PERFORMANCE STUDY ON IEEE 802.11 WIRELESS LOCAL AREA NETWORK SECURITY

By

Nedier Janvier Senat

A thesis submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

In

COMPUTER ENGINEERING

UNIVERSITY OF PUERTO RICO
MAYAGÜEZ CAMPUS
2006

Approved by:

Manuel Rodriguez, PhD Member, Graduate Committee	Date
Nestor Rodriguez, PhD Member, Graduate Committee	Date
Yi Qian, PhD President, Graduate Committee	Date
Dorothy Bollman, PhD Representative of Graduate Studies	Date
Isidoro Couvertier, PhD Chairperson of the Department	Date

ABSTRACT

The IEEE 802.11 Wireless Networks gains its popularity and fame by providing the users with several advantages in accessing information. WLANs provide true mobility and flexibility to users. Another advantage of wireless technology is installation. A physical or cable connection is no longer needed because a single connection to the access point via electromagnetic waves is all that is necessary. This both decreases installation costs and allows for wireless networks to be installed in locations where previously it would have been difficult or impossible to install wiring. Such benefits and advantages bring up some security and performance problems.

Various researchers have proposed several solutions to improve WLAN security and to understand the impact of the security mechanisms on the performance of the network. However, the establishment of a tradeoff between security and network performance is often neglected. The aim of our research thesis is to quantify the impact of the security mechanisms on the performance of the network.

This research thesis investigates the effect of multiple security mechanisms on the performance of multi-client saturated and unsaturated networks. The performance effect of different TCP and UDP packet size distributions on secure networks is also studied. Our results prove that the security mechanisms affect the network performance in different ways and the more secure the network is, the lower the performance is. Our results provide ways in which to configure wireless networks such that security requirements can be met in relation to quantifiable performance impact in practical situations.

RESUMEN

El IEEE 802.11 (redes inalámbricas) gana su renombre y fama proveyendo a los usuarios varias ventajas accesando informaciones. WLAN provee mobilidad verdadera y flexibilidad a los usuarios. Otra ventaja que provee las redes inalámbricas es la instalación. Una instalación física no es necesaria porque una única conexión al punto de acceso o antena usando ondas electromagnéticas es todo lo que es necesario. Ambos, decrece el costo de instalación y permite de instalar redes inalámbricas en locaciones donde fue realmente difícil de instalar redes (LAN) previamente. Tales beneficios y ventajas traen problemas de seguridad y de desempeño.

Varios investigadores han propuesto varias soluciones para mejorar la seguridad de WLAN y para entender el impacto de los mecanismos de seguridad sobre el desempeño de la red. Sin embargo, el establecimiento de una compensación entre la seguridad y el desempeño de la red se descuida a menudo. El objetivo de nuestra investigación es de cuantificar el impacto de los mecanismos de seguridad sobre el desempeño de la red.

Esta tesis investiga el efecto de varios mecanismos de seguridad sobre el desempeño de las redes inalámbricas saturadas y no saturadas de multi-cliente. El efecto del desempeño de distribuciones de paquetes usando TCP y UDP como tipo de tráfico en redes seguras también fue estudiado. Nuestros resultados demuestran que los mecanismos de seguridad afectan el desempeño de la red en diversas maneras y mas seguro es la red, menos es el desempeño. Nuestros resultados proveen maneras de las cuales que se pueden configurar las redes inalámbricas tales que los requisitos de seguridad se pueden resolver en lo referente al impacto cuantificable del desempeño en situaciones prácticas.

To my Dad "Pierre Sorel Janvier" who died during my studies and to my mom "Anne Marie Senat" and my sister "Aelle Janvier" who were always supportive during my graduate studies.

ACKNOWLEDGEMENTS

During my graduate studies at the University of Puerto Rico, I have collaborated and worked with several professors, persons and institutions directly and indirectly for my research and when things become difficult and complicated, I was always being encouraged by different family members and friends. Without their support and help, it would definitely have been impossible for me to terminate the research work and my thesis. Then, I want to dedicate this section to thank them and express my appreciation for their support.

Firstly, I would like to thank GOD for giving me the strength and health to hang on there for two years to terminate my master's thesis and my graduate studies. I would like to express my gratitude to my advisor Dr. Yi Qian for believing in me and giving me the opportunity to work with him for my thesis and to provide me with a scholarship to pay for my studies. I can not forget about Dr. Nestor Rodriguez and Dr. Manuel Rodriguez who were always there for me to answer my questions and to give advice; thank you very much. I would like to thank Angel, Martin and Carlos for helping out with the experiment setups and with any problems related to networking.

I would like to thank Hernan Mendez for being a good friend and for his support, especially when things got very complicated. I would like to thank my mom Anne Marie Senat for her love, financial support and for always being there for me. Finally, I want to thank all my friends who have always been supportive from the beginning of my graduate studies until the end.

Nedier Janvier

Table of Contents

Table List

Tables **Page**

Figure List

Figures **Pages**

CHAPTER 1

Introduction

The needs of accessing information while moving around make mobile technologies very demanding and preferred by a lot of users. In fact, when we talk about mobility, the closest term that comes to our mind is “Wireless Network” which is any network system that provides users with both mobility and flexibility in accessing information. Because of the needs for mobile communication, wireless network has become very popular. Unlike the wired Local Area Network, IEEE 802.11, one of the most popular WLAN does not require a physical connection from the client to be connected to the network because the data is transmitted and received over the air. It uses an access point to establish the connection between users and servers by transmitting data over the air. Such benefits of mobility and access bring up some security and performance issues. The fact that the data is transferred over the air makes it really easy for an attacker to intercept it and use it for wrong purposes. However, security is a very important problem because people use wireless network services for various purposes such as: online transactions using a credit card, sending email or exchanging personal data. Thus, the interception of these types of information by an attacker can cause a lot of damages to companies and users.

Several security algorithms have been proposed by researchers from different manufacturers to solve the IEEE 802.11 security problems. Usually, the use of these security mechanisms can decrease the performance of the network. The problem of the impact of the security mechanisms on the performance of the network is worth studying.

1.1 Problem Statement and Justification

Wireless computing is a rapidly emerging technology that provides users with network connectivity without being tethered off of a wired network. Once the user is connected to the network via wireless, he/she has the opportunity to move around with his/her laptop and still be able to access the resources of the network. That's why users like the wireless technology so much.

In fact, most of the time, when it comes to naive network users, their only concerns is to be connected and being able to access information on the network and they never think about the existing security risks when someone is navigating on the internet or exchanging information via a network. This is especially tune of wireless users. All they have in mind is to be able to access information everywhere without the need of a physical connection, but they never realize that a wireless network have serious security flaws because of its transmission medium which is the air. Thus, it is very easy for an attacker to access a wireless network without authorization and to use information or resources of the network for the wrong purposes.

The security of the wireless network is an important topic that needs to be studied. Over the years, several security mechanisms have been proposed by the wireless network equipment manufacturers and researchers. Even though they are not completely secure, they provide some security means to the users against attackers. The drawback of using the security mechanisms is that they affect the performance of the network. Thus, some work needs to be done with the main goal of providing a way to protect the wireless network while taking into

consideration the performance of the network. A tradeoff between security and performance is necessary in order to protect the wireless LAN.

1.2 Objectives

Although wireless network is among the fastest-growing trends in technology, the key point of the companies from adopting it, is security. The main concerns for enterprises are the security risks associated with WLAN and the overhead or performance problem involved with managing these risks.

Because of the security issues of the Wireless Local Area Network, several researchers have conducted research on the IEEE 802.11 WLAN to improve its security measures. The main purpose of this project is to understand the security problems and vulnerabilities of the IEEE 802.11 and to quantify the impact of the security mechanisms on the performance of the Wireless Local Area Network. Then, make an analytical comparison of the performance of different security enhancement schemes and propose the security mechanism that provides the best tradeoff between performance and security as recommendation for the protection of the IEEE 802.11 WLAN.

The objective of this thesis is to identify the performance and security issues of Wireless Local Area Networks using several security mechanisms. The goal of the research study can be subdivided into four questions:

- How is the network performance at each security level?
- Do the security mechanisms have any impact on performance while using the IEEE 802.11 model?

- Do the security mechanisms have an impact on different traffic types?
- Do the traffic types (TCP and UDP) affect the performance of the network differently?

The outcome of the investigation is a proposed wireless security policy guidelines or recommendations based on the results of the experiments that provide tradeoffs between security and performance.

1.3 Thesis Outline

Chapter 2 provides an overview of Wireless Local Area Network. A complete overview of the IEEE 802.11 and protocol being used is presented. In Chapter 3, we present several security mechanisms for the IEEE 802.11 and the security treats that can affect them.

Chapter 4 presents a brief overview of the network performance metrics and also discusses prior research carried out on the performance of the network when different security layers are applied.

Chapter 5 explains the methodology being used to conduct the experiment; the manual setup of the Wireless LAN and the equipments used to obtain accurate results.

In Chapter 6, the results and data collected during the experimentation are presented, analyzed and validated. The impact of the security layers against the network performance is evaluated based on the traffic types such as TCP and UDP and for different security mechanisms. The impact of the security mechanisms against multiple clients is also measured.

In Chapter 7, we provide some recommendations based on the results of our experiment on how to configure and choose a security mechanism based on a tradeoff between performance and security. We conclude our study and indicate several subjects for future work in Chapter 8.

CHAPTER 2

Wireless Local Area Network

Since the invention of laptop computers, many people had a dream of walking into an office and magically having their notebook computer being connected to the internet [40]. Consequently, various group of researchers started working on ways and different approaches to accomplish this goal. It has been less than a decade since researchers have come up with a practical technique that allows users to move around an office with a mobile device and still be able to connect to the internet and access network resources without the need for a physical connection. Both the office and the mobile devices have to be equipped with short-range radio transmitters and receivers to allow them to communicate. That approach quickly led to Wireless Local Area Networks (WLAN) being marketed by several companies.

IEEE 802.11 is the major Wireless Local Area Network standard. This chapter presents an overview of the IEEE 802.11 standard.

2.1 Wireless LAN Overview

The wireless LAN technology and industry were born in the mid 1980s when radio frequency (RF) spectrum was first made available by the Federal Communications Commission (FCC). When it was first introduced to the market, growth was considerably slow. Lately, wireless LAN technology is experiencing incredible growth. In addition to the flexibility it provides to the users, one of the key reasons that allows its growth is the increased bandwidth made

possible by the IEEE 802.11 standard. Table 2-1 provides some key and important characteristics of the 802.11 standard.

Table 2.1: Characteristics of 802.11 Wireless LANs [26]

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hoping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), Infrared (IR).
Frequency Band	2.4 GHz (ISM band) and 5 GHz.
Data Rates	1 Mbps, 2 Mbps, 5.5 Mbps (11b), 11Mbps (11b), 54 Mbps (11a)
Data and Network Security	RC-4 based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management. (AES is being considered for 802.11i).
Operating Range	Up to 150 feet indoors and 1500 feet outdoors.
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless clients cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode: throughput decreases with distance and load.

2.2 Brief History

Motorola developed one of the first commercial WLAN systems with its Altair product. However, early technologies had several problems that prohibited its pervasive use; these LANs were expensive, provided low data rates, prone to radio interference and were designed mostly to proprietary RF technologies [26]. In 1990, IEEE initiated the 802.11 project with the main goal of developing a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity within an area. It was in 1997 that IEEE first approved the 802.11 international standard. In 1999, IEEE ratified the 802.11a and

802.11b standards. Since then, several other 802.11 standards have been ratified such as: 802.11g, 802.11e, 802.11i et al.

