions and attacks which attempt to break through the security of the network and to take appropriate actions. Intrusions are of different kinds it can be an intruder outside of the network who wants to steal the passwords and sneak into the network to steal valuable information or it can be a valid user who is exploiting the rules. It can also seem to be a valid user but may be not. Thus Mac address spoofing etc can also be done.

According to security incidents that occur on a network, the vast majority comes from inside the networks that are authorized but dissatisfied employees. Others come from the outside trying to enter the network. Intrusion Detection systems are the softwares that can be used to detect and respond to intrusions on time.

Intrusion detection system is an important part of an information security system which is a complement to network firewalls. [16] IDS tools always do a complete watch of networks. Mainly large organizations have installed some sort of intrusion detection tool. IDS is mainly needed in online-retail and e-commerce due to the attacks seen on E-Bay and Amazon [18]. Thus due to the increasing incidences of security, any entity on the Internet is not save from security point of view.

Thus should have an IDS installed. Intrusions can be provoked by financial, political, military, or personal reasons, so no organization should feel protected. Therefore if you have a network, you are a probable target. We can divide the IDS into two categories:

Anomaly Detection

It is a type of technique in which we wait to see some abnormal behavior in the traffic on the network. In this technique we have to decide that which kind of activity will be marked as an abnormality and which is normal traffic behavior. Whenever an abnormal behavior is identified a flag will be raised.

Misuse Detection

It is a type of technique in which a pattern is identified. On the basis of which different attacks are identified and a slight variation in the attacks could also be identified. They are useful for known attacks only.

Unknown attacks or new attacks could not be identified because no pattern will be available for it in the database.

Types of IDS

There are different types of IDS:

Network IDS

This type of ids is based on the analysis of the traffic between the hosts. They are also called Packet sniffers. They capture packets and compare them with a known database to determine anomaly and misuse detection.

Host based IDS

This is the type of IDS based on the detection of malicious behavior on the host only. It checks and monitors the attacks on a given host. Thus the difference between the Network and the Host IDS is that the NIDS checks the traffic between the hosts and the HIDS checks the host only.

Hybrid Intrusion Detection

It is the type of IDS which contains the qualities of both network IDS and the Host IDS. It analyzes both the traffic between the hosts and also checks for some malicious activity on the host.

1.2.5 Efficiency of IDS

Efficiency of IDS is checked through accuracy, performance, completeness, fault tolerance and completeness.

Accuracy: Accuracy is the correct decision of attacks and intrusions.

Performance: It is the speed with which events are processed. The real-time detection of intrusions is not possible if performance is not good.

Completeness: Completeness means to detect all attacks. It is not possible to have a complete knowledge about all attacks and intrusions.

Fault tolerance: IDS should itself be tolerant to attacks as it should be designed like this by keeping this quality in mind.

Timeliness: To enable the security officer to take timely decisions before the extreme damage can happen. IDS has to take timely analysis actions to inform officer as quickly as possible. And also to stop the intrusions from weakening the audit process timely actions has to be taken.

In this thesis many technological problems were faced. First of all the last work was a simulation thus it was unknown that which real time problems we can face. Dump files were collected of the real time environment. Problems were faced during dumping as there are several tools present for dumping but they didn't give us the Datalink layer packets .Wireshark and CommView were used to collect dump files but they didn't give us the Datalink layer packets. Sequence numbers were needed which were not given by these tools in Windows. Than Kismet tool was used for dumping traffic. It gave us Data link layer packets and the Sequence number field we needed to extract.

1.3 Research Domain/Problem Domain

Denying the legal users from a particular service is called denial of service attack. It is basically the prevention of transmission of data to and fro from stations. E.g. deauthentication attack,power saving attack etc

1.3.1 Problem in Deauthentication and Disassociation Attack

Frames of deauthentication and disassociation sent without encrypted them can result in spoofing attack. Thus the genuine users can be stopped to use the services it deserves. Therefore DOS is achieved [25]. Thus the attacker is making the user to re-authenticate and re-associate again and again.

In 802.11 the management and control frames do not have any technique or way to identify or check the identity of any frames that whether they are from a valid MAC address or not. Attackers can exploit this weakness in security.

An 802.11 client has to authenticate itself to the AP for communication purpose which is done through an Authentication message and when it has decided to discontinue it is done through a deauthentication message. The deauthentication messages and the disassociation messages are not encrypted with a keying material. An attacker can use the MAC address of both the AP and the client to send spoofed de-authentication and disassociation messages. The client will be unable to communicate further and will not receive frames destined for it.

This creates holes in the security. The Disassociation attack is same as the Deauthentication attack but is not as hard as the Deauthentication attack which makes the user to do more work to return to the authenticated and associated state. Thus Denial of Service is maintained in both cases with Deauthentication requiring more effort for recovery than the disassociation.

If an attacker launches a malicious de-authentication message than the non linear variation in the Sequence number between the data frames can detect the attack. A threshold is set, if the change in the sequence number is more than that threshold it is detected that there is an intruder. But if the abrupt change in the Sequence number is due to the Loss in the channel than the threshold fails in this condition. If we consider the abrupt change due to attack and if it is due to Loss in the channel than it will lead us to serious problems. A lot of experiments and work has been done for normal communication channel .But has not been done in the sense of Loss in the channel. Thus a defense mechanism for Loss in the channel is required and which is tried to be tackled in this thesis.

1.4 Proposed Approach

1.4.1 Artificial Immune System:

A new intellectual procedure or technique influenced by immunology has emerged called as Artificial Immune System. This technique has been applied in many fields like engineering and computer science to find the solution to many problems. It is a new evolving field which yet does not give a fixed algorithm template to solve problems and the actual implementations may change from time to time. [20]

It has been inspired from Biological Immune System which contains the properties of robustness and adaptability which tackle with the unknown pathogens like viruses, bacteria etc without knowing its overall structure. Immune system is divided into two categories.

Innate immunity:

is present from before birth and is static which destroys certain foreign particles. It comes from the mother. It can operate against almost any substance.

Acquired immunity:

This is a kind of immunity found in vertebrates. This immunity when comes across a new substance triggers the immunity and develops a response for it and keeps that immunity in the body for a long period of time. The Acquired immune system include following characteristics:

- **Recognition of Foreignness**: In order to locate and destroy the foreign materials like bacteria and viruses etc the immune system must be able to recognize them
- **Specificity**: For different foreign materials resistance to them will be different although two materials are slightly different.

- **Memory**: The immune system should remember how to tackle with the foreign material when first time it was handled and should have a long lasting effect.

Thus Computer science field got influenced from this immunity concept and they are trying to handle most of their problems through it.

This thesis deals with the real time dealing of deauthentication and disassociation attack. A threshold is set by the difference in the sequence numbers of the beacon frames which is the heart beat of the channels. AIS have been used to tackle with the problem. It consists of two phases. Learning phase and Detection phase. In learning phase threshold is set and in detection phase attack is detected.

Chapter 2
Literature Review

Chapter 2

In this chapter we have given the literature we studied while doing this thesis.

Literature Review

In [3] the author has given an experimental analysis of 802.11 attacks and its remedy by giving low over head changes in the implementation.802.11 network is deployed more due to its confidentiality but this network is more vulnerable to Denial of service attacks like de-authentication, disassociation, power saving attack etc. It has given a heuristic idea to deal with the de-authentication attack by waiting for 10 seconds after receiving a de-authentication frame. To see whether data packets are received after the de-authentication request or not. If are not received than it's a legitimate de-authentication request, otherwise a legitimate user after de-authenticating cannot send data packets. It's a good approach but it consumes some time while performing some action.

In [1] the author identified the threats caused by denial-of-service (DOS) attacks against 802.11 MAC. The attacks which prevent legal users from accessing the network are a big problem. Their proposed defense against the de-authentication attack is straight forward. An access point, upon receiving a de-authentication request, places it on a wait queue for a certain period of time. If time expires and no other traffic from that node has been seen, the request is honored and the node de-authenticated. On the other hand, if traffic from that node is seen before time expires, the request is dropped and not honored.

In [6] [7] the author dealt with deauthentication attack in 802.11 using genetic programming approach. Fitness function and feature set were used. 100 percent detection rate was found and a similar approach was proposed for other denial of service attacks which were not in the training data.

In [2] an AIS based NIDS is proposed for preventing de-authentication and disassociation attacks. This AIS base model undergoes through a learning phase. In learning phase it develops a sense of self and non-self. It is assumed that in this phase only non malicious traffic will be in network. After that it enter it detection phase where it have two antibodies one for de-authentication attack and one for disassociation attack. Under attack condition an intruder spoofs the MAC address of AP and any station in network. Then intruder sends de-authentication and disassociation request on the behalf of the attacked node. AP de-authenticates and then disassociates the node. AIS model presented in this paper whenever finds the de-authentication or disassociation frame it calculates the difference in sequence numbers with the help of Euclidean distance formula. If difference is greater than a certain threshold then that frame is categorized as non-self otherwise self.

Author has done different experiments on different threshold and the best threshold for de-authentication attack is 4. And the best threshold for disassociation attack is 3. Results are very good as true positive rate is very high, which is almost 100%. And false positive rate is very low. Our work will basically continue this work and we will work for the Lossy channel.

Artificial Immune System (AIS) works just like Biological immune system (BIS) in vertebrates. As BIS protects the body from foreign antigens similarly we are designing an artificial immune system for De-Authentication and Disassociation.

As the Human Immune System (HIS) can defend against foreign antigens similarly computer scientists want to build a similar system for security. These systems would have the same qualities and properties as HIS [1].

The human immune system protects the human body similarly will be the artificial immune system [1] from foreign materials. It is hoped that the AIS could be able to deal with the dynamic nature of computer security which is lacked.

A number of artificial immune systems (AIS) [8] have been built for a wide range of applications including document classification, fraud detection, Data Mining, Pattern Recognition and Network and host-based intrusion detection. These AIS systems have proved to be better than the existing statistical and machine learning techniques.

A number of immune models [8] have been explored like Immune Network models, Negative selection and Clonal selection. Immune model is built on the concept of B-cells ant T-cells [1] [8] which are in human body. B-cells are built in the Bone marrow and the T-cells are made in the Thymus. B-cells secrets antibodies and T-cells kill antigens. Variety of B-cells and T-cells are made

from the Gene libraries. Maturing B-cells and T-cells pass through a negative selection process which means that the new B-cells and T-cells first pass through the bone marrow and the Thymus. If they attach to the self cells of the body then they are killed before releasing them into the body. When B-cells are attached to the antigens with high affinity greater than a specific threshold than they activate directly. If below a specific threshold than T-cells get attached to the antigen and send Chemical signals to B-cells due to which it activates, grows and differentiate. With or without the assistance of the T-cells the Colony is made of the activated B-cells that have the similar antigen binding properties. Similar properties are also required in the Intrusion Detection Systems (IDS) .We want a distributed, self-organizing and Light Weight IDS [1] like the HIS.
A cheap solution given in [3] is to collect the deauthentication messages in a queue for 5-10 seconds. If data packets are received after de-authentication message is received, that message is then discarded. But this approach led to a number of new vulnerabilities [3].

Another approach [2] used the fact that the Sequence numbers of the frames vary linearly in case of a normal activity.

In [10] security features of IDSs is discussed in detail more concerned with the managers and security officers decisions. It defines the IDS as a burglar alarm which notifies about an attack which disturbs the confidentiality and integrity of the system.IDS up to now are not mature yet.

Research is going on to make them as effective as possible. It described different types of IDS i.e. Signature based and anomaly based.

In [22] some techniques have been discussed about the Mac address spoofing used by the attackers to interrupt the network. As MAC changing is allowed by the vendors it is also used in the negative sense by the attackers. The attackers change their MAC and become a legitimate use to the AP. Thus causes unnoticeable damages to the network. MAC addresses have been used globally as a unique identifier and are maintained internationally by IEEE. The first 3 bytes are given to the hardware manufacturers called OUI (Organizational Unique Identifier) for unique identification. The IEEE maintains the list of MAC addresses prefixes and company information to which they are assigned. These lists are locally available to the public.

The author has proposed that these lists can be used to check whether the MAC addresses used by an attacker is included in the list or not as the attacker uses randomly generated MAC addresses .MAC addresses having prefixes not yet assigned by the IEEE can be marked as anomalous activity. The drawback of this technique is that since list of OUI is publicly available so it would fail if an attacker change the randomization procedure to select randomly first three bytes from the available list of OUI. The author has also suggested the close analysis of the sequence numbers with particular MAC addresses.

If we keep track of the sequence numbers used by a particular MAC address than we can find out the MAC address spoofing but it has a drawback that if the client went out of the Cell and came back with a different series of Sequence number than it will be difficult for us to find the MAC address Spoofing.

The 802.11 protocol stipulates that every participating device will monotonically increment the 12-bit sequence number field in the 802.11 header of every management and data frame however control frames do not get a sequence number. If a device is posing as another device, a naive attack will produce two distinct but interleaved streams of sequence numbers which can be detected easily if there is little loss.

One way a sophisticated attacker could cover his tracks would be to have the sequence number of his frame match that of a recent frame sent by the victim and flip the retransmit bit in the 802.11 header making the repeated sequence number appear like a natural retransmission. Another technique the sophisticated attacker might employ would include hijacking the entire sequence by sending out a frame with the next successive sequence number while corrupting the legitimate frame from the victim so that it gets dropped by any receiving node.

In [4] Fuzzy System Based Technique is used in which a multi-agent system called MMDS (Multilevel Monitoring and Detection System) is proposed. It provides a hierarchical security agent framework. In this framework a security node consists of four agents as shown in the Figure 3.

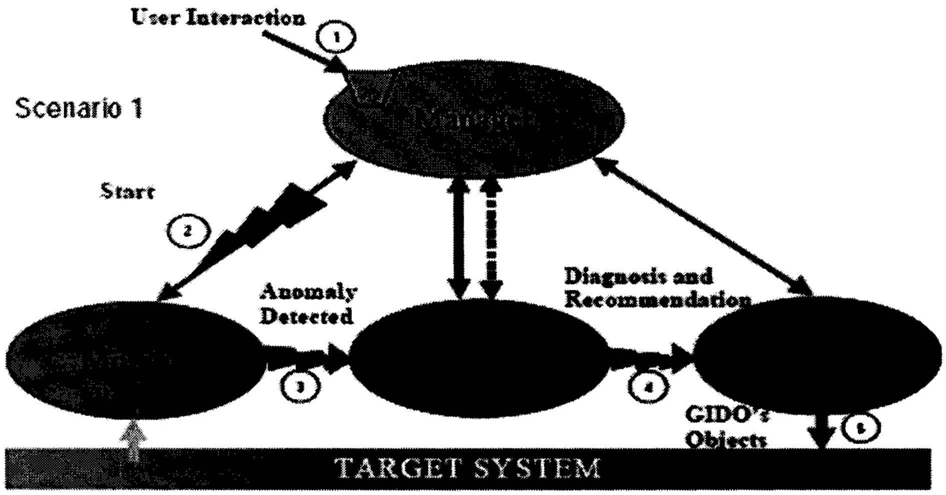


Fig 2.1: MMDS Security Agent Architecture [23].

Manager coordinates all the activities of the agents during sensing, communicating and generating responses. Monitor agent detects anomaly. Decision consists of fuzzy decision engine to take actions against anomaly. Action takes necessary actions on the basis of the decision made. Fuzzy decision engine is trained by using parameter-free genetic algorithm. It evolves fuzzy rules to classify training data correctly. It can take decision in real time due to its large decision objectives. Monitor checks fluctuation/patterns of sequence numbers to detect anomaly. The drawback of this technique is that it has not been tested for broader set of attacks.

Snort-wireless is an intrusion detection system that detects the spoof using a configurable preprocessor called MacSpoof. MacSpoof depends on the sequence number and it has a parameters called ”tolerate gap” which specify the gap limit between consecutive frames. MacSpoof checks if there are two consecutive frame with the sequence number greater than tolerate-gap limit then it says that gap has occurred.

Another configurable parameter is the ”threshold” which checks if the certain number of gaps have occurred i.e. greater than a certain threshold then MacSpoof will trigger an alert.

Finally we have a” expire time out”parameter that checks the time window within which a tolerate-gap has occurred. The challenge with this technique is setting the threshold. If the threshold is too low, there will be many false positives from natural loss, however, if it is too high this will result in missed detections And the weakness of this technique is that the gaps are not necessarily due to malicious activity. They could be natural as well [24].

In [24] MAC address spoofing is detected through Sequence Number Rate analysis and Signal Strength Fourier Analysis. The Sequence Number Rate Analysis (SNRA) technique calculates a transmission rate. If the set of sequence numbers and arrival times suggests a transmission rate that is greater than the proposed transmission limit, then SNRA concludes a spoof has occurred.

By using this method, gaps from natural frame loss do not cause false alarms because they will not yield an abnormally large transmission rate. The basis for the SNRA is simple. An estimated limit that how many frames can be sent in one second by an 802.11 device is calculated and it is 5314 frames. When the calculated frame transmission rate surpasses this theoretical transmission limit, the SNRA concludes that a spoof has occurred.

In [24] Signal strength is also used to detect MAC spoofing under the assumption that packets from two different devices will be received at two different power levels. Thus packets with same MAC address received at 2 different power levels will be considered as spoof. The weakness is that using Signal strength for spoof detection can be challenging due to unknown environmental effects on signals. Due to calibration drift in low-quality wireless networking cards because of signal strengths instability present significant challenges to detect wireless spoofs.

The Sequence Number based technique is discussed by [26]. This technique deals with normal sequence number advance, abnormal as well as duplicate sequence numbers. The author has used a Monitoring node for analysis purpose which is in Monitoring mode and captures all traffic in the air .An analysis based on sequence number distribution of frames coming from station as well as from AP has been performed. When the gap between the frames is greater than 3 it means that the monitor node has failed to capture the intermediate frames and it's an abnormal sequence number advance.

We cannot conclude that this difference is because of spoofing. So in this case the station will be put into the verification state where the monitoring station checks if the next sequence number is smaller than current sequence number but larger than last sequence number then it detects the frame carrying the current sequence number has been spoofed.The limitation of this technique is that the victim node should be in the same wireless network as the attacker node so that the latest value of the victim node's sequence number could be obtained. Spoof detection cannot be done by the algotithm if the nodes are in different networks because the verification check for the sequence number could not be done.