2.3 Wireless LAN Requirements

Wireless Local Area Network provides users with several advantages such as mobility, greater flexibility and increased productivity. But users still keep asking if WLANs provide the same services and capabilities as wired LANs. Thus, the wireless community faces certain challenges and constraints to meet these objectives. Willing to meet these objectives, the IEEE 802.11 standard committee has to come up with WLANs system that can meet certain requirements typical of any LAN such as high capacity, ability to cover short distances, full connectivity among attached stations and broadcast capability. They also have to meet certain requirements specific to their intended environment such as:

- **Throughput:** Because of physical limitations and limited bandwidth, currently WLANs are operating at data rates between 1 to 54 Mb/s while wired LAN can be operated at a transmission speed of 10 GB/s.
- **Number of nodes:** WLANs should be able to allow hundreds of nodes to communicate with each other across multiple cells.
- **Transmission robustness and security:** A wireless LAN needs to be properly designed to avoid interference and security problems since if not, the network may be prone to interference and it will be easier for an attacker to eavesdrop and get access to it. A proper

design of the WLAN allows reliable transmission and a high level of security against eavesdropping.

• **Service area:** A typical coverage area for a wireless LAN is approximately of 100 to 300 meters.

• **Power consumption:** When users are connected to a wired LAN, most of the times their devices are connected to a power outlet plug that produces a current of 110 V, which is different for connections to a wireless LAN where the majority of devices are mobile, portable and typically battery powered. Thus, the use of a battery is definitely required for wireless devices. Therefore, devices must be designed to be very energy-efficient, resulting in “sleep” modes and low-power displays, causing users to make cost versus performance and cost versus capability trade-offs [16].

• **Handoff/roaming:** When the wireless LAN of an organization is composed of several cells, the MAC protocol being used should allow the user and his/her mobile devices to move from one cell to another.

• **Dynamic configuration:** The MAC protocol being used for network management should allow organizations or enterprises dynamically and automatically to add, delete or relocate end systems without interrupting other users of the wireless LAN.

2.4 Architecture

The *basic service set* (BSS) is the fundamental building block of the IEEE 802.11 architecture [16]. A BSS is a group of stations that are functioning under the direct control of

a single coordination function such as Distributed Coordination Function (DCF) or Point Coordination Function (PCF). The geographical area covered by the BSS is called a basic set area (BSA) which is equivalent to a cell referring to cellular communications network. Normally, all the stations in a BSS can communicate with each other and they can also interact with other stations in another basic set. In fact, the 802.11 standard can be operated in two different modes: Ad-Hoc and Infrastructure mode.

In the infrastructure mode, also known as basic service set, the WLAN consists of at least one access point (AP) that regulates and manages the activities of the network and a set of mobile devices connected to it. In this type of wireless network, the functionality of the network is centralized into the access point because all messages sent have to pass through the access point first before reaching the node receiver. In certain cases, depending on the configuration of the network, the users have to identify himself/herself to the access point by using a user name and password to get access to the network. In some cases where the wireless network has to communicate or interact with a wired network, the access point is used as an Ethernet bridge to maintain the connection. Figure 2.1 .b shows an example of a wireless network in a single cell consisting of one access point and four stations connected to it.

The Ad-Hoc mode is also called peer-to-peer or Independent Basic Service Set (IBSS). A WLAN is said to be in that mode when it is a self-configuring network consisting of a set of autonomous mobile users that communicate over relatively bandwidth constrained wireless links. This type of network requires at least two mobile devices (PCs) equipped with wireless cards or a transmitter and receiver to be able to form a simple peer-to-peer network that will

allow the PCs to share resources. The mobile devices can communicate directly with each other without the help of an access point, and therefore have no fixed infrastructure. Because the nodes are mobile, the topology of the network can be changed without any prediction. All the activities of the network such as: discovering the type of topology to be used, delivering and routing messages must be done by the nodes themselves. It is a decentralized network type where the functionality of the wireless local area network is based on the nodes.

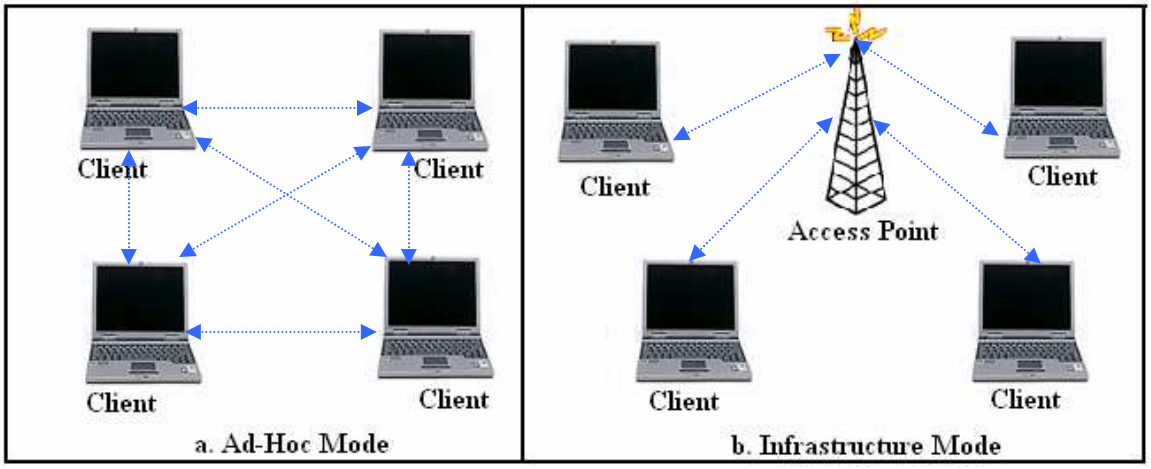

Figure 2.1: Ad-Hoc and Infrastructure Modes

Figure 2.1.a shows an example of an Ad-Hoc network composed of four clients that interchange information with each other. The main problem of Ad-Hoc network is security because the fact that the network doesn't have a fixed topology and a centralized structure make it easier for an attacker to access the network.

In some particular cases a WLAN may be formed by a single cell with only one access point, but most of the times the network will be formed with several cells in which the access points are connected through a backbone called a *distribution system* (DS), typically Ethernet.

Together, the whole interconnected wireless LANs including several different cells, their access points and the distribution system, is seen by the upper layers of the OSI model as a single network and is called the *Extended Service Set (ESS)*. The standard also includes a definition of a concept named Portal which is a device that connects an 802.11 and an 802 LAN. Figure 2.2 shows a typical Wireless LAN including the components described previously.

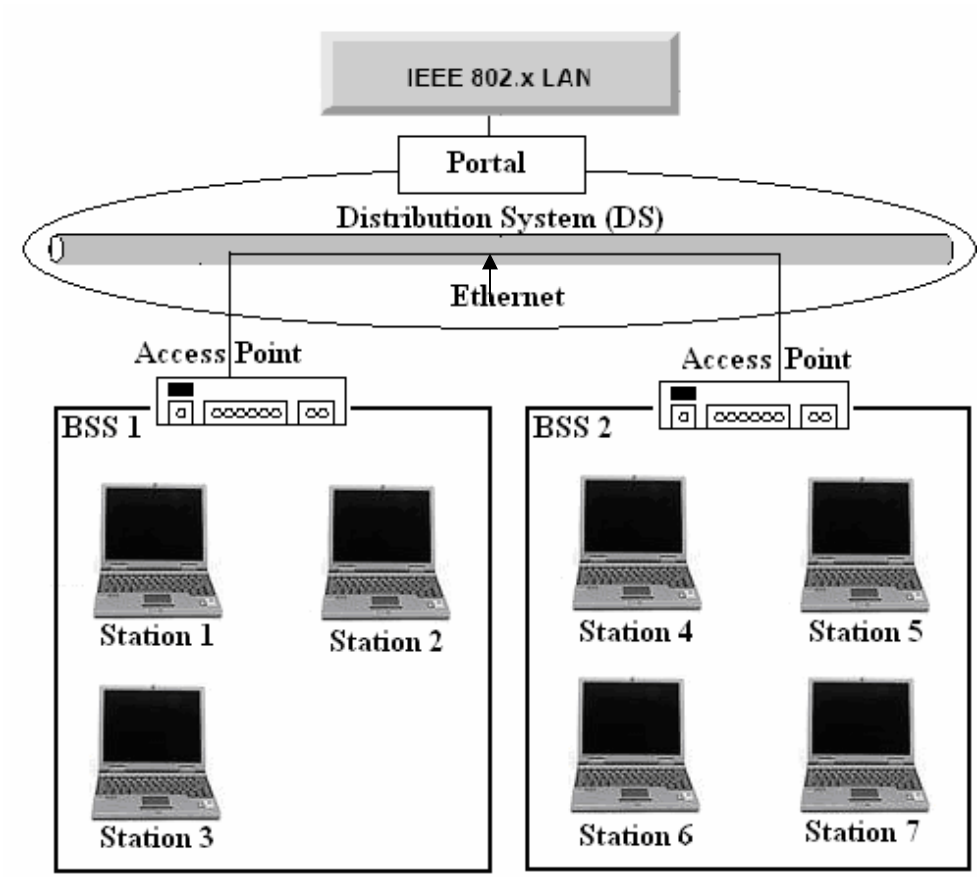

Figure 2.2: Extended Service Set [37]

Even though the 802.11 standard does not require it, practically, a typical installation will place the access points and the portal on the same or a single physical entity that is connected to the 802 LAN.

2.5 Services

The IEEE 802.11 standard defines several services that the wireless LAN has to possess to possibly match the great functionality in wired LANs. The main services are: *Association, Authentication Security and Privacy*.

• **Association:** To be able to connect to a wireless LAN, a mobile device has to provide certain information such as identity, data rates supported, power management requirements and address to the network. To do so, it must establish an association with one of the access points of the network. The access point based on the information provided by the mobile station and its capability might accept or refuse its association to the network. Once the base station accepts the mobile station, it has the capability to communicate the information of the user to another access point which makes it easier for the user to move around. This is called reassociation and makes it possible for an established association or an accepted user to transfer from one access point to another. Another service, called disassociation, makes it possible for a mobile or a base station to notify other base stations when an existing association is terminated.

• **Authentication security:** Because of the fact that wireless communication can easily be sent or received by unauthorized stations, a mobile station must authenticate itself to the network before being allowed to send data or messages across the WLAN. Once a station is accepted by a base station, the base station sends a special challenge frame to it just to see if the station knows the password or secret key that is assigned to it. If the station returns a correct answer to the base station, it is completely enrolled in the cell.

• **Privacy:** The confidentiality of the information being sent over a wireless network is very important and to accomplish this, the messages need to be encrypted. To affirm the security or privacy in the 802.11 standard, the *Wired Equivalent Privacy* (WEP) algorithm is used. To provide both privacy and data integrity, the WEP algorithm uses an encryption scheme based on the RC4 encryption algorithm which based on the idea that two communicating parties must share a 40 or 128-bit key, which encrypts and decrypts all frames [37].

2.6 Protocol Layers

A typical protocol stack of IEEE 802.11 is given in Figure 2.3. The protocol stack of the 802.11 standard consists of three layers: logical link control, media access control and physical layer as illustrated in the figure.

The logical link control layer provides an interface to higher layer and performs some basic link layer functions such as error and flow control. A LAN always needs some ways to control access to the transmission medium of the network so that the devices will use the capacity efficiently. This responsibility belongs to the MAC protocol which ensures that all devices on the network are corporate. The physical layer corresponds to the OSI physical layer fairly well and the IEEE committee issued the physical layer for 802.11 in three stages. As shown in Figure 2.3, it includes the MAC layer and three physical layers: direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS) and infrared.