In [28] it has been discussed that in 802.11 wireless LANs MAC addresses can be easily spoofed. The received signal strength (RSS) is a value that is hard to make it fake and it is related to the transmitter's location. If attacker and the victim are at a specific distance than RSS value can be used to differentiate them to detect MAC spoofing.

The RSS pattern covered by 20 air monitors of 802.11 has been analyzed by the author. Due to antenna diversity a multiple Gaussian distribution is achieved. Signal strength can be used to increase the robustness of wireless communication. In this approach signal strength is calculated from different angles thus we have a Gaussian distribution. Therefore RSS profiles are made for spoofing detection. This technique is robust against antenna diversity and uses the three proposed algorithms based on local statistics combining local results from Air Monitors and global multi-Air Monitor detection. RF frequencies act as an identifier for the transceivers. The drawback of this approach is that it has assumed that the stations are stationary and there are not changing their place because if they move than their will de diversity in the RSS values received at different places in different angles. The challenge is to determine that the change in profile comes due to change in place or spoofing. And it is nearly impossible for an attacker to match the victims RSS profile as made by different Air monitors.

In [28] the author has used beacon frames to find the throughout, collision probability and performance of the wireless network 802.11g. Beacon frames are control frames used by the Access Point to continuously announce the network identity. This paper proposes a mathematical model to know the influence of the beacon frames on the network .The model is only tested through simulation and thus not tested in the Real environment. The results showed that beacon frames didn't have any effect on the network performance.

METHODS	ADVANTAGES	DISADVANTAGES
OUI BASED TECHNIQUE	Pre-fixing OUI makes Mac Addresses globally unique	OUI list is publicly available so any attacker can take that and prefix different OUI randomly with the Mac Address.
MMDS	Better accommodation of fluctuations in Sequence Number Changes	Has not been tested for broader sets of attacks, i.e., it is not tested for accommodation of sequence number changes due to lost frames, duplicated frames and out-of-order frames
Snort Wireless Mac Spoof	Simple: solely based on sequence number gap	Has not been tested for broader sets of attacks, i.e., it (i)Difficult to set the threshold (ii) High frame loss leads to generation of False positives (iii)Very new frames lead to missed detections (iv)Gaps can be natural not always due to malicious activity
Sequence Number Rate Analysis	Gaps from natural frame loss do not cause false alarms	Value of actual Transmission rate greater than theoretical transmission limit cannot always be due to spoofing

Sequence Number Based MAC Spoof Detection	Simple technique does not involves changes in Firmware	Victim node and Attacker node should be in the same Wireless network.
Heuristic For Spoof Detection	Simple heuristic is used	It is not used for Control frames Spoofing

Table 2.1: Comparison of Different MAC Spoofing Detection Techniques

Chapter 3
Requirement Analysis

Chapter 3

In this chapter we have discussed the factors due to which we have done this research. The MAC layer 802.11 has many flaws which have been discussed in this chapter. In section 3.3 problem scenario has been also discussed in detail.

Requirement Analysis

With the increasing popularity and usage of 802.11 security vulnerabilities has been identified at the MAC (Media Access Layer) layer. The techniques used for MAC layer security are not much secure. Thus security is the main issue in 802.11b especially. WEP(Wired Equivalent Privacy) is a classical framework deployed for Mac layer security and it uses WEP (Wired Equivalent Privacy) algorithms[4] .But open Source powerful tools are available that can break WEP. Other schemes like WPA (Wifi Protected Access) have also been used for security but they all did not provide full protection.

3.1 WEP setup

The IEEE 802.11 standard describes the communication mechanism in wireless local area networks. The Wired Equivalent Privacy (WEP) algorithm is used to protect the wireless communication from illegal and unauthorized Access. Its main aim was to provide confidentiality and protect from Eavesdropping. [9]

WEP relies on a secret key that is shared between an Access point and a mobile station. The secret key is used before transmission for the encryption of packets and an integrity check is applied to confirm that packets are not changed in the way. The standard does not describe in detail that how the shared key is established. A single key is distributed between all mobile stations and access points. Following are the problems and the technical details of the attacks related to the algorithm.

3.1.1 Problems

RC4 encryption algorithm is used by WEP. It is known as a stream cipher. A vast number of pseudo-random key streams are generated from a short key. The sender XORs the key stream with the plaintext to produce cipher text. The Recipient has a copy of the same key, and also generates an identical key stream. By XORing the ciphertext with the key stream gives us the original plaintext.

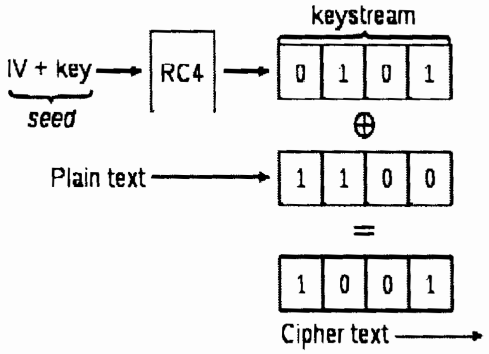


Fig 3.1: Basic WEP encryption [29]

Stream ciphers are not strong to several attacks. If a bit in the cipher text is changed by an attacker, then upon decryption, the corresponding bit in the plaintext will also be changed without having noticed. Eavesdropper can also intercept the cipher texts. If two cipher texts encrypted with the same key stream are intercepted, it is possible to obtain the XOR of the two plaintexts. Thus statistical attacks can be done to find the plain text. If more cipher texts use the same key streams than it becomes easy to find the key. When a plaintext is known than it becomes easy to recover all of the key streams.

WEP carved out the defenses against both of these attacks but were of no use. An integrity Check field id used to check wether the packet has been changed in the transit or not. An Initialization Vector (IV) is used which is added to the shared secret key and thus produces a different stream of keys for each packet. The IV is also included in the packet. The integrity check is put into practice as a CRC-32 checksum. CRC-32 linearality means that changing some bits in the encrypted packet and adjusting checksum similarly can produce the same packet as original or making the packet appear valid.

The initialization vector in WEP is a 24-bit field, which gives a small space of initialization vector due to which reuse of key stream happens. An access point which sends 1500 byte packets at 11Mbps, will exhaust the space of IVs after 1500*8/ (11*10^6)*2^24 = 18000 seconds. This time can become even smaller, since many packets are smaller than 1500 bytes. Thus two cipher texts that are encrypted with the same key stream can be found and perform statistical attacks with the help of which plaintext can be recovered. The key is easier to find when used same by all stations. If two common wireless cards are inserted at the same time than IV collision can take place in abundance.

3.1.2 Passive Attack to Decrypt Traffic

A passive eavesdropper quietly listens the traffic until an IV collision occurs. We can get the XOR of the two plaintext by XORing two encrypted packets encrypted with same IV. The contents of the message can be obtained by this value of XOR's.

IP traffic contains many repeatedness of the shared key or IV. This repeatness can be used to find out many of the contents of the messages and intelligent guesses and statistical analysis can be done to find the exact messages.

In a small amount of time, it is expected to find a sufficient number of messages encrypted with the same key stream.The plaintext for all other messages with same IV could be found if plaintext for one IV is found as all the pairwise XORs are known.

Another technique used by the attackers is that they use a host somewhere on the Internet to send traffic to any host on the wireless network. The attacker knows which messages it has sent. When the attacker intercepts the encrypted packets it comes to know which IV has been used. Thus many messages being encrypted by that IV can me decrypted easily.

3.1.3 Active Attack

A number of encrypted plain text messages could be generated by calculating the CRC-32 for each packet.A new packet can be built by calculating the CRC-32, and performing bit flips on the original encrypted message to change the plaintext to the new message. Without having the full knowledge of the message, it is possible to flip selected bits in a message and successfully adjust the encrypted CRC to obtain a correct encrypted version of a modified packet. Selective modification can be done if an attacker knows some information about the packet.

3.1.4 Active Attack from Both Ends

The attacker in this case does not have to know the contents of the packets or the IV it basically just have to know the information about the headers of the packet, e.g. if it knows the Destination address of the packet it can change the destination of the packet.And the attacker can send the packets to the machine it knows on the Internet. In infrastructure networks the Access Points are attached to the Internet. Thus the packets decrypted by the AP can be than send to the attacker known Computer on the Internet through different gateways and Routers. Destination Ports can be also be changed if we get to know the TCP headers. If port no's are changed to 80 than the packets can be passed through firewalls easily.

3.1.5 Table-based Attack

A decryption table can be made due to the small space of possible initialization Vectors When the plaintext for some packets is known than it can be used to calculate the RC4 key stream by IV. The key stream can be used to decrypt all other packets that use the same IV. With the pasage of time a table of IV's could be made.This table requires a small amount of storage of almost 15GB. The attacker can decrypt every packet that is sent over the wireless link by this table.

3.2 WPA

The WPA is a certification mark that indicates compliance with a security protocol designed to enhance the security of wireless networks created by the WiFi Alliance. There are two flavors of this protocol: Enterprise and Personal.

Enterprise is used with IEEE 802.11 X Authentication Server which distributes different keys to the clients for secure communication While Personal uses a Pre Shared Key which is distributed among all the computers. In this mode the security depends upon the secrecy of the key and strength. The WiFi group introduced this protocol so that before IEEE 802.11i group finishes its work we have a standard to implement.