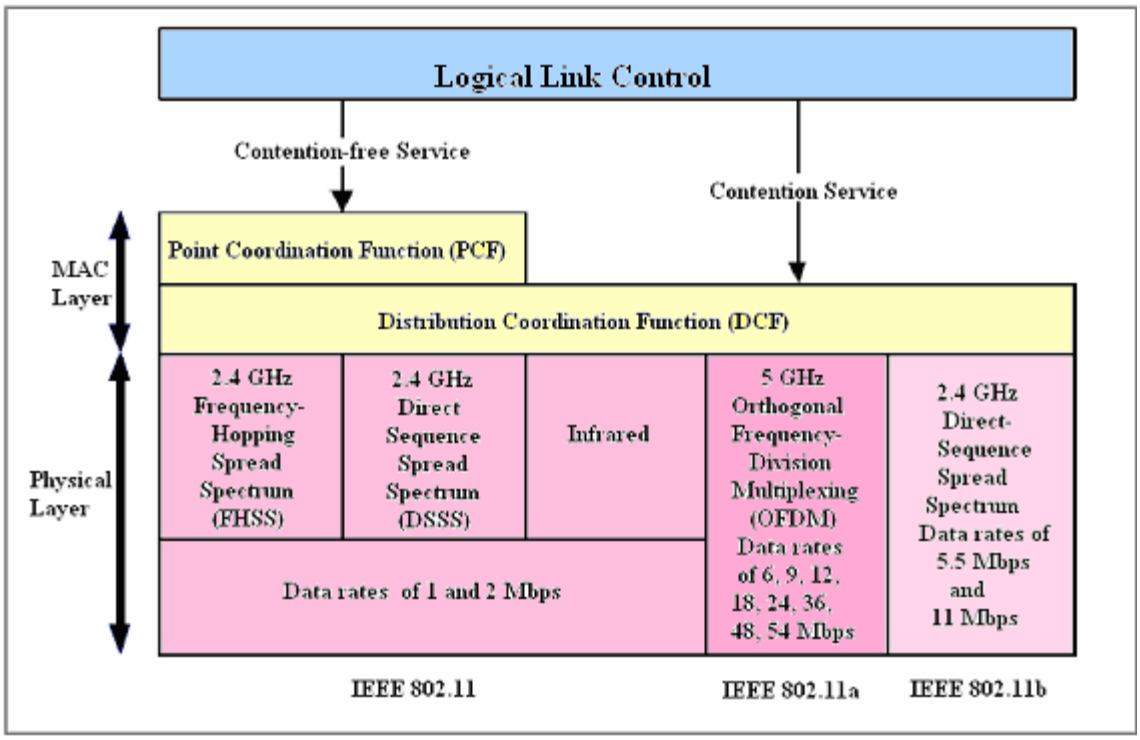

Figure 2.3: IEEE 802.11 Protocol Stack [37, 38]

2.6.1 Physical Layer

The physical layer describes the frequency band, data rate and encoding technique. The 802.11 standard has three physical layers and these are the following:

• *Direct-sequence spread spectrum (DSSS)*: The 802.11 standard defines this medium as operating in the 2.4 GHz ISM band, at data rate of 1 and 2 Mbps. Each bit is transmitted as 11 chips by using what is called a *Barker sequence.* It uses phase shift modulation at 1 Mbaud, transmitting 1 bit per baud when operating at 1 and 2 bits per baud when operating at 2 Mbps. No license is required to use this band in the US. The total number of available channels depends on the bandwidth allocated by the national regulatory agencies.

• *Frequency-hopping spread spectrum (FHSS):* uses 79 channels and operates in the 2.4 GHz ISM band, at data rates of 1 and 2 Mbps. A pseudorandom number generator is used to produce the sequence of frequencies hop. As long as all stations use the same seed to the pseudorandom number generator and stay synchronized in time, they will hop to the same frequencies simultaneously. The dwell time, which is the amount of time at each frequency, is an adjustable parameter but must be less than 400 msecs. FHSS randomization provides a fair way to allocate spectrum in the unregulated ISM band and provides a measure of security because an attacker who does not know the hopping sequence or dwell time will not be able to eavesdrop on transmissions.

• *Infrared (IR):* The IR or infrared band specification identifies a wavelength range from 850 to 950 nm. The IR band is designed for indoor use only and operates with nondirected transmissions. The IR specification was designed to enable stations to receive line-of-site and reflected transmissions. Encoding of the basic access rate of 1 Mb/s is performed using 16-pulse position modulation (PPM) where 4 data bits are mapped to 16 coded bits for transmission. The enhanced access rate (2Mb/s) is performed using 4-PPM, where 2 data bits are mapped to 4 coded bits for transmission [16].

2.6.2 MAC Layer

The MAC layer is responsible for allocating channel procedures, addressing protocol data unit (PDU), formatting frames and error checking. This protocol requires only one station to transmit at a time and also data to be transmitted in blocks or frames. User data, destination and source address, error detection code and MAC control bits are included in every frame.

Each mobile station monitors the shared medium for frames with a destination address that matches its address and copies the frames addressed to itself. In fact, the MAC layer can be operated in two modes: the lower one, which is the distributed coordination function (DCF), and the upper one, which is the point coordination function (PCF).

2.6.2.1 Distributed Coordination Function (DCF)

The DCF mode is one of the most widely used methods to support the asynchronous data transfer in WLAN. This method does not use any central control such as access point, and then all the stations have to support and capable of using the DCF mode. It is based on a protocol named CSMA/CA (CSMA with Collision Avoidance protocol). This protocol uses both virtual and physical channel sensing. In IEEE 802.11, carrier sensing is performed at both the air interface, referred to as physical carrier sensing, and at the MAC sub layer, referred to as virtual carrier sensing [16]. The CSMA/CA uses two methods of operation. In the first method, a station might want to transmit information but first it checks the channel and if it is idle, it can start transmitting. In the case where a collision occurs, the colliding stations have to wait for a random time based on the Ethernet binary exponential backoff algorithm before trying again later. The other method of operation uses MACAW and virtual channel sensing.

2.6.2.2 Point Coordination Function (PCF)

The point coordination function is a centralized algorithm that provides contention-free service by polling mobile devices in turn. This method uses an access point to control the

activity and traffic in its cell. The access point polls the stations to see if they have any frames to send. Because the traffic is being controlled by the access point, no collisions ever happen in the PCF mode.

2.7 Different 802.11 Standard

There are several different IEEE 802.11 Standards. The most used and important standards are IEEE 802.11b, IEEE 802.11 a, IEEE802.11g, IEEE 802.11e and IEEE 802.11i.

2.7.1 IEEE 802.11b

The 802.11b standard was ratified in 1999 and it is an extension of the original version 802.11 DSSS scheme that provides data rates of 5.5 and 11 Mbps. It uses the same CSMA/CA media access method defined in the 802.11 standard. The 802.11b protocol uses complementary code keying (CCK) as its modulation technique which is a variation on CDMA that provides higher speed transmission. The typical indoor range for the standard is 90 meters at 1 Mbps and 30 meters at 11 Mbps. The limitations of it are the interference with other wireless technologies and security issues. The IEEE 802.11b standard is currently the most commonly used in commercial products.

2.7.2 IEEE 802.11a

The 802.11a standard was also ratified in 1999 and it operates in the 5 GHz band. It uses the same core protocol as the original one which is the IEEE 802.11.It uses an orthogonal frequency-division multiplexing (OFDM) also called multicarrier modulation that uses

multiple carrier signals at different frequencies, sending some of the bits on each channel [38]. However, the OFDM dedicates all of the sub channels to a single data source. The available data rates for this standard are: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps.

2.7.3 IEEE 802.11g

The IEEE 802.11g standard was ratified in June 2003 and it extends the data rates of 802.11b from 12 to 54 Mbps per channel. Just like the 802.11b, it operates in the 2.4 GHz range. The orthogonal frequency-division multiplexing (OFDM) is the modulation scheme used by the 802.11g for the data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps and reverts to CCK for 5.5 and 11 mbps and DSSS for 1 and 2 Mbps. With this standard, 802.11b devices will work when connected to an 802.11g access point, and 802.11g devices will work when connected to an 802.11b access point, in both cases using the lower 802.11b data rate [38].

2.7.4 IEEE 802.11e

The IEEE 802.11e revises the MAC layer with the idea of improving QoS (Quality of Service), MAC address enhancement and security mechanisms. It accommodates time-scheduling and polled communication during null periods when no other data is moving through the system. It also improves polling efficiency and channel robustness. These types of improvements and enhancements provide the quality necessary for services such as IP telephony and video streaming. A quality of service station is any base station implementing 802.11e [38].

2.7.5 IEEE 802.11i

The IEEE 802.11i standard defines security and authentication mechanisms at the MAC layer. This is the standard that provides the strongest security means for wireless LANs. It addresses the security issues of the WEP algorithm originally designed for the MAC layer of 802.11. The IEEE 802.11i addresses and improves three main security areas: authentication, key management and data transfer privacy [8]. All of these areas are extremely lacking in the WEP algorithm. Figure 2.4 presents a general overview of the 802.11i standard operation.

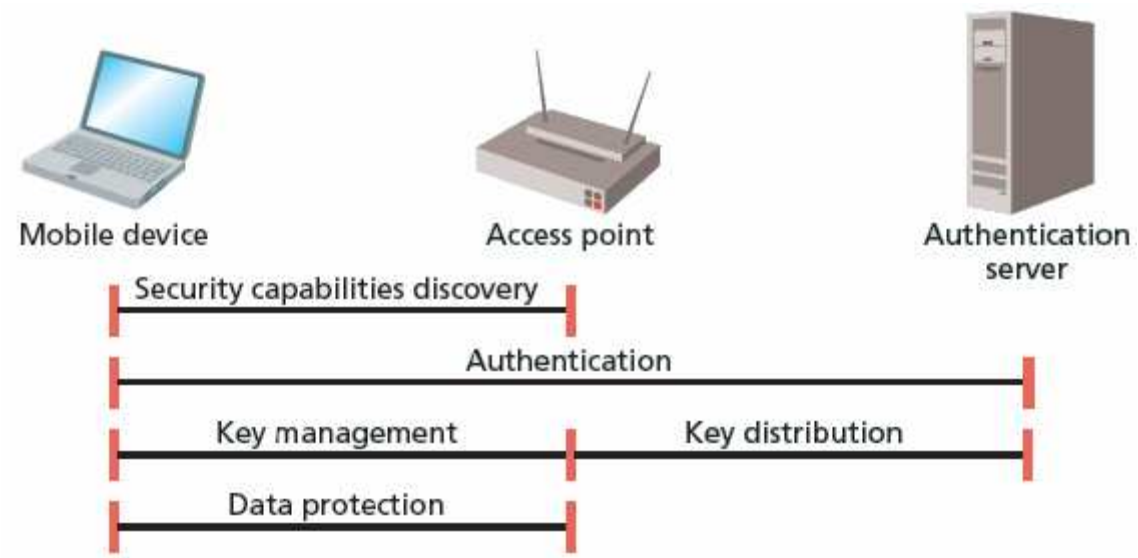

Figure 2.4: 802.11i operational phases [38]

The 802.11i standard improves authentication by requiring the use of an authentication server (RADIUS) and by defining a more robust authentication protocol. It also implements a two-way authentication method to prevent the man-in-the-middle attacks that have been so prevalent on 802.11b networks [8]. In fact, new keys have been introduced in the 802.11i standard to allow two-way authentication. The first is the master key (MK) which is a

symmetric key that facilitates authentication of a host with the authentication server. The pairwise master key (PMK) which is a private, symmetric key that is used by the client or user and access point to control access to the network. The authentication method of the 802.11i can be divided into two different paths. Firstly, the user to access point communication and secondly, the access point to authentication server communication.

The second area of improvement by the 802.11i is key management. Besides the MK and PMK mentioned earlier, there are other keys such as pairwise transient key (PTK), the key confirmation key (KCK), the key encryption key (KEK), the group transient key (GTK) and the temporal key (TK). With all of these keys, a reliable key management is needed for 802.11i. The 802.11i standard manages the keys as followed. Firstly, it uses the RADIUS server to pass the PMK from the authentication server to the access point. Secondly, it uses the PMK and a process known as 4-way handshake to derive and verify the PTK. Finally, it uses a procedure named group key handshake to send the GTK from the access point to the user. Using this simple process, 802.11i provides reliable and secure key management.