RC4 stream cipher with a 128-bit key and a larger initialization vector of 48-bit for increased defense and security is used to encrypt data. Temporal Key Integrity Protocol (TKIP) is used which dynamically generates new keys as the system is used. A more secure message authentication code which is more secure than CRC-32 is used in this protocol. Here it is termed as **MIC** "message integrity code" which is used in this protocol, using an algorithm named "Michael".

The number of packets encrypted with the same key is reduced by increasing the size of key and IV.A message authentication code made it difficult to break the WLAN. The system will be shut down by the TKIP for one minute if two frames are found that fail the Michael check after passing all other integrity checks. It will then be required to generate new keys and re-authentication will be done when the network restarts, thus forcing the attacker to start over again.

3.2.1 WPA Problems

Most of the gaps in WEP's security were handled by WPA. But with new system comes new problems, and this is also true with WPA. [30]

3.2.1.1 Cracking the Pre-shared password

The wireless network gets its primary master key from the Pre shared key if the authentication server is not used for the distribution of the keys. This key is than used to create a MIC value which is used in the 4 way handshake for authentication. The MIC is created by combining Source address, Destination address, some random data and the key. Problem is this that all this information is passed as plain text in the message during the four way handshake. Thus it is easy for an attacker to use this information to authenticate itself to the network. Thus an attacker can make a list that contains the passwords cracked.

3.2.1.2 MIC Denial of Service Attack

The MIC is created using Michael algorithm, which have a built in protection mechanism to prevent invalid Integrity check value. As a result, any attempted attack on a MIC value will result in a complete disconnect of all wireless devices for one minute, and a password change. The MIC value can therefore be used itself for Denial of Service attack.

3.3 Problem Scenarios

3.3.1 802.11Authentication

The station first find an AP by active scanning or passive scanning. In Active scanning the client itself tries to find the AP by sending probe requests while in passive scanning the client receives the beacon frames which tell it about the information of AP. Once the AP is located than the client authenticate itself with the AP. AP doesn't authenticate itself with the client. The authentication and the encryption mechanism use the same secret key therefore an attacker can make use of the weaknesses of both the authentication and the encryption method to break into the WLAN network. Using different keys for different tasks is a better security practice. One dilemma is this that the station is authenticated only once at the start of the communication when the station tries to connect to the AP. After that the client is considered as a valid station and no authentication is done afterwards. Thus an attacker can spoof the MAC address and send messages on the behalf of the authenticated user and can use the encrypted messages of another station. Thus will not be detected by the AP.

802.11 define two authentication subtypes:

Open system

1) Client 1 sends an authentication request to Client 2
2) Client 2 sends the reply back to Client 1.

This means Null authentication. Any station that wants to authenticate is granted permission without any security checks.

Shared key

It uses WEP keys and is more insecure and has many flaws.

3.3.2 802.11Association

Association is done after Authentication. Data transfer starts after Association. Association Request and response steps are performed between the client and the AP. An association ID is given to the client and is added to the database of the connected clients in the AP. AP responds with a De-authentication frame when attempts by a client are made without proper Authentication and association. Acknowledgement for data frames are sent by the AP. The AP will deliver the data frames destined to a destination. It will also forward data directed to the client from the wired network. APs can also exchange traffic between two clients, but this is not common.

Chapter 4
Design and Implementation

Chapter 4

The design phase creates architecture for the developing implementations. It defines the software to be implemented. The design phase is to create a model of the system, which could be used afterwards to build the system. The Aim of this chapter is to find the most suitable possible design within the limitations imposed by the requirement and the physical and social environment in which the system will operate. In section 4.3 methodology and framework has been discussed.

4.1 Introduction

The goal of the project is to implement an efficient algorithm using artificial immune system techniques to deal with the Deauthentication and Disassociation attacks. Steps are followed just like the natural Immune system. Thus as natural phenomena's are best; similarly an attempt is made to get the best result for tackling these attacks.

4.2 Design Requirements

Immunology is the study of the protection against diseases. It protect against foreign invaders. It requires Learning and Memory. Due to the Remarkable Immune system properties like uniqueness, diversity, robustness, multilayered, reinforcement of learning and memory, imperfect recognition etc the artificial immune system is made.

Artificial Immune System:

AIS are basically intelligent methodologies used to solve the real world problems influenced by natural Immune system and immune functions, principles and models. Different kinds of problems can be solved through AIS like data analysis, search and optimization, Intrusion Detection, data mining, fault and anomaly detection etc.

The Immune system is divided into 2 broad concepts Innate and Adaptive. The Adaptive is than divided into Humoral and Cellular. The Humoral response is defined by the interaction of the antibodies and antigens. Antibodies are specific proteins produced by the immune cells to tackle with antigens. Antigens are harmful organisms entering the body from the outside world like viruses, bacteria that are usually the antibodies generators. They stimulate the immune system. Thus immunology is based upon the interaction of these two entities. Immune system differentiates between self and non-self cells. Antigenic encounters may result in cell death. Therefore some kind of positive and negative selection is done.

Applications Made Using AIS:

1) Pattern Recognition

2) Function Approximation
3) Optimization
4) Generation of Emergent Behaviors
5) Machine Learning
6) Associative Memories
7) Fault and Anomaly Detection
8) Control and Scheduling
9) Network Security
10) Evolutionary programming

4.3 Methodology / Framework

The framework consists of 2 phases

1) Training Phase
2) Detection Phase

4.3.1 Training Phase:

In the training phase the system is given time to learn from its environment. No malicious attack is considered during this phase. Threshold is set during this phase. Threshold is set using the beacon frames which is one of the Management frames. Beacon frames are the heart beat of a WLAN. They are transmitted throughout the life time of the WLAN. They are transmitted periodically to announce the existence of a WLAN. Beacon frames are transmitted by the Access Point in an Infrastructure network while in an Adhoc network this work is distributed among the stations. A typical beacon frame is 50 bytes long containing a frame header and CRC (Cyclic Redundancy Check) field which provide error detection capability. The destination address is set to all ones which means that the frame is destined for all the stations and thus all should receive them and process each beacon frame. The beacon frames consists of specific information needed by the Network.

1. Beacon Interval:

It defines the gap between each beacon. This interval tells the station when to wake up to receive the data destined for it in the Power Save mode.

2. Time Stamp:

A station uses this information for synchronization with all the stations connected with the same AP. The station updates its local clock by using this time stamp.

3. **Service Set Identifier (SSID):**

The SSID is the name and identification of the wireless LAN. AP includes the SSID in the beacon that any station which wants to get associate, automatically configures the NIC with the proper SS To reduce security risks some AP's disable the SSID from being broadcast in beacon frames.

4. **Supported rates:**

It is the information that explains the data rates that which a wireless LAN will support e.g. 1, 2, 5.5 Mbps data rates.

5. **Parameter Sets:**

Specific signaling method information is included in Beacon like frequency hopping spread spectr or direct sequence spread spectrum.

6. **Traffic Indication Map (TIM):**

TIM indicates the stations that which station has data frames buffered in AP buffer waiting for th in the Power Save mode.

4.3.2 Detection Phase:

In this phase attack is launched and it is detected that whether the System is able to tackle th malicious Deauthentication and Dissassociation attack or not. Antibodies are produced from th fields taken from Data packets and Antigens are produced by the fields taken from th Deauthentication and Dissassociation frames. Observation shows that the their seems to be a bi gap in the sequence number due to attack but a big gap can also come due to a lossy channel. Thu to tackle loss we have tolerized or trained our detectors with the normal traffic of the Beacon frame and set a threshold. As beacon frames are the heart beat of a WLAN therefore they can be used t calculate the loss in the channel. Beacon frames can be set to different rates i.e. 50ms, 100ms, 20 ms etc. However the default rate is 100ms. Thus at different rates the Threshold is set and the resu is tested that at which rate efficient detection can be achieved.

TH-6594

Euclidean Distance matching technique is used to match antigens with antibodies. The formula is:

$$\mathrm{d}(\mathrm{p},\mathrm{q}) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + \cdots + (p_n - q_n)^2} = \sqrt{\sum_{i=1}^{n} (p_i - q_i)^2}.$$

4.3.3 Structure of an Antigen:

Type	Source Address	Destination Address	Sequence No

Fig 4.1: Antigen

4.3.4 Structure of an Antibody:

Type	Source Address	Destination Address	Sequence No

Fig.4.2: Antibody

In Fig 3 and 4 Type is usually 00 and the subtype value is changed for both Deauthentication and Dissassociation frames which are 1100 and 1010 respectively. Source Address will have the Sender address and Destination Address will have the target address. Sequence No will contain the no of frame which is coming. This structure is made from the MAC frame format of 802.11b

4.4 Deployment/Environment

We are deploying our application in C# and using SharpPcap Dll. Pcap is an open source library used fo *ca*pturing and processing network packets. Pcap is used in Linux and WinPcap is used in Windows. SharpPcap is a Dll made for C# environment utilizing this library.

Many network tools use WinPcap for analysis, troubleshooting, security and monitoring purposes.

In particular, classical tools that rely on WinPcap are:

1) network and protocol analyzers
2) user-level bridges and routers
3) network monitors
4) traffic loggers
5) traffic generators
6) network intrusion detection systems (NIDS)
7) network scanners
8) security tools

SharpPcap is based on an open source library WinPcap and is used for packet capturing and ana a .NET environment. The aim of this library is to provide an API for capturing, analyzing,i and building packets using any .NET language.