IEEE 802.11i provides the use of three different security encryption schemes to protect the privacy of users. They are identified as CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol), TKIP (Temporal Key Integrity Protocol) and WRAP (Wireless Robust Authenticated Protocol). CCMP uses the newly approved AES (Advanced Encryption Standard) encryption standard to encrypt data. It was designed from the beginning with the idea to handle packet-based communications and it provides both authenticity and privacy by encoding the plaintext before encrypting it. It has been shown that this method is probably secure but the drawback of it is that it requires a hardware

upgrade which makes it very expensive to use. That is why the two other protocols have been included into the 802.11i standard. The WRAP protocol is the original implementation of AES for wireless LANs. However, the methodologies being used in WARP were proved to be insecure, similar to the ones found in WEP. TKIP provides a data transfer solution that is intended to patch the holes discovered in WEP [8]. The problems addresses by the TKIP are data forgery, replay attacks, encryption misuse and key reuse. The most interesting point about the TKIP protocol is that it does not require a hardware upgrade; only a software upgrade is needed.

2.8 Benefits and Obstacles

The IEEE 802.11 standard provides several benefits to wireless users but at the same time, there are some obstacles that are related to it. In this section, we present the benefits and obstacles of the 802.11 standard.

2.8.1 Benefits

IEEE 802.11 provides four primary benefits to the users: User mobility, rapid installation, flexibility and scalability.

- **User mobility**: Wireless LANs allow users to move around with a laptop and still be able to access network resources and the internet without any need for a physical connection.
- **Rapid installation:** The time required to create a wireless LAN is definitely less than to create a wired LAN because the wireless LAN does not require cable installation or pulling them through walls or ceilings.

- **Flexibility:** 802.11 allows users to install and take down wireless LANs in location as necessary. The installation of a small wireless LAN for temporary needs such as a conference, trade show or normal meeting is very easily done.
- **Scalability:** WLAN topologies can be easily and quickly configured to meet specific application and installation needs and to scale from small peer to peer networks to very large enterprise networks that enable roaming over a broad area.

2.8.2 Obstacles

The IEEE 802.11 standard has faced several obstacles during its functioning. One of the main problems for the 802.11 is the interference with other devices or systems that are operated in the same frequency range such as Bluetooth, HomeRF and many other devices. A group called 802.15 is studying that problem to see how they can allow two systems with the same frequency range to operate and exchange information in the same area without any interference problems.

Another major problem of the 802.11 is security. Wireless LANs are uniquely vulnerable to both eavesdropping and unauthorized transmission because transmission is done over the air instead of using a decent cable. In fact, the IEEE 802.11 standard has provided certain ways to address security problems. Several security mechanisms have been developed and made available to wireless users. The 802.11 standard that provides the stronger security mechanism is the 802.11i.

2.9 Summary

This chapter reviews the wireless Local area network technology. Firstly, a brief overview and history of the IEEE 802.11 were given. The requirements needed to establish a wireless LAN were presented. Two different types of IEEE 802.11 operation mode were discussed: Infrastructure and Ad hoc mode. The important services needed for a wireless LAN were reviewed. The 802.11 protocol layers such as physical and MAC layers were discussed. Different IEEE 802.11 standards were presented. Finally, the benefits and obstacles related to the 802.11 standard were given.

CHAPTER 3

Wireless LAN Security

Wireless Local Area Networks have gained a tremendous and incredible popularity across the computer network market over the years. However, the threats and security fears associated with them have caused some network managers and administrator to avoid installing wireless LAN, regardless of the numerous benefits that they provide. Several manufacturers understand the fears, uncertainties and doubts caused by the security problems of the Wireless Local Area Network. They realize that coming up with a security measure to make the WLAN more secure would be a great asset and source of profit for them. Thus, they invest in research with the goal of coming up with a solution that satisfies the needs of the buyers when it comes to the security of the IEEE 802.11 WLAN. As results of these researches, several measures of security have been proposed by these manufacturers and some of them have been used by the IEEE 802.11 [3, 34, 2, 9 and 35].

In this chapter, the security issues related to the IEEE 802.11 are presented. Then, we review the different existing security mechanisms available in the market. Security threats and vulnerabilities associated with the WLAN are explored and several countermeasures to fight them are being proposed.

3.1 Goals of Wireless LAN Security

The main goal of the wireless LAN security is to protect the privacy of the clients just to make sure that an attacker is not able to access the network without any permission and

attack them. The following goals should be considered to implement effective wireless LAN security:

• Maintain the confidentiality of data as it is stored, processed or transmitted on a wireless LAN.

• Maintain the integrity of data as it is stored, processed or transmitted over a wireless local area network.

• Maintain the availability of data stored on a wireless LAN, as well as the ability to process and transmit the data in a timely fashion.

• Identify and ensure the identity of the sender and receiver of a message.

3.2 IEEE 802.11 Standard

This section presents the security mechanisms available in the IEEE 802.11 standard and their weaknesses. The keying management problems of the WEP and its weakness have been identified and the improvements to solve the security flaws are also presented.

3.2.1 802.11 Security Issues

Contrary to a wired network, a wireless LAN does not have a physical connection; it sends data over the air using radio waves that travel between client devices and base station. That means; any WLAN station within an access point service area can receive data transmitted to or from the access point. Thus, if not encrypted the data or packets transmitted can be viewed by anyone within the radio frequency range. The transmission mode of the WLAN has made it one of the most targeted network technologies for hackers [15]. However, the traditional

802.11 WLAN provides some security means to protect the network. These security means include the use of open or shared-key authentication and static wired equivalent privacy (WEP) keys. Their combination provides a level of access control and privacy but each one of them can be compromised. The following subsections describe the issues and security challenges being confronted by the IEEE 802.11.

3.2.1.1 Authentication

The IEEE 802.11 supports two types of client authentication methods: the open and shared-key authentication.

- *Open authentication method*: This is the default authentication method. When it is being used, it does not require an authentication at all and anybody can access the network resources at anytime. It involves a little more than supplying the correct service set ID (SSID). With open authentication, the use of WEP prevents the client from sending and receiving data from the access point, unless that he has the correct WEP key [15].
- *Shared-key authentication method*: In the use of this method, the access point sends a challenge text packet to the client station and the client has to know and encrypt it with the right WEP key and return it to the access point. If the client does not know the key or has a wrong key, he/she will not be able to authenticate to the system. This method is not really secure because an attacker can easily detect both the clear text challenge and the WEP key and uses them to access the resources of the network.

3.2.1.2 Key Management

Another type of key being used is the key management which is a static WEP key that can be either 40 bits or 128 bits of sizes. When this method is used, the static key has to be the same on every devices of the wireless LAN. The drawback of using it is that, if the static WEP key has been deciphered by an attacker, there is no way of knowing that.

3.2.1.3 WEP Protocol

One of the first security mechanisms proposed by the manufacturers is the Wired Equivalent Privacy (WEP) protocol. It is included as part of the 802.11 standard for encrypting WLAN traffic. It was designed to protect data at the link layer and prevent unauthorized access to 802.11 data frames [32]. It requires that all the communicating devices to share the same key. WEP can be used at both 40 or 128-bit depend on the need or the choices of the network administrator.

The WEP protocol uses the symmetric stream cipher RC4 algorithm invented by Ron Rivest to encrypt all network data traffic. In this algorithm, the same key is being used for the encryption and decryption processes. Figure 3.1 illustrates the functioning of the encryption method of the Wired Equivalent Privacy Protocol.

Based on Figure 3.1, The WEP protocol uses two processes that are applied to the plaintext data. The first one encrypts the plaintext and the second one protects it against any unauthorized modifications. Then, the secret key, 40 bits of size is combined with a 24 bits initialization vector (IV) resulting in a 64-bit total key size. The resulting key is placed into the pseudorandom number generator (PRNG). The PRNG (RC4) on its turn, outputs a

pseudorandom key sequence based on the input key. Then, the resulting sequence is being used for data encryption by doing a bitwise XOR.

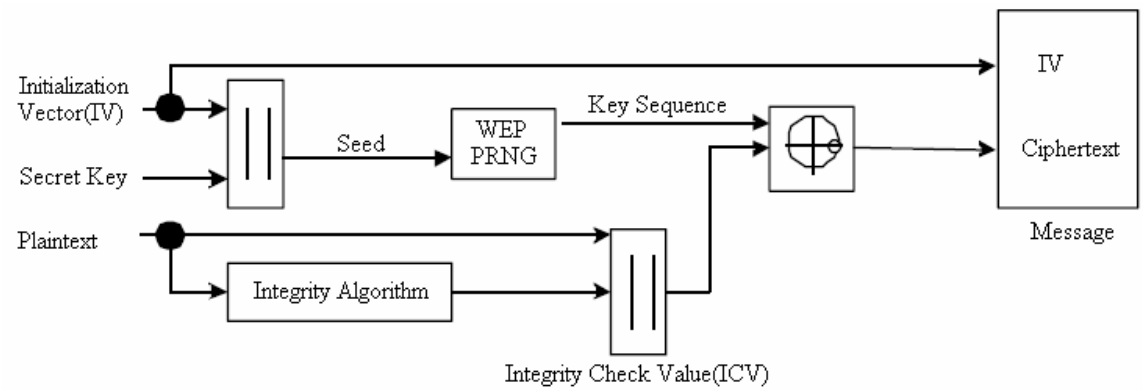

Figure 3.1: WEP Encryption [44]

In the decryption approach of the WEP shows in Figure 3.2, The IV (Initialization Vector) of the incoming message is used for the generation of the sequence key necessary for the decryption of the incoming message.

From Figure 3.2, the combination of the ciphertext and the proper key sequence produces the original plaintext and ICV (Integrity Check Value). The decryption is verified by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV to the ICV transmitted with the message. In case where the output ICV is different from the ICV transmitted, the receive message is in error and an error indication will be sent to the MAC management and to the sending station. Mobile clients with erroneous messages caused by the inability to decrypt will not be able to authenticate and access the network resources.

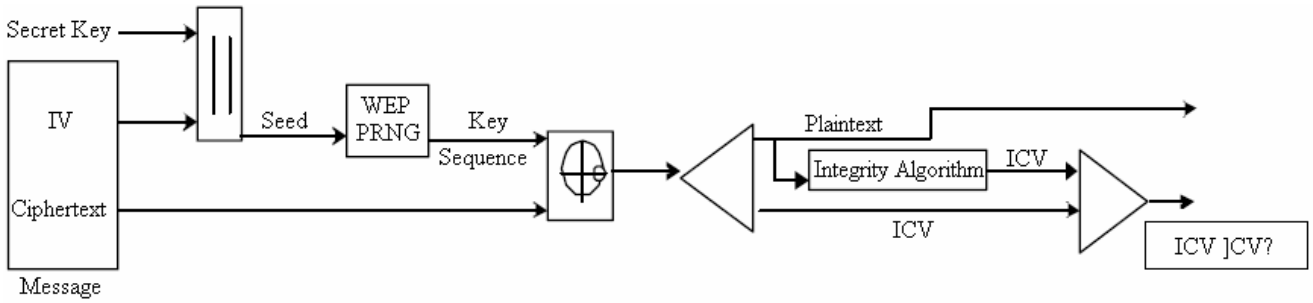

Figure 3.2: WEP Decryption [44]

In fact, the WEP protocol provides some security measures for the IEEE 802.11 but it still remains ineffective face to certain attacks. Several researches or documents prove the ineffectiveness of the WEP [7, 20, and 43].

3.2.2 WEP Security Problems

The WEP protocol provides some security means some security means for the IEEE 802.11. It decreases the effectiveness of the attacks but it is insufficient because it is vulnerable to various cryptographic attacks that reveal the shared key used to encrypt and authenticate data. It also uses a static key that requires manual rotation but practically it is even impossible to use it for a relatively small number of wireless clients. The vulnerabilities of the WEP protocol arise from various design flaws. Some of the flaws are the lack of key management processes, the generation of small initialization vectors (IV) and short encryption keys [34]. The initialization vector (IV) is a long sequence of pseudo random bytes generated by the WEP algorithm [8].

In [7], a group of researchers prove that the WEP protocol falls short of accomplishing its security goals. They stated that the reused of the keystream by the WEP can lead to several

attacks. One of the reason that keystream is reused coming from improper IV (Initialization Vector) management. Because the shared key generally changes very rarely, the reuse of IV often causes the reuse of the RC4 keystream. IVs are publicly transmitted and that's one of the reasons that make it easy for an attacker to detect it. Therefore, any reuse of old IV values exposes the system to keystream reuse attack. From the same paper, they also proved that, when the IV of an encrypted message is discovered, it is very easy to recover its plaintext by using various methods of attacks. Once an attacker intercepts the plaintext of a message, he learns the value of the key stream used to encrypt the message. Then, he/she can use this keystream to decrypt other messages that use the same IV. Over the time, the attacker will be able to build a table of keystreams corresponding to each IV or even a full decryption dictionary to break up the security encryption provided by the WEP protocol. They also claimed that the checksum method being used by the WEP protocol to ensure that packets do not modify while transmission is inefficient. They proved that messages can be modified in transit without detection, in violation of the security goals. Most of these claims about the safety issues of the WEP protocol were also supported by other researchers in [43 and 2].

Another group of researchers composed of Fluhrer, Mantin and Shamir discovered several shortcomings and problems with the RC4 key-scheduling algorithm being used by the WEP. The attack illustrated in [20] focuses on a large class of weak initialization vectors (IV) that can be generated by the RC4 algorithm and brings up several methods to be used to break up the security key by using certain patterns in the initialization vectors. The attack being used is known as FMS attack and it is completely passive. This type of attacks discusses the

theoretical derivation of a WEP key in a range of 100,000 to 1,000,000 packets encrypted using the same key [15].

They are several tools out there on the wireless market that make it really easy for a hacker to attack a wireless system. One of the most popular one is Airopeek which is a program from WildPackets that includes the capability to penetrate the WEP key and provides an attacker with plaintext decodes. Another popular tool based on the FMS attack is the Air Snort which can also help an attacker in his attacks against wireless systems.

Based on these research results, it is obvious that the security level provided by the WEP protocol is ineffective. Therefore, new solutions and enhancements of this protocol are needed.

3.2.3 WEP Improvements

The security measures provided in the 802.11 standards are all vulnerable to attacks. Therefore, systems should deploy additional higher-level security mechanisms such as access control, end-to-end encryption, password protection, authentication, virtual private networks, or firewalls and assume the use of WEP as a very basic layer of security only [3]. The IEEE 802.11 committee creates a task group denominated 802.11i [41] to enhance the security and authentication mechanism of the current 802.11. Their work has resulted in:

- The improvement of the WEP with the *Temporal Key Integrity Protocol* (TKIP
- The deployment of *Enhanced Security Network* (ESN) solution
- The substitution of the 802.11 standard with 802.1x authentication and key

3.2.3.1 WEP Improvement with TKIP

The Temporal Key Integrity Protocol (TKIP) [34, 9], a new security standard also named WEP2 was proposed by the IEEE 802.11i working group. It is an immediate replacement for WEP that fixes the very well-known problem of small initialization vectors (IV) and short encryption keys. It uses RC4, the same symmetric encryption algorithm as WEP and 48-bit vectors, which limit existing cryptographic attacks against WEP. It solves the short-key problem of the WEP by generating longer keys. In case of undetected WEP modification attacks, TKIP uses the Message Integrity Code (MIC) technique to fix the security problems. The Michael message integrity check technique keeps messages from being replayed or modified by an attacker. TKIP is not an ideal operation because it is not being accepted by all existing applications. Still, it can be used as a more robust solution to replace the Wired Equivalent Privacy protocol (WEP).

3.2.3.2 ESN Solutions Proposed

The ESN solution is focused on stronger encryption for data over wireless networks by using a non-proprietary 128-bit encryption solution, which support the *advanced encryption standard* (AES) algorithm [44]. HMAC4-SHA1-128 can be used as the hashing function to support message authentication with AES.

3.2.3.3 Substitution of the 802.11 Standard with 802.1x

One of the alternatives to improve the WLAN security is to develop a framework for providing centralized authentication and dynamic key distribution. This alternative is based

on the IEEE 802.11 Task Group “i” end-to-end framework using 802.1x. The IEEE 802.1x is an authentication standard for 802-based LANs using port-based network access control. The three main elements of an 802.1x approach follow [15]:

- Mutual authentication between client and authentication server (Remote Access Dial-In User Service [RADIUS]).
- Encryption keys dynamically derived after authentication.
- Centralized policy control, where session time-out triggers reauthentication and new encryption key generation.

3.3 Wireless Security Threats and Attacks

The security solutions decrease the chances or opportunities for an attacker to penetrate the WLAN but still most of them are vulnerable to attacks. The attacks that allow unauthorized users to get access to the system are divided into: active and passive attacks. Figure 3.3 shows several types of attacks and security threats that can be used by an attacker to attack a wireless LAN.

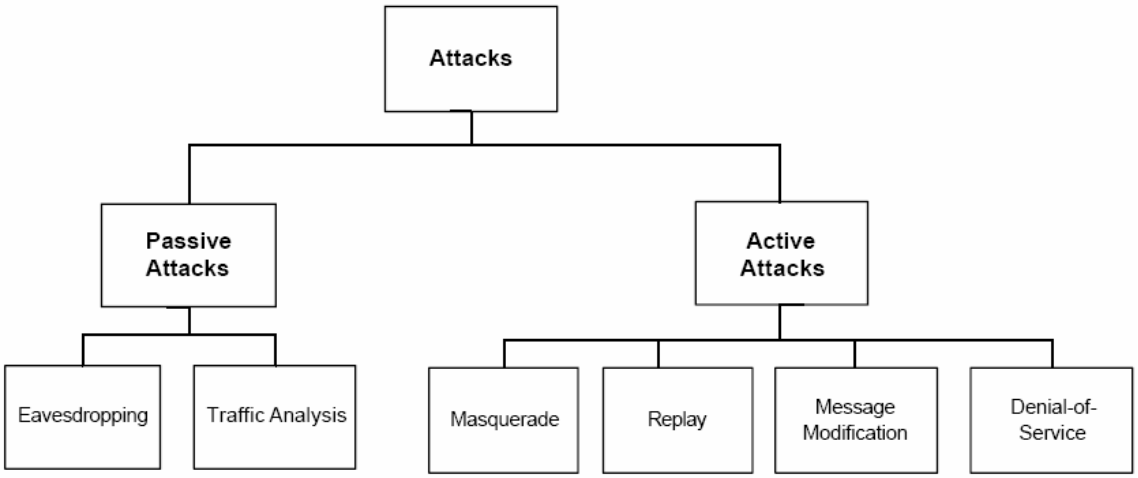

Figure 3.3: Security Threats and Attacks [26]

3.3.1 Active Attacks

This is the type of attack in which the attacker or hacker gains access to a network and make some modifications to the resources or to the messages being transmitted over this network. It is possible to detect this type of attack but in some cases, it may not be preventable. There are four different types of active attacks: masquerading, replay, message modification and denial-of-service. These attacks are defined below.

- *Masquerading*: The attacker uses a sniffer to capture user name and password of an authorized user to get access to the network or to gain certain unauthorized privileges. He/She can also place his/her own access point into the network and tricks unwitting users to reveal passwords.
- *Replay*: The attacker listens and monitors the traffic between two parties (passive attack) and retransmits the message as one of the legitimate user.
- *Message Modification*: The attacker changes the contents of a legitimate message by deleting, adding to, changing or reordering it.
- *Denial-of-service*: The attacker prevents or prohibits the normal use, functioning and management of a network by injecting a large amount of traffic into the network. The technical term for it is jamming or flooding the frequency of the network. The legitimate traffic gets jammed because illegitimate traffic overwhelms the frequencies, and legitimate traffic can not get through.

3.3.2 Passive Attacks

This is an attack in which an attacker or hacker gets access to a network but does not change or makes any modifications to the resources of the network. There are two types of passive attacks: Eavesdropping and Traffic analysis. These two types of attacks are described below.

- *Eavesdropping*: In this type of attack, the attacker uses several tools to listen or monitor the transmissions for message content. An example of that is a hacker walking or driving around a neighborhood with his/her laptop and listening or monitoring traffic within two workstations or a wireless handset and a base station.
- *Traffic Analysis*: The attacker monitors the traffic of a network and obtains a lot of information about this network. Once the attacker obtains these information, he/she can analyze them statistically and find himself a way to access the network. He/She can also build an attack dictionary by using the statistics obtained from the monitoring session.

Various security algorithms have been invented and some of them provide good security features against these attacks, especially the Advanced Encryption Standard (AES) Algorithm which took an attacker an infinite number of years by using current computing capability to decrypt it [37]. In fact, several countermeasures need to be taken or applied to protect Wireless LAN against the possible attacks.

3.4 Countermeasures

Several countermeasures can be used to address or fight specific attacks and threats related to the Wireless LANs. Certain countermeasures involved: the change of SSID, the usage of the

MAC authentication security mean and the WEP authentication protocol built in of most of the access point. This section discusses different basic security measures to prevent casual attacks.

3.4.1 Updating Default Passwords

Usually, the access point or wireless devices come with a default password or without any password. Then, it is the responsibility of the administrator of the network to change the default password or to come up with a new password to protect the network against certain threats or attacks.

3.4.2 Changing default SSID

The access point should not use the default SSID provided by the manufacturer because most of them have published on the net and they are well known by the attackers. Then, the default SSID needs to be changed at the first use and configuration of the access point to avoid easy access by unauthorized users. Even though an equipped attacker can capture the SSID over the wireless interface, it has to be changed just to prevent unequipped users or attackers to access the resources of the network.

3.4.3 Enable MAC Authentication

A MAC address is a hardware address that uniquely identifies each computer or attached device on a network. Networks use the MAC address to regulate communications between different computer network interface cards (NICs). The IEEE 802.11 WLAN used the Media

Access Control (MAC) address filtering to increase the security of the network. When it is used or enabled as security measure, the clients are authorized by their unique device MAC address. In that case, clients who want to use the network have to take their wireless card to the network administrator so it can be registered, then they will have access to the network. This technique increases the security means but it still have some defections because an attacker can easily determine the MAC address authorized by a wireless network via eavesdropping and programs his/her wireless card by using some software to enter the desired MAC address and get access to the network. The MAC authentication method is not completely secure but it is better to enable the MAC authentication method instead of not using any security means.

3.4.4 WEP Authentication and Encryption

The wireless equipments or access point are not shipped out with the WEP security protocol activated. By default, the WEP encryption is disabled. It is the responsibility of the network administrator to activate the WEP protocol and to use the shared authentication method instead of open system as basic protection of the wireless LAN. As mentioned before, the WEP protocol supports two sizes of encryption key: 40 or 128 bits. It is important to use the strongest encryption method (128 bits) available as long as it is not affected the network. However, as we have seen previously, the WEP is vulnerable to several attacks no matter what the size of the key is (Section 3.1.2).

3.4.5 Default Channel Modification

To avoid Denial of Service (DoS) attacks and radio interference between two access points in close proximity, the setting of the default channel must be modified to operate in different frequency band. Once that is being done, it reduces the chances of having interference problem.

3.4.6 DHCP Server Usage

For certain wireless LAN, the connection of a user to the network is being done automatically by using a Dynamic Host Control Protocol (DHCP) server. The DHCP server automatically assigns or provides IP addresses to the clients that are associated with an Access Point. The use of a DHCP server provides users the advantages of roaming or establishing ad-hoc networks. The treat with the DHCP server is that a malicious user or an attacker could easily get unauthorized access on the network through the use of a portable computer with a wireless network interface card. Since the DHCP server will not necessary know which wireless devices have access, it will automatically assign the laptop a valid IP address. Then, the attacker has access to the network.

Several solutions can be used to fix the DHCP unsecured problems. Firstly, these problems can be solved by assigning a static IP address to each client of the WLAN instead of using DHCP server. But, this method can be practically used for small networks and it also negates certain advantages of the network such as: roaming and the establishment of ad-hoc networks. Another possible solution is to implement the DHCP server inside of a wired network's firewall that grants access to a wireless network located outside of the wired network's

firewall. The last solution is to use access point with integrated firewalls. In fact, a network administrator should evaluate the need for a DHCP server by taking into consideration the size of their network.

3.5 Additional Security Extensions

So far, several security mechanisms and methods have been presented but they are all vulnerable to attacks. Thus, additional means and extensions of security are needed. This section presents the strongest security mechanisms for wireless LANs.