The following list illustrates the features currently supported by SharpPcap:

1) Show details about physical network interface on a Windows machine.
2) Captures low-level network packets of a given interface.
3) Deals with following protocols: *Ethernet*, *ARP*, *IP*, *TCP*, *UDP*, *ICMP*, *IGMP*.
4) Injects low-level network packets on a given interface.
5) Deals with offline packet capture files.
6) Network statistics can be calculated on a given network interface.

Chapter 5
Results

Chapter 5

In this chapter we are discussing the Experimental setup, attack scenario and the tools used in the thesis in detail. Results and its conclusion are also discussed.

Results

5.1 Experimental Setup

An experimental environment is illustrated in Fig1 where Access Point D-Link is used to connect the workstations. Two Laptops Hp and Dell were used as clients and one laptop Dell was used as an Attacker machine. The clients had operating system XP and the attacking machine had the Linux version installed Back Track3.Dumps Were taken on this Linux machine by using Kismet. Kismet is a Layer 2 capturing tool. Wireshark and Commview were also used to take the dumps but they were giving the packets a form of Faked Ethernet packets. AP starts to generate Beacon frames as the client wants to connect with it. Than after sometime Data transfer gets starts. We launched an attack by using the MDK3 and Aircrack-ng tools.

In Aircrack-ng we can determine how many packets we want to sent but in MDK3 we can't define how many packets we want to send. It just sent a flood of De-authentication and Disassociation packets of 16 or more packets per second as the client tries to connect to the AP. Thus it does not allow the AP to have any connection with the client. Therefore just makes it disconnected forever and it can also damage the clients.

Kismet is used to capture the dumps through the entire procedure. We can set the beacon frames through the AP configuration software which is shown in diagram. For beacon setting we have to go into Wireless Advance Settings.

In our experiment, we observe that the security schemes such as Wired Equivalent Privacy (WEP), Temporal Key Integrity Protocol (TKIP) cannot prevent any of these DOS attacks, and there is no need to report each one of them under different DOS attacks. As these packets of Deauthentication and Disassociations are not encrypted and anyone can spoof the MAC address and use it to launch these attacks. The Mac address of one of our connected clients were used by the Attacking tools to send spoofed Deauthentication and Disassociation packets.

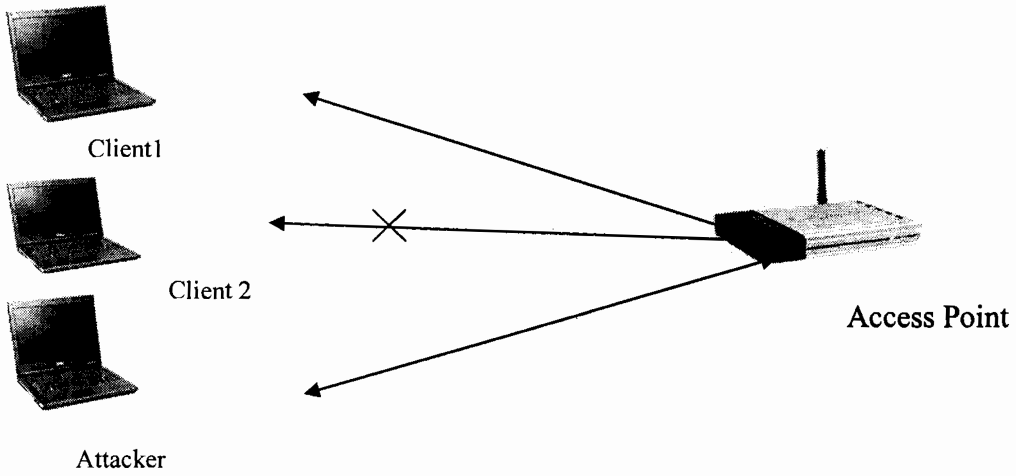
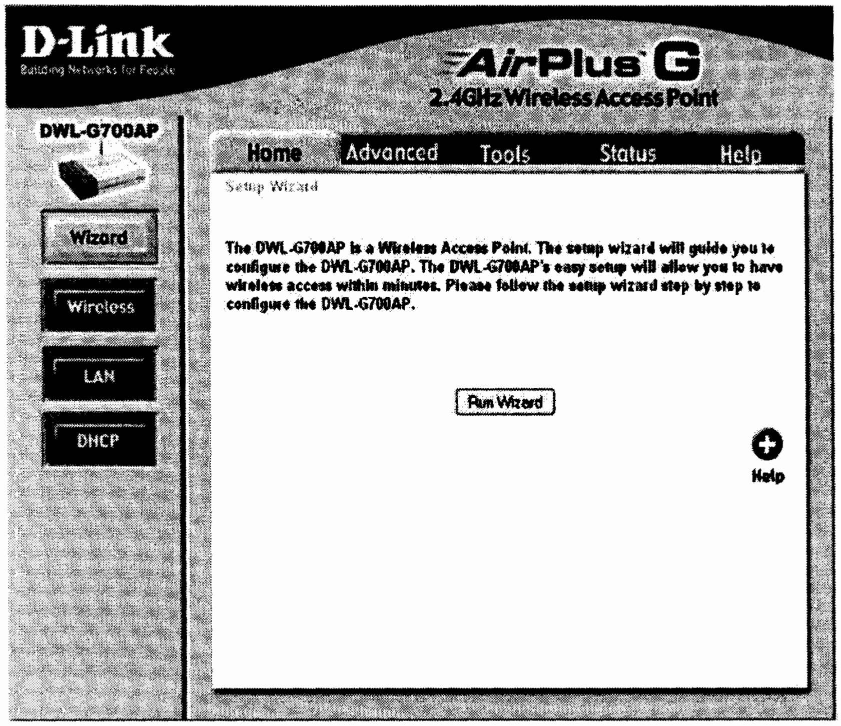


Fig 5.1 Experimental Setup

Thus beacon interval was the independent variable that was varied to check to set the best Threshold ever possible according to the environment. All experiments were performed in the same environment. Thus we performed the experiment to check whether the Beacon interval is a good and efficient factor to set the Threshold or not. And thus it is proved from the experiments that it is an efficient factor that can be used to set the threshold as they are unused periodic signals which can tell us about the loss in the channel without any extra efforts.



The DWL-G700AP is a Wireless Access Point. The setup wizard will guide you to configure the DWL-G700AP. The DWL-G700AP's easy setup will allow you to have wireless access within minutes. Please follow the setup wizard step by step to configure the DWL-G700AP.

Fig 5.2 D-Link Configuration Page

5.2 Attack Scenario

Consider an attack scenario in which two nodes are authenticated and associated with the AP. If a malicious nodes spoofs the MAC address of one of the authenticated clients and starts sending deauthentication frames to the AP. Than the client will be disconnected from the AP and will try again to connect itself to the AP. Thus the client be kept away from the AP forever if Deauthentication and Disassociation frames are sent for indefinite period of time. The more the frequency of the Deauthentication and Disassociation frames sent the more the client will have to try to connect itself to the AP. Thus there is a need that the malicious Deauthentication and Dissassociation frames are detected and ignored or discarded so that the client remains connected. Our AIS system detects the malicious Deauthentication and Disassociation frames by taking the difference in the sequence numbers of the antibody and the antigen. If the difference is greater than the set Threshold then the frame is declared as malicious.

Attack is done through Aircrack-ng and MDK3 in Linux environment. Aircrack-ng has a window version also but it operates on specific cards.

Following are the steps done to crack the WEP/WPA:

In Aircrack-ng first the Wireless card is put into Monitoring mode. Then the card is made ready to do packet injection. And then cracking is done. But we utilized it for packet injection only.

```
$ aireplay-ng -0 4 -a $AP -c $MAC ath1
```

This is the command used for Deauthentication attack. After –a comes the AP MAC address and after –c Client MAC address is put.

4 means that 4 times the packet will be sent and –a means that it's a deauthentication packet. Thus options can be varied to do different works.

5.3 Dataset Collection

Datasets for both training and testing are collected through a tool called Kismet. Kismet is a network analyzer. Kismet passively collects all the data passing through the air. Kismet is a layer 2 means Data link layer tool. Beacon frames are present in the training set which are used to set the Threshold. There are different Training and Testing datasets. Results have been tested with different value of the beacon interval. Results have been tested by keeping a beacon interval of 10, 50,100,150, 200 and 400.

5.4 Performance Metrics

An ROC graph is a technique for visualizing, organizing and selecting classifiers based on their performance. ROC graphs have long been used in signal detection theory to depict the tradeoff between hit rates and false alarm rates of classifiers. It's basically Cost Benefit analysis.

True Positives represent the benefits and False positives show the costs.

Accuracy=TP+TN/P+N

tp rate=TP/P

fp rate=FP/N

fn=FN/P

Recall=TP/P

F-measure=2/1/1+precision/recall

tp rate shows the hit rate of the classifier and fp rate shows the false alarm rate of classifier.

tp rate= positives correctly classified/Total positives

fp rate=negatives incorrectly identified/Total negatives

tn rate=negatives correctly classified/Total negatives

fn rate=positives incorrectly identified/Total positives

ROC graphs are two-dimensional graphs in which TP rate is plotted on the Y axis and FP rate is plotted on the X axis. An ROC graph depicts relative trade-offs between benefits (true positives) and costs (false positives). Each discrete classifier produces an (fp rate, tp rate) pair corresponding to a single point in ROC space.