3.5.1 IPSec

IPSec is a framework of open standards for ensuring secure private communications over IP networks [15]. It has a practical application to secure wireless LANs by overlapping IPSec on top of cleartext 802.11 wireless traffic. When IPSec is used in a WLAN, an IPSec client is placed on every PC connected to the wireless network and the user is required to establish an IPSec tunnel to route any traffic to the wired network, in case of existence of a backbone wired network.

IPSec is used to provide confidentiality of IP traffic, as well as authentication and anti-replay capabilities. For the confidentiality achievement process, IPSec uses the Data Encryption Standard (DES) called Triple DES (3DES) or the new Advanced Encryption Standard (AES). Two major architectures and corresponding packet types are supported by IPSec:

- Encapsulating Security Payload (ESP) header which provides privacy, authenticity and integrity.

- Authentication Header (AH) that provides integrity and authentication only for packets.

The IPSec can operate in two different modes; the *transport mode* which can secure an existing IP packet from source to destination and the *tunnel mode* that can put an existing IP packet inside a new IP packet that is sent to a tunnel end point in the IPSec format, typically between a pair of firewalls/security gateways over an untrusted network. Figure 3.4 shows both, the operational tunnel mode of the IPSec.

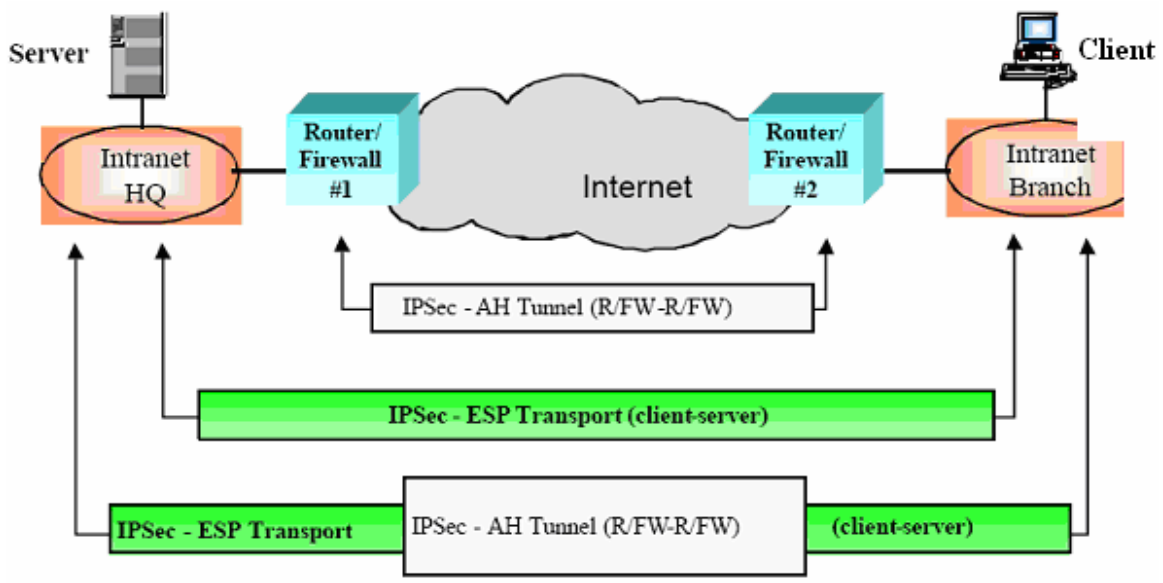

Figure 3.4: IPSec Operational Tunnel Modes [44]

In fact, IPSec is used primarily for data confidentiality and device authentication. Some extensions to the standard allow for user authentication and authorization to occur as part of the IPSec process.

3.5.2 Robust Security Network Protocol

The Robust Security Network (RSN) also known as the 802.1x standard is another security mechanism used to restrict access to unauthorized user to the wireless network by centralizing authentication of the WLAN users and mitigates some of the weaknesses of the WEP. It is essentially a standard for sending authentication messages (keys) between an 802.11 access point and a centralized authentication server, usually a RADIUS (Remote Authentication Dial-in User Service) server [9]. The protocol used in the RSN method is called Extensible Authentication Protocol (EAP).

3.5.2.1 Extensible Authentication Protocol

The Extensible Authentication Protocol (EAP) was originally created as an extension to the Point-to-Point Protocol (PPP) that allows for development of arbitrary network access authentication methods and provides centralized authentication and dynamic key distribution. When EAP is used as security mechanism in a WLAN environment, a client that associates with an access point can not gain access to the network until he/she performs a network logon. After association, the client performs mutual authentication into the networks by exchanging EAP messages with the access point or the RADIUS server of the WLAN, verifying the RADIUS server credentials and vice versa. An EAP supplicant is used on the client machine to obtain the user credentials such as: user ID and password, or digital certificate. If the mutual authentication between client and server is successful, the RADIUS server and client then derive a client-specific WEP key to be used by the client for the current

logon session. In the EAP authentication process, user passwords and session keys are never transmitted in the clear, over the wireless link.

In fact, EAP provides three significant benefits when it comes to the 802.11 security:

- The first benefit provided is the mutual authentication scheme, as described previously. This scheme eliminates completely the types of attacks named “man-in-the-middle (MITM) attacks”.
- The second one is the centralized management and distribution of encryption keys. Even tough the WEP implementation of RC4 had no security flaws; there would still be the administrative difficulty of distributing static keys to all the access points and clients in the network. Each time a wireless device got lost, the network would need to be rekeyed to prevent the lost system from gaining unauthorized access [15].
- The third benefit is the ability that the EAP security mechanism has to define centralized policy control.

Several and different types of EAP are available today for user authentication over either wired or wireless network. Current available EAP types include: EAP-TLS, EAP-TTLS, LEAP, PEAP and EAP MD-5.

3.5.2.1.1 EAP-TLS (Transport Layer Security)

This is one of the most common implementation being used. It is highly secure because it requires asymmetric public and private keys on the client and server side to have the authentication phase going on. It takes a lot of steps to deploy the EAP-TLS within an organization and it is not a simple task. Figure 3.5 illustrates the steps that are being taking

place into the wireless LAN between a client, the access point and the RADIUS server for authentication process.

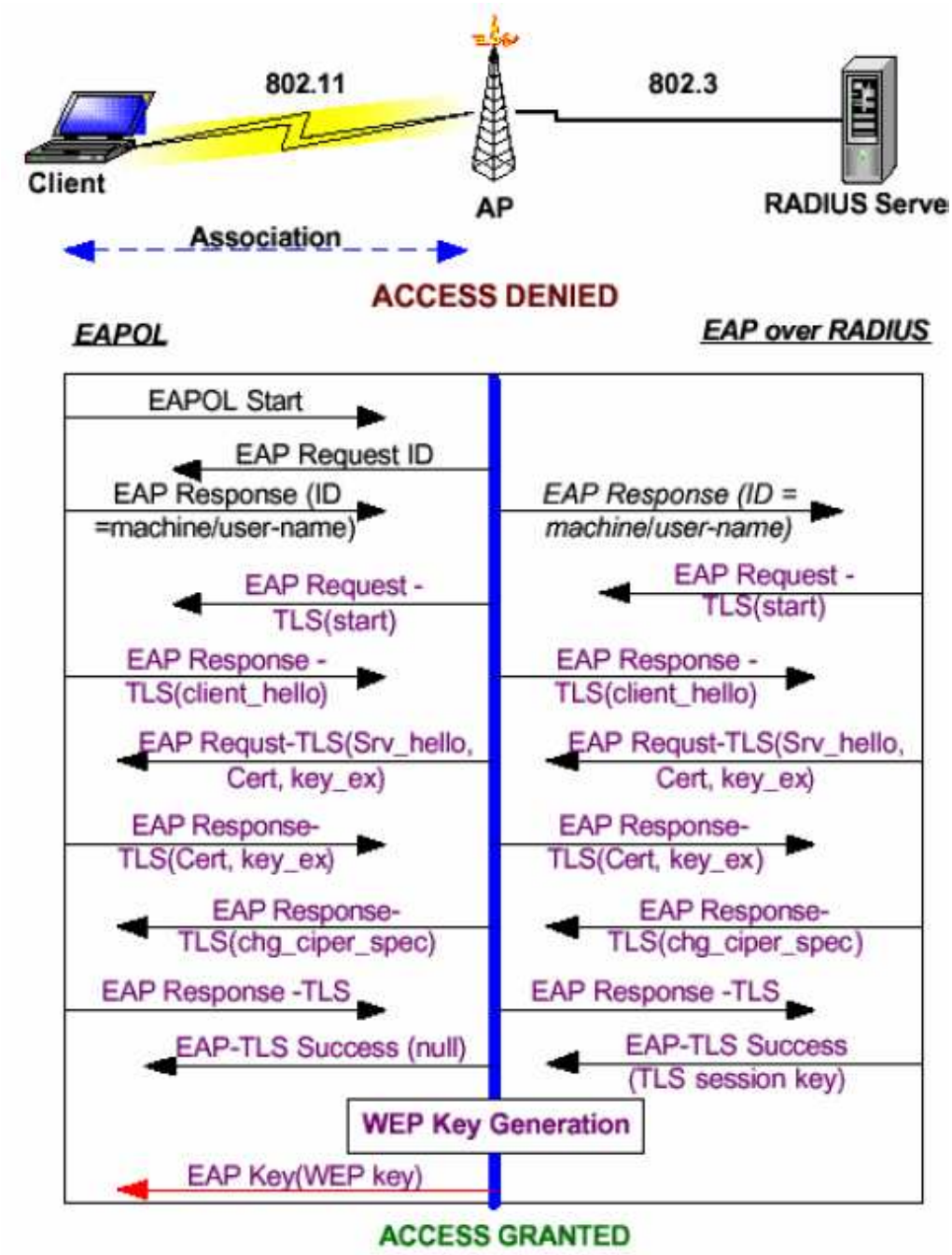

Figure 3.5: EAP-TLS Authentication Process [33]

3.5.2.1.2 EAP-TTLS (Tunnel Transport Layer Security)

This version of EAP developed by Funk Software requires a certificate only on the authentication of the server, which making it easier to deploy and almost as secure as EAP-TLS.

3.5.2.1.3 EAP-MD5

This is the least secure version and it does not support dynamic WEP key rotation. It is susceptible to dictionary attacks because it uses user name and password for authentication. Figure 3.6 illustrates the authentication process steps for EAP-MD5.

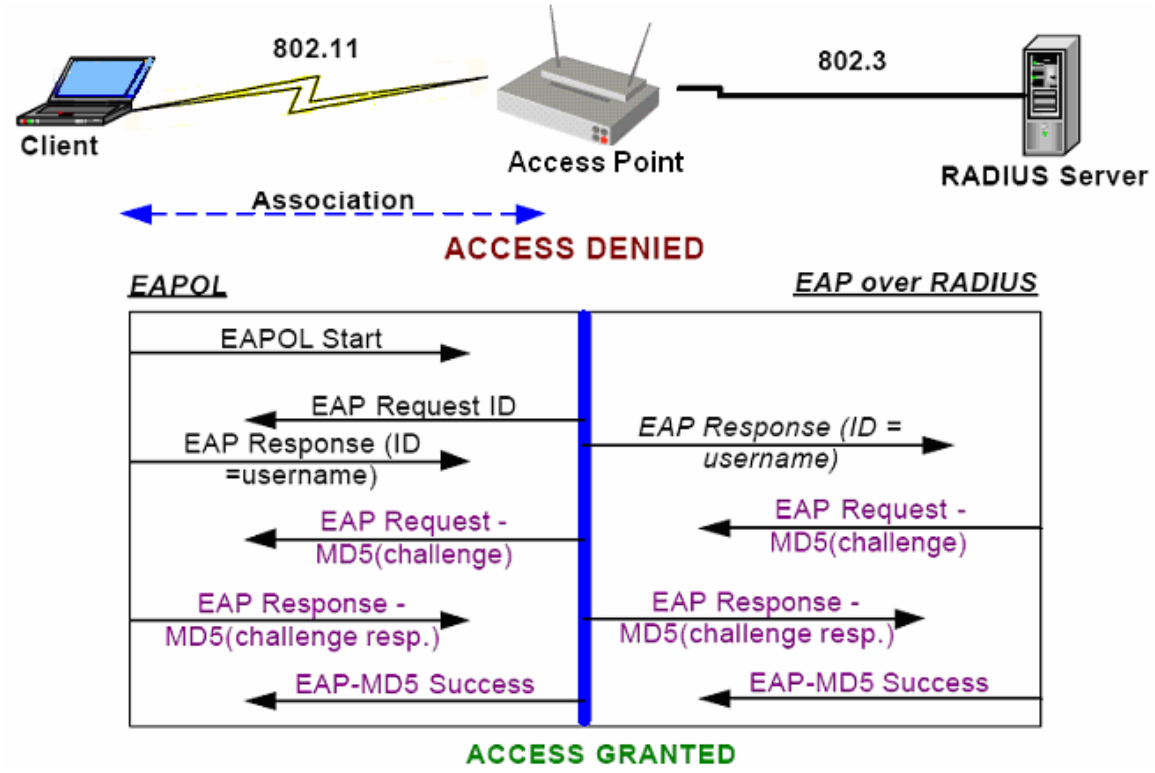

Figure 3.6: EAP-MD5 Authentication Process [44]

3.5.2.1.4 LEAP (Lightweight EAP)

This is the Cisco's version of EAP, which initially worked only with Cisco Access Point but is now being supported more widely. When it is being used as security mechanism, mutual authentication relies on a shared secret, the user's logon and password, which is known by the client and the network. The RADIUS server sends an authentication challenge to the client. The client uses a one-way hash of the user-supplied password to fashion a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, enabling the client to authenticate the RADIUS server. When this is complete, an EAP-Success message is sent to the client and both the client and the RADIUS server derive the dynamic WEP key [15].

3.5.2.1.5 PEAP (Protected EAP)

PEAP is a similar and more secure version of EAP co-developed by Cisco and Microsoft. It was designed with the purpose to resolve the problem in which, the entire EAP conversation might be sent as clear text and an attacker with access to the media can inject packets into the conversation or capture the EAP messages from a successful authentication for offline analysis [17]. PEAP solves this problem by first creating a secure channel that is both encrypted and integrity-protected with TLS.

3.5.2.2 Wifi Protected Access (WPA)

WiFi Protected Access (WPA) is also a security mechanism that uses 802.1x authentication combines with Temporal Key Integrity Protocol (TKIP) encryption to make Wireless LAN more secure against attacks. The TKIP protocol includes key mixing function, a message integrity check feature and a re-keying mechanism that rotates keys faster than they can be cracked by hackers. Many security experts and researchers believe that the combination of TKIP and 802.1x mechanisms should provide adequate security for most WLAN users.

3.6 Summary

This chapter presents an overview of the security mechanisms that can be used to protect a wireless LAN. The WEP and other basics security means used to protect the WLAN were revealed insecure. The threats and security issues that can affect the WLAN were also given. These threats were divided into active and passive threats. Faced to the WLAN security problems, several countermeasures that need to be taken to protect the wireless network were also presented. At the end of this chapter, other security mechanisms such as EAP, PEAP and WPA (Wifi Protected Access) were also presented.

CHAPTER 4
Wireless LAN Performance

In this chapter, we first explain the importance of performance evaluation or performance study of a network. Then, we provide an overview of the performance metrics and variables necessary to measure the performance of a network. We also review previous wireless LAN performance analysis work done one the IEEE 802.11 standard.

4.1 Performance Evaluation

Selecting a specific security protocol or mechanism to protect a wireless local area network that will provide the optimum service to users requires up-front analysis and knowledge. The security mechanisms are very important and useful for the protection of the network, but if they are not used properly or choose adequately, they can actually decrease the productivity or performance of the network. For example, a wireless LAN can provide a mean to streamline information processing and eliminate redundancies, but it may also deter users from logging on because of link or security mechanism problems. To the common users, data communications, security mechanisms, wire and wireless LANs are a black hole of protocols because they do not have any knowledge about them. To alleviate these problems, the users should be educated about the basics of communication, security mechanisms and WLANs and be provided with metrics and tools with which they can adequately face the myriad issues and select a security mechanism to protect their network based on their needs.

Another option is that, an investigation can be performed by researcher more knowledgeable about the security field to come up with a solution that provides a tradeoff between performance and security when it comes to wireless LANs. Once the researchers obtain some results and come up with some conclusions about the best way to protect the WLANs based on security and performance tradeoff, they can advice the normal users on making decision about which security mechanism or protocols they have to use to protect their network. Then, when it comes to the choice of a security mechanism to protect a wireless LAN, a performance evaluation or study is needed to be done.

4.2 Performance Metrics

When it comes to performance evaluation of a computer network or a wireless LAN, one of the major things we have to take in consideration is the performance metrics that we are going to use for our study. Sometimes, it might be a little difficult to make a choice because the metrics can be qualitative or quantitative. But, to be scientific and precise in our performance study, we must focus on measurable quantitative qualities of a network or a WLAN under study. There are many possible choices for measuring performance, but when it comes to wireless LAN or any type of computers networks, the most common performance metrics are: response time (sometimes called speed, reaction time), throughput (sometimes called capacity or bandwidth), accuracy, utilization (sometimes referred to as efficiency or business), reliability and cost/performance ratio.

4.2.1 Response Time

When it comes to wireless LAN, the response time is the time required for traffic to travel between two points or the time interval between a user's request for service and the services return of results, as shown in Figure 4.1. This is the best measure that can help and used to determine the effectiveness of a network. No matter what the reason of the slow response, users will always be frustrated as a result of delayed traffic. Certain factors that can affect the response time are: network congestion, security protocols or mechanisms, size of packets and traffic types.

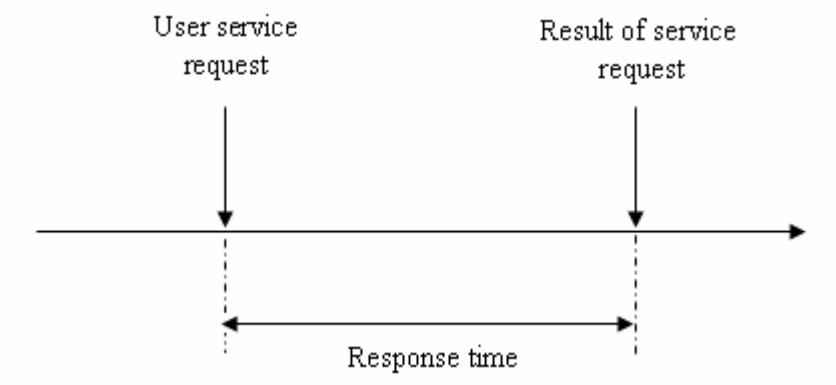

Figure 4.1: Typical Response Time Measurement [21]

In fact, whenever possible, the response time should be measured as it appears to users. A user perceives response as the time from when they press enter or click on a button until the screen displays [37]. This elapsed time includes the time required for each network device, the user workstation and the destination server to process the traffic.

4.2.2 Throughput

The throughput is a measure of the number of items or amount of data transmitted over a wired or wireless LAN in a predefined period of time. For network and communications systems, it can be measured in terms of MPS for messages per second, BPS for bits per second or PPS for packets per second. Just like for the response time, the throughput will increase as additional load is placed on the system or into the network [21]. However, unlike the response time, there will be a point in which the throughput will maximize and possibly begin to degrade, as shown in Figure 4.2. If we take a closer look at this figure, we notice that the throughput seems to increase when the load is increasing and then decreases as a saturation point is reached.

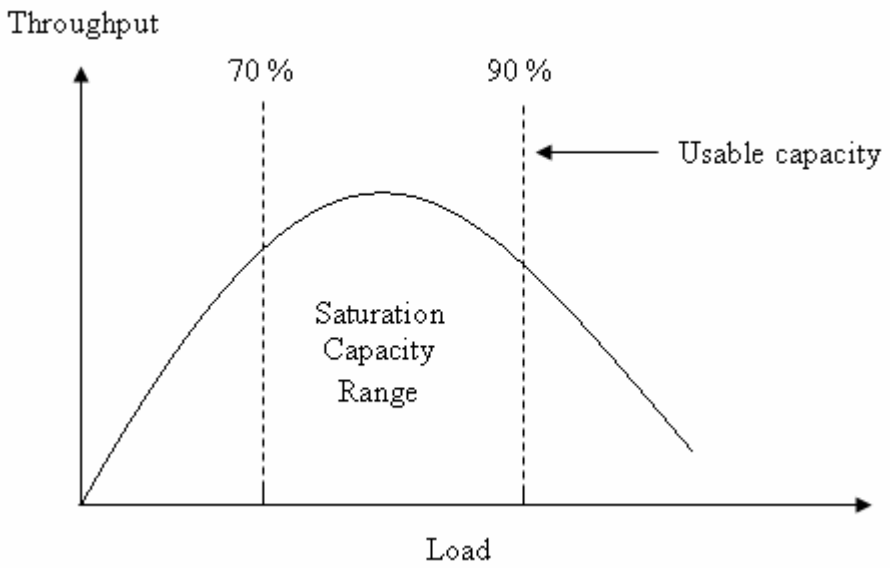

Figure 4.2: Throughput curves versus load quantity [21]

In a wireless LAN, most of the time when the load decreases, the throughput increases and when the load increases, the throughput decreases.

4.2.3 Error Rate

This is the measure of interface traffic that does not result in error over a network. It can be expressed in terms of a percentage that compares the success rate to total packet rate over a period of time [14]. To be able to obtain the accuracy of a network, it is very important to calculate the error rate for the number of packets coming into the network. For example, if 4 out of every 100 packets result in error, the error rate would be 4 % and the accuracy rate would be 96 %. Certain aspects that can cause errors are: electrical and frequency interference, faulty hardware or software.

4.2.4 Utilization, Reliability and Availability

The utilization of a resource over a network is a measure of how busy the resource is. It can be computed or calculated as the fraction of time the resource is busy servicing clients divided by the entire time period:

$$\text{Utilization} = \text{time busy} / (\text{time busy} + \text{time idle})$$

Utilization is a very important measure for a system administrator because through its value, he/she can understand if the network is very saturated or unsaturated. Some other important measures in analyzing a network system are: reliability and availability. Reliability is a measure of the probability of errors or a typical time between errors. The availability of a network is measured in term of its reliability. It is the measure of time that a network system or resources of a network is available to a user. This is one of the primary metrics being used by network managers [14].

4.3 Wireless LAN Performance

When it comes to the development or establishment of a wireless LAN, security is a very important issue; every decision must be taken with security in mind. Certainly, one or the combination of existing security mechanisms must be used to protect the network. However, the use of these security mechanisms can affect the performance of the network. Then, a performance evaluation study of the WLAN when security protocols are being used is needed. In this section, the results of some previous studies being done on the performance of the WLANs are presented.

In [16], Balachandran et al. presented and analyzed user behavior and network performance in a public-area wireless network using a workload captured at an ACM conference. They concluded that the load distribution in terms of bandwidth across the access points is highly uneven and not very well correlated with the number of users associated with the access points. They also concluded that the existing access point load balancing algorithms that attempt to balance access point load according to the number of users alone are inefficient or can perform poorly. They also admitted that such balancing algorithms would benefit from the additional complexity of balancing users across access points according to their actual bandwidth requirements.

Bing measured the network performance of two commercial IEEE 802.11 standards at the medium access control sub-layer in [27]. Several tests were conducted on the WLANs by taking in considerations important performance metrics such as response time and throughput under various network loads. The results proved that the buffering and fragmentation of data frames can seriously influence the performance of an 802.11 wireless LAN. Even though the

length of a data frame and the bit rate of the wireless transceiver also affect the wireless LANs transmission capabilities, its performance is generally unaffected by the type of frame addressing and the use of reservation frames such as RTS and CTS.