Several points in ROC space are important to note. The lower left point (0, 0) represents the strategy of never issuing a positive classification; such a classifier commits no false positive errors but also gains no true positives. The opposite strategy, of unconditionally issuing positive classifications, is represented by the upper right point (1, 1).

One point in ROC space is better than another if it is to the northwest (tp rate is higher, fp rate is lower). Classifiers appearing on the left hand-side of an ROC graph, near the X axis, may be thought of as conservative: they make positive classifications only with strong evidence so they make few false positive errors, but they often have low true positive rates as well.

Classifiers on the upper right-hand side of an ROC graph may be thought of as liberal: they make positive classifications with weak evidence so they classify nearly all positives correctly, but they often have high false positive rates. Many real world domains are dominated by large numbers of negative instances, so performance in the far left-hand side of the ROC graph becomes more interesting.

The diagonal line y = x represents the strategy of randomly guessing of a class. For example, if a classifier randomly guesses the positive class half the time, it can be expected to get half the positives and half the negatives correct; this yields the point (0.5, 0.5) in ROC space. If it guesses the positive class 90% of the time, it can be expected to get 90% of the positives correct but its false positive rate will increase to 90% as well, yielding (0.9, 0.9) in ROC space. Thus a random classifier will produce a ROC point that slides" back and forth on the diagonal based on the frequency with which it guesses the positive class.

Any classifier that appears in the lower right triangle performs worse than random guessing.

Analysis of Graph:

TP Graph

tp rate=TP/P

Beacon Interval	TP Rate
25	0.96
50	0.90
100	0.88
200	0.87
400	0.75

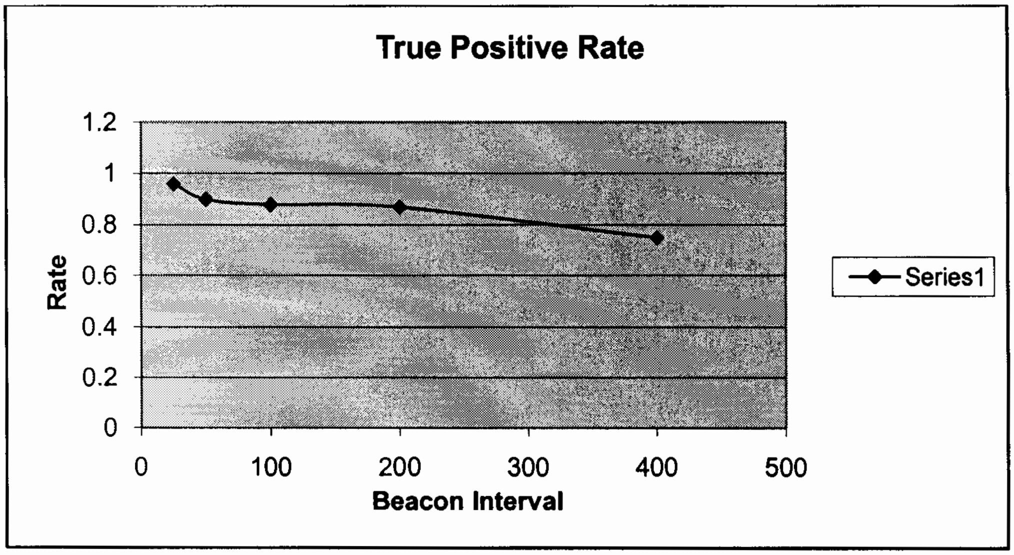


Fig 5.3: True Positive Rate

Experiments show that as the beacon interval goes down the result is becoming good as we are getting more number of packets at low beacon interval. The more the number of packets the better threshold is set in a short fixed time. Thus we get more better average at lower beacon interval.

But as the number of packets will increase the overhead on the network will also increase. Traffic will be loaded with beacon frames. But if we increase the beacon interval less number of beacon frames will be sent which is good for clients in Power save mode.

The clients can sleep long and battery will be utilized less but it has a drawback also that it makes delay the association and roaming process because stations scanning for available access points may miss the beacons.

You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down. In addition, stations using power save mode will need to consume more power because they'll need to awaken more often, which reduces power saving mode benefits

FP Graph:

Fp rate=FP/N

Beacon Interval	FP Rate
25	0.01
50	0.0172
100	0.0267
200	0.05
400	0.08

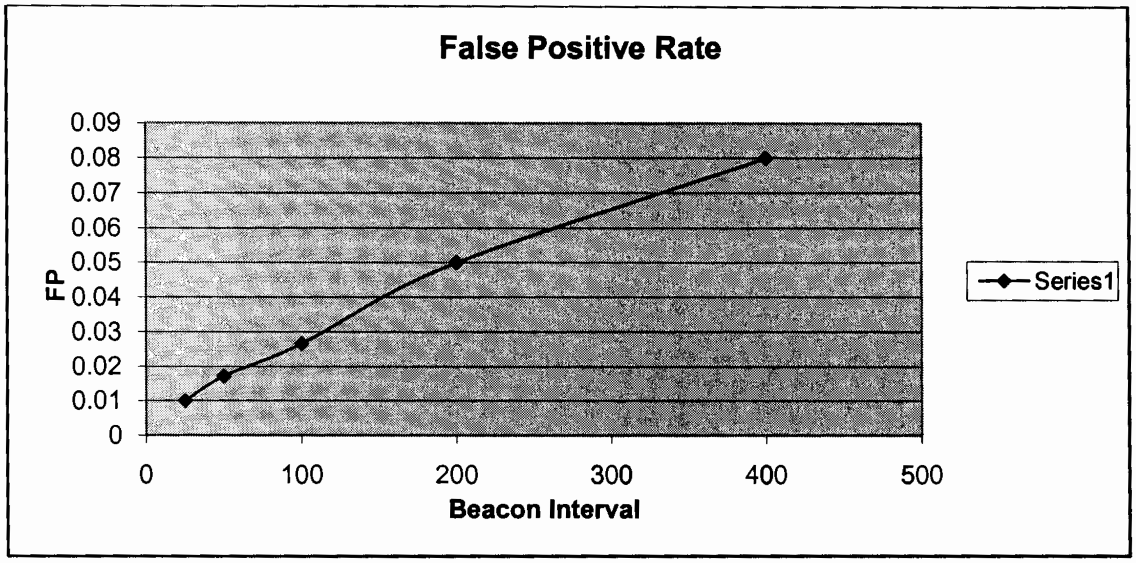


Fig 5.4: False Positive Rate

FP rate means that negatives are classified as positives. It means that normal de-authentication and disassociation packets we are getting are classified as attacks. Thus these are the mistakes which our classifier will make. Thus it represents the cost our classifier will commit. FP rate is less at 25 beacon interval and is also good at 50 and 100 beacon interval.

TN Graph:

tn rate=TN/N

Beacon Interval	TN Rate
25	0.98
50	0.98
100	0.97
200	0.94
400	0.91

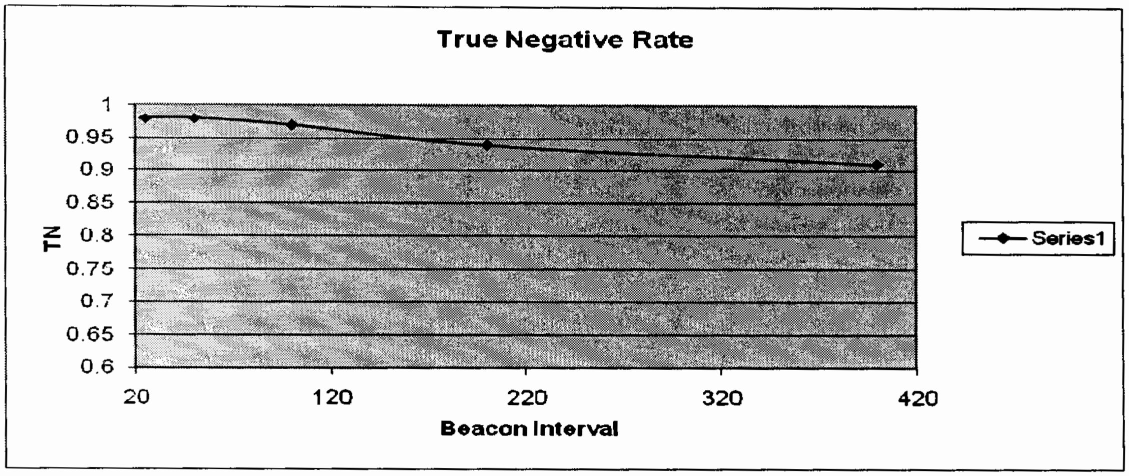


Fig 5.5: True Negative Rate

This is the graph which shows that the real normal de-authentication and disassociation packets are considered as real de-authentication and disassociation packets. We are getting better values at 25, 50 and 100 beacon interval. On some beacon intervals we are not getting good values due to the big gap in the Sequence number which comes in these packets. This unexpected gap is produced by the client without any reason.