In [12], the performance of an 802.11a wireless LAN was measured in terms of data link rate and throughput by Chen et al. Comparing to the 802.11b standard, the results showed that the 802.11a provides not only higher end-user speeds but also allows reductions in WLAN deployment cost. It is way cheaper to deploy a wireless LAN using the IEEE 802.11a than the 802.11b.

An empirical characterization of the instantaneous throughput in 802.11b WLANs as a function of number of stations sharing the access point was presented in [42]. The results proved that as the number of stations increases, the throughput of the network decreases and its variance increases.

In [25], Kamerman et al. measured the throughput of an 802.11 WLANs respecting to different types of overhead. The impact of several sources of overhead was modeled. Sources included gap time, preamble, physical layer, MAC layer and TCP/IP header fields, ACK and request frames. After measurement of the net throughput and detailed monitoring of actual exchange of frames, this modeling was refined. A close fit was found between the results for IEEE 802.11b obtained from this model and as measured using currently available 2.4 GHz products.

Wong [44] evaluated the impact of different security mechanisms over the performance of an 802.11 wireless network by measuring the throughput and response time of HTTP and FTP

traffic types in an unsaturated simple point-to-point architecture. The results showed that different security mechanisms degraded the performance of the network in different ways.

In a study [3] based on [44], Baghaei evaluated the effect of several security mechanisms on the performance of an IEEE 802.11b wireless LAN by measuring the throughput and response time of UDP and TCP traffic types for saturated and unsaturated network. In this study, the traffic was generated by an IP traffic generator for a single cell network composed of three clients and a server. The results proved that the more secure is the network, the lower is the performance.

Duchamp and Reynolds [18] evaluated the performance of a high-speed commercial spread-spectrum wireless LAN that uses the CSMA/CA multiple-access strategy. In their study, they measured specifically throughput, packet loss rates, range and patterns of errors within packets. They concluded that CSMA/CA was quite successful in allocating bandwidth under stress, but that packet capture rate degraded very quickly once the LAN's effective range was exceeded.

4.4 Summary

This chapter starts by explaining the importance of a performance study before making decisions on any security mechanism to use for a WLAN. It goes on to cover several performance metrics such as: response time, throughput, error rate, utilization, reliability and availability. Then, prior studies based on the performance of wireless LAN are also surveyed. The previous study of the impact of security on performance concluded that, the higher the security level, the lower the performance.

CHAPTER 5
Experiment Methodology

Our main objective in this research is to study and evaluate the impact of several security mechanisms on the performance of an 802.11g WLAN. Just like for most of the experimental research work, a methodology and some procedures need to be followed. In this chapter, we present the methodologies and procedures being followed during our research work.

5.1 Wireless LAN Setup

In our experiment, we used Windows-based operating systems because Windows XP and Windows 2003 Server have a built in implementation of the IEEE 802.11 security mechanisms and 802.1x authentication protocol such as: EAP and PEAP. Figure 5.1 shows a graphical setup representation of our single cell network. The experiments were conducted using the following equipment and software:

One Server

- Windows 2003 server
- 3.20 GHz, 1GB RAM and an RJ-45 cable
- IP Traffic Generator and Ethereal software

Three Clients

- Windows XP Professional
- Pentium M processor, 1.70 GHz, 768 MB of RAM, Intel and Linksys Wireless LAN Cards

- IP Traffic Generator software

Access Point

- Cisco Aironet 1130AG Series

Switching Hub

- Linksys EtherFast 3116 16-port 10/100 Ethernet Switch

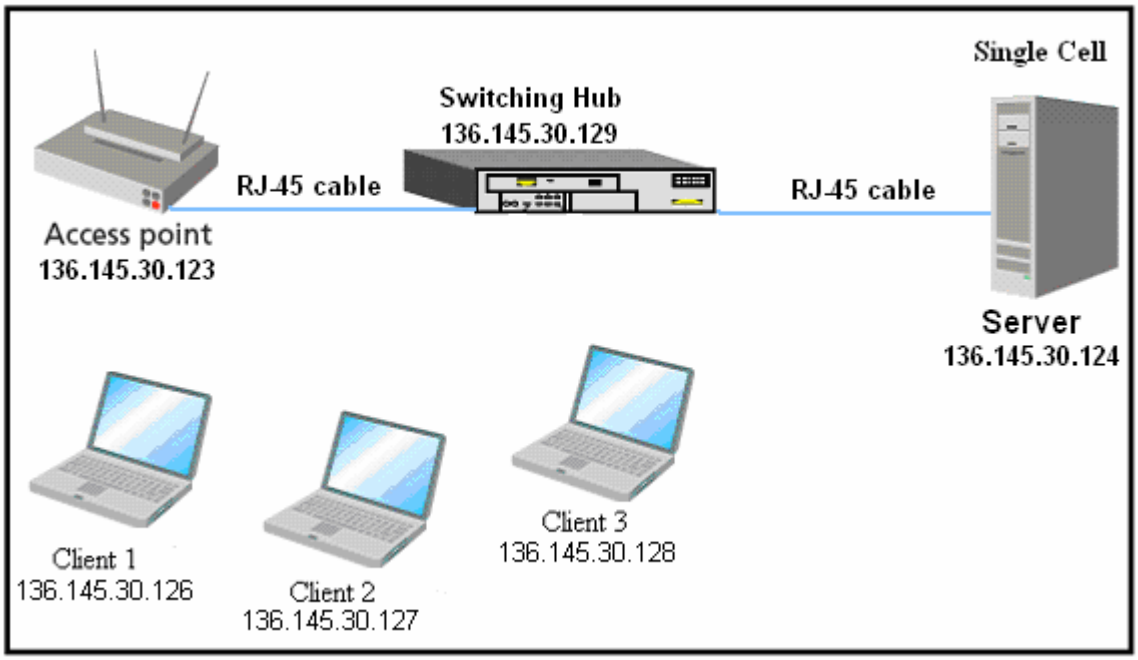

Figure 5.1: Network Topology Setup

In our experiment, we used a single cell that included one server, three clients, one access point and one switch. The network traffic was generated by the IP traffic generator software [24] installed on both the server and the clients. The bandwidth or the transmission speed of the ethernet connection between the Access Point and the server was equal to 100 Mbps. Between the access point and the clients, the bandwidth was 11 Mbps. During the

experimentation, the results for throughput and response time were collected from the server by using a sniffer or network tool named *Ethereal* [19]. The section that follows presents the security mechanisms that were used during our experiment.

5.2 Security Mechanisms

The following ten security mechanisms available from both IEEE 802.11 and IEEE 802.1x standards were used in our experimentation:

1. **No security with SSID:** this is the default security setting provided by vendors. There is no security mechanism activated but an SSID is created and only the client with the right SSID will be able to connect to the network.

2. **MAC address authentication:** this mechanism provides MAC address authentication carried out at the AP.

3. **WEP authentication:** the shared key authentication method specified in the 802.11 standard is used.

4. **WEP authentication with 40-bit WEP encryption*:*** this mechanism combines the encryption algorithm to provide data privacy. It adds the RC4 encryption algorithm

5. **WEP authentication with 128-bit WEP encryption:** the 128-bit shared key used is proprietary-based (in the case of Lucent). This mechanism is the same as above using 128-bit keys.

6. **TKIP with 128-bit WEP encryption:** This is the improvement of the WEP algorithm mixed with WEP 128-bit

7. **EAP-TLS authentication:** this is the PKI-based authentication method supported by 802.1x, using digital certificates to authenticate the client into a wireless LAN.

8. **EAP-TLS with 40-bit WEP encryption:** the combined effect of these tools provides the strongest encryption and authentication using per-session keys.

9. **EAP-TLS with 128-bit WEP encryption:** this mechanism is the same as above using 128-bit keys.

10. **PEAP authentication:** This is an EAP authentication type supported by 802.1x that handles security by creating a secure channel that can be served both for encrypted and integrity-protected with TLS.

The first six security mechanisms are consistent with the 802.11 standard. The security mechanisms 7 to 10 are provided by the 802.1x standard. The next section provides some information about the configuration of these security mechanisms from the access point, the server and the clients.

5.3 Security Mechanisms Configuration

During our experiment, the first six security mechanisms were simple to configure because their configuration was being done by using the interface of the access point and the interface of the software installed on both the clients computers and server. The other four security mechanisms were a little difficult to configure because the use of a server for authentication of the clients was required and several steps needed to be taken for the configuration of the security mechanisms on both the server and the access point. In this section, a brief guide on how to configure the security mechanisms is provided.

5.3.1 Configuration of the First Six Security Mechanisms

The configuration of the first six security mechanisms was very simple. For the first one, we created an SSID and checked the option “no security” in the access point interface and we configured the client wireless card with the right SSID. Then, the client was able to connect to the WLAN. For the second one, we added the MAC address of the clients into the MAC address list provided into the interface of the access point. The next three security mechanisms were configured by checking the WEP option into the access point interface, by adding the WEP secret key into its field and by configuring the client laptop with the WEP security option. The TKPI was also setup into the access point and clients computers. Appendix B contains the details on how to configure the security mechanisms.

5.3.2 Configuration of the Last Four Security Mechanisms

Figure 5.2 illustrates an implementation of the 802.1x security model that the four last security mechanisms had been followed. For the security mechanisms 6 to 9, EAP-TLS was used. This type of security requires a Radius server to perform the authentication and a certificate from the client to be able to access the network. Then, on the server side, from the windows 2003 server, a RADIUS server and certificate authorities were added to the basic network structure to provide the authentication support. The RADIUS server supported wireless user sign-on, and a certificate authority was used to issue certificates to users for EAP-TLS authentication. The clients obtained a certificate from a server and they installed it so they could be able to access the network. A step by step instruction is given on how to configure Radius server, IAS server, DNS server and security mechanisms in [31] and [17].

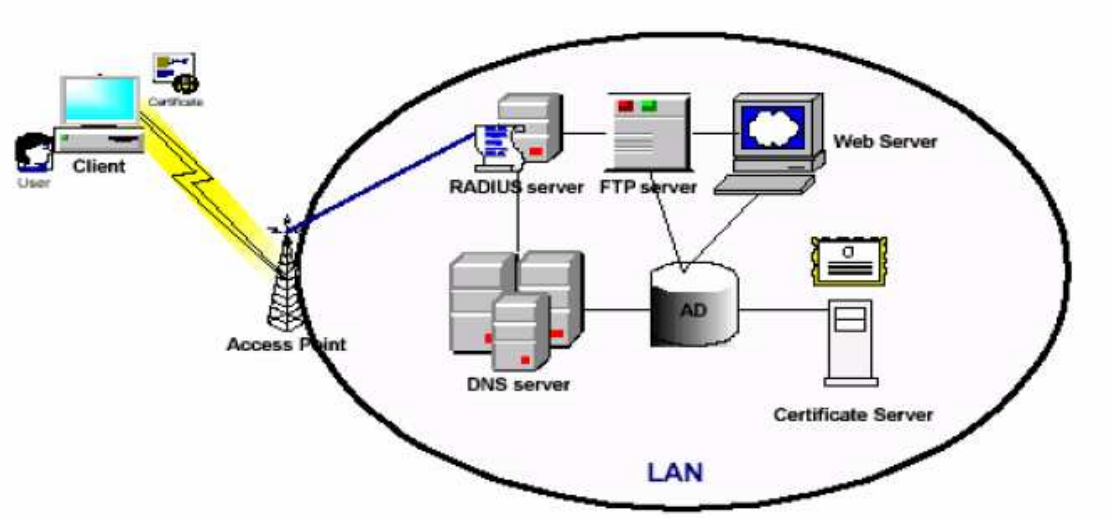

Figure 5.2: 802.1x Model Implementation [3]

The PEAP security mechanism is also an EAP type; then, the same procedures to setup the EAP-TLS can be used to set it up. The only difference is that, from the server, PEAP is needed to be selected as security protocol. From the access point, the security options need to be configured for the PEAP protocol.

5.4 Traffic Generator

As we stated earlier, our experiment was based on a single cell architecture; the clients were connected to the access point. The access point was connected to a switch that was connected