FN Graph:

fn rate=FN/P

Beacon Interval	FN Rate
25	0.038
50	0.10
100	0.11
200	0.12
400	0.25

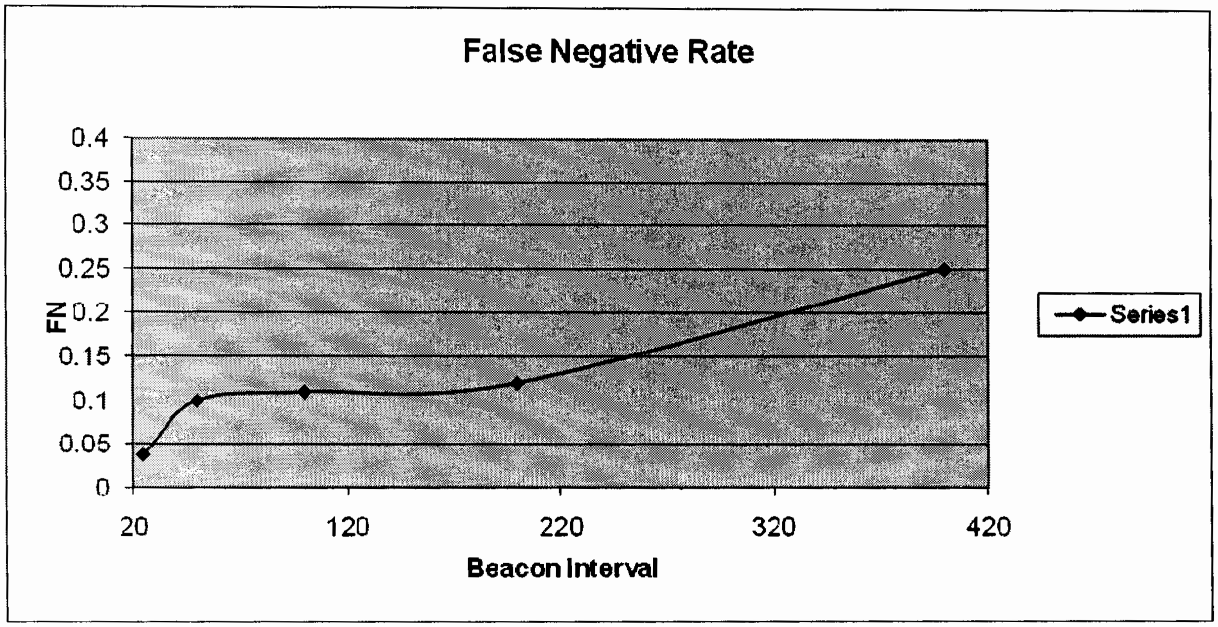


Fig 5.6: False Negative Rate

The graph shows values almost similar in identifying positives as negatives. It means that malicious packets are identified as normal de-authentication and disassociation packets. The more these values are less the more good will be the classifier. Thus the cost will be less. Therefore there will be fewer false alarms. FN rate is good at 25 beacon interval mainly. Thus the better the Threshold is set the more better will be the detections.

Performance:

FP Rate	TP Rate
0.01	0.96
0.0172	0.9
0.0267	0.88
0.05	0.87
0.08	0.75

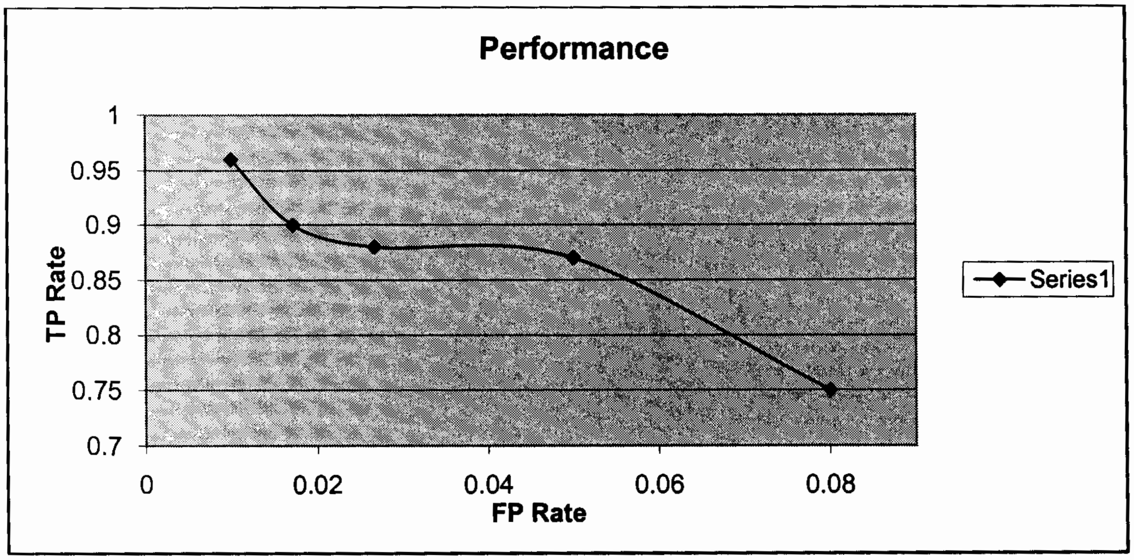


Fig 5.7: Performance Graph

This is a graph which shows the relationship between benefits and costs. The more the benefits and the less the costs are preferred. The values at the right side of the diagonal of graphs are not accepted as they have more costs or false alarm values. The value (0.01, 0.96) seems to be the best value as the FP rate 0.01 is low and the TP rate 0.96 is high. The value (0.017, 0.91) is also acceptable as the TP rate 0.91 is high and the FP rate is high low. (0.02, 0.88) at 100 beacon interval is also acceptable as it is on the left side of the diagonal.

We are getting the value (0.01, 0.96) at 25 beacon interval. Thus the low the beacon interval the better classifier we will get.

Accuracy:

Beacon Interval	Accuracy
25	0.987
50	0.978
100	0.971
200	0.92
400	0.87

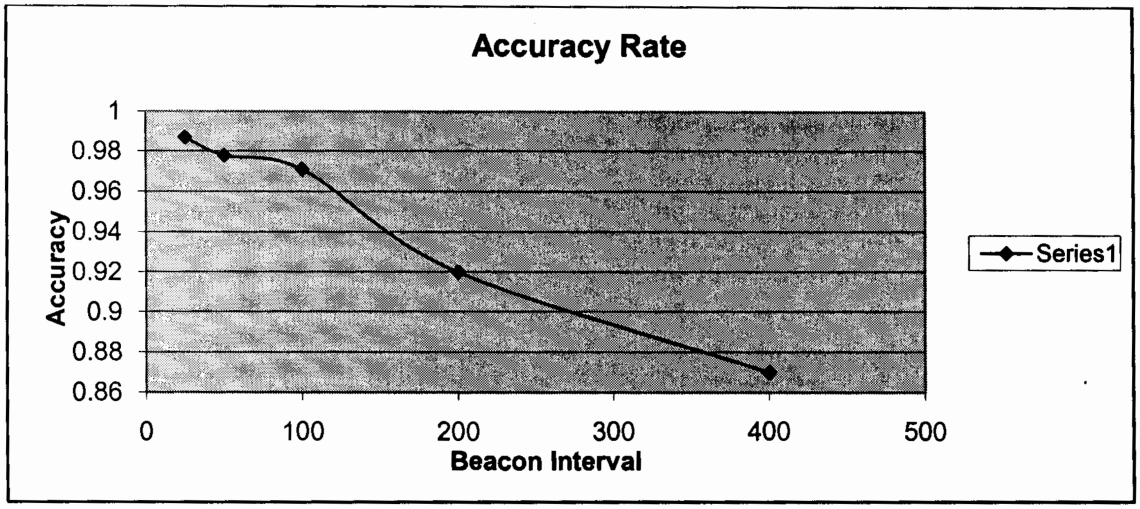


Fig 5.8: Accuracy Rate

Accuracy defines that how many packets are handled correctly. Accuracy Rate is good at 25.50 and 100 beacon interval.

Conclusion:

An important aspect of AIS is to set threshold during the training phase. We used beacon frames for this purpose. Beacon frames are the frames which exist in the network even if no data transfer is taking place. So we are able to train our system before any data transmission. AIS is trained on difference between the sequence numbers of beacon frames so in this way it incorporates the lossiness of channel. We have also carried out our experiments by setting different beacon interval. The value of beacon interval ranges from 25-400.

Figure 5.1 and 5.2 are showing the true positives and false Positive rate with varying beacon interval values. Values has been taken and calculated on different beacon intervals to show which interval could be suitable for the detection of an anomaly. True Positives rate is 1 at beacon interval value of 100. This means that all spoofed packets are considered spoofed. And false positive rate is very low at beacon interval value of 100.

Thus shown by the results we are getting good values at 25, 50 and 100 beacon interval. 25 beacon interval is giving us best value in performance and Accuracy both graphs. But we have to balance also that by getting good classifiers whether we don't overload the network traffic with beacon frames only. The network will be overloaded with beacon frames at lower beacon interval. So we should take a beacon interval according to the load of our network. If our network is heavily loaded than we should select a beacon interval that gives good classification not best and producing less burden on the network. Some classification can be compromised for less load of beacon intervals on the network.

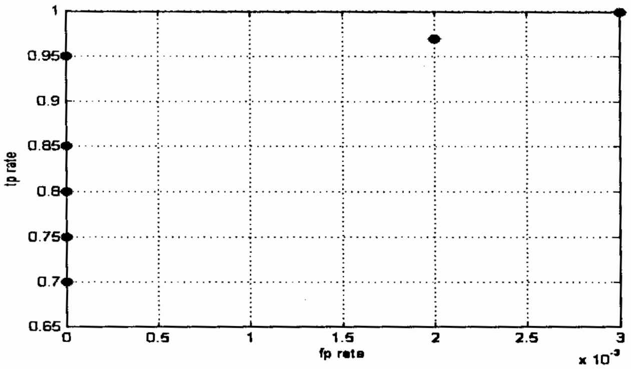


Fig 5.7: Performance of Previous Work

Performance of the previous work is static as the Threshold was static. Our work showed a better performance at a low beacon interval but the values of the performance will change with the change of the Environment. We will not always get static values as shown but we will get better performance on lower beacon intervals according to the experiment performed.

Chapter 6
Conclusion

Chapter 6

6.2 Achievements

A Defense mechanism to tackle with Deauthentication and Dissaasociation attack has been designed in Real environment by keeping in mind the lossiness of the channel to be noted.

6.3 Improvements

The results can be improved by putting some other criteria for noting the lossiness of the channel. E.g. Signal strengths. Signal strengths can be used for finding the loss in the channel. But by implementing this idea other issues arises as signal strength on each client would be different thus signal strength should be calculated at each client and then the Threshold value will not be the same for the whole network. It will be different for each client as signal strengths will be different at each client.

6.4 Future Recommendations

A full Intrusion Detection System can be developed by using Artificial immune System. AIS is a new field and can be used to implement many other problems. As natural techniques and ways to tackle problems are the best made by Nature so it can be used to handle the attacks and problems made by humans. Other decision methods like neural networks, decision trees can also implemented for distinguishing between the self and non-self.

Other Denial of Service attacks can also be handled by using AIS like Man in the Middle attack, power saving attack etc. With detection, Prevention and avoidance techniques can also be designed for the Wireless network 802.11. Many other flavors of IEEE 802.11 have been made and are under process thus can also be handled using AIS.

AIS can also be implemented at different layers of the Network to tackle with different attacks.

References

References:

1) Jungwon Kim,Peter Bentley: The Human Immune System and Network Intrusion Detection, Department of Computer Science, University College London Gower Street,London.

2) M..ZubairShafiq,Muddasir Farooq, Defense against 802.11 DOS Attacks using Artificial Immune System, 6th International Conference on Artificial Immune Systems, In LNCS, Brazil 2007

3) John Bellardo and Stefan Savage, 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions, In Proceedings of 12th USENIX Security Symposium 2003, Pp. 15-28

4) ANSI/IEEEStd802.11,1999Edition(R2003),url:standards.ieee.org/getieee802/802.11.html

5) Tom Fawcett, ROC Graphs: Notes and Practical Considerations for Researchers, HP Laboratories, 16 March 2004

6) Patrick LaRoche and A. Nur Zincir-Heywood :802.11 De-authentication Attack Detection using Genetic Programming, Valencia, EuroGP ,2006

7) Patrick LaRoche and A. Nur Zincir-Heywood :802.11 Network Intrusion Detection using Genetic Programming, GECCO, Workshop Program, 2005

8) Dipankar Dasgupta:Advances in Artificial Immune Systems :In IEEE Computational Intelligence Magazine , November 2006

9) url:http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm

10) R. Heady, G.Luger, A. Maccabe and M. Servilla. The architecture of a network level intrusion detection system, Technical report, Computer Science Department, University of New Mexico, August 1990

11) U Aickelin, P Bentley, S Cayzer, J Kim, J McLeod Danger Theory: The Link between AIS and IDS?,HP Laboratories Bristol , July 2003

12) Jungwon Kim§, Peter J. Bentley§, Uwe Aickelin*, Julie Greensmith*,Gianni edesco†, Jamie Twycross, Immune System Approaches to Intrusion Detection - A Review : In ACM , April 2008

13) Divyata Dal1, Siby Abraham, Ajith Abraham, Sugata Sanyal and Mukund Sanglikar, Evolution Induced Secondary Immunity: An Artificial Immune System based Intrusion Detection System: In 2nd International Conference on Security Information and Networks , 2009

14) Aickelin University of Nottingham, UKD. Dasgupta University of Memphis, Memphis, TN 38152, USA Artificial Immune System Chapter 13.

15) Stefan Axelsson ,Intrusion Detection Systems: A Survey and Taxonomy, Department of Computer Engineering Chalmers University of Technology Goteborg, Sweden 14 March 2000

16) Bace, Rebecca, "An Introduction to Intrusion Detection and Assessment for System and Network Security Management," ICSA White Paper, 1998.

17) http://www.securityfocus.com/infocus/1564

18) Paul Innella and Oba McMillan, Tetrad Digital Integrity ,An Introduction to Intrusion Detection Systems, LLC last updated December 6, 2001

19) Herve Debar IBM Research, Zurich Research Laboratory, Sauumerstrasse 4, CH-8803 Ruschlikon, An Introduction to Intrusion-Detection Systems Switzerland, 2002

20) U. Aickelin, Chapter 13 ARTIFICIAL IMMUNE SYSTEMS University of Nottingham, UK D. Dasgupta University of Memphis, Memphis, TN 38152, USA

21) Tom Karygiannis, Les Owens Wireless Network Security 802.11, Bluetooth and Handheld Devices National Institute of Standards and Technology U.S Department of Commerce Special Publication 800-48

22) Joshua Wright, Detecting Wireless LAN MAC Address Spoofing,http://home.jwu.edu/ jwright/papers/wlan-mac-spoof.pdf , January 2003.

23) D. Dasgupta and J. Gomez and F. Gonzalez and M. Kaniganti and K.Yallapu and R. Yarramsetti, MMDS:Multilevel Monitoring and Detection System, In the proceedings of the 15th Annual Computer Security Incident Handling Conference (FIRST), Ottawa, Canada June 22-27, 2003.

24) Douglas Madory, New Methods of Spoof Detection in 802.11b Wireless Networking, http://www.cs.dartmouth.edu/map/papers/madory-msthesis.pdf: In Thesis of Thayer School of Engineering Darmoutj College Hanover,New Hampshire ,June 2006

25) Aseem Tandon, s802.11 Denial-of-Service Attacks Real Vulnerabilities and Practical Solutions, http://www.comp.nus.edu.sg/~cs4236/stu-present/aseem.ppt ,March 23, 2004

26) Pablo Brenner A Technical Tutorial on the IEEE 802.11 Protocol BreezeCom Wireless Communication 1997.

27) Fanglu Guo and Tzi-cker Chiueh, Sequence Number-Based MAC Address Spoof Detection, Volume 3858 of Lecture Notes in Computer Science, pp.309-329, Springer, Berlin,January 2006.

28) Yong Sheng3, Keren Tan1, Guanling Chen2, David Kotz1, Andrew Campbell1 Detecting MAC layer Spoofing Using Received Signal Strength, Proceedings 27th Annual Joint Conference IEEE Computer and Communications Societies (INFOCOM), April 2008, pp. 1768-1776

29) Lopez-Aguilera, E.Casademont, J Cotrina J, IEEE 802.11g performance in presence of beacon control frames 15th IEEE Symposium Sept 5-8 2004 Volume: 1, pp.318- 322 ,Vol.1

30) http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

31) http://www.informit.com/guides/content.aspx?g=security&seqNum=86

Acronyms

Acronyms

Term	Abbreviation	Meaning
Intrusion detection system	IDS	Software systems which identify misuse of computer networks.
Misuse detection	-	Intrusion pattern matching algorithm
Anomaly detection	-	Detection of difference from a learned norm
False positive	FP	An error, where normal is wrongly identified as an intrusion
False negative	FN	An error, where an intrusion is wrongly identified as normal
Human Immune System	HIS	The cells and processes that protect us against harmful pathogens.
Artificial Immune Systems	AIS	The range of algorithms (e.g. negative selection) based on inspiration from the human immune system
Antigen	Ag	In biology, the molecule used by immune cells to identify pathogens; in AIS, the datum analyzed during the detection process. Self-antigens comprise normal data; non-self antigens comprise abnormal data (potentially representing a pathogen or intrusion).
Antibody	various (Ig, IgG, IgA, IgM, IgD, IgE)	In biology, a protein produced by B-cells that is designed to stick to specific antigens, in AIS, often used interchangeably with “detector” and sometimes confused with T-cells or B-cells.
Danger Theory	DT	Theory of HIS that suggests harmful pathogens can be detected by examining “danger signals” generated by cells killed abnormally by pathogens.
Negative Selection	NS	Theory of HIS that suggests the immune system performs anomaly detection by creating detectors that match everything except “self antigens”.
Dendritic cell	DC	An important class of antigen presenting cells in the HIS that ingests antigens or protein fragments and that are receptive to danger signals.
B-cell	-	Important immune cells in the HIS that produces antibodies.
T-cell	various (naïve, Th, Th1, Th2, CTL)	Significant immune cells in the HIS that differentiate into different classes when mature, such as helper T (Th) and killer T cells (CTL). T cells primarily detect intracellular pathogens that escape antibody detection.

International Islamic Univ.
CENTRAL
LIBRARY
ISLAMABAD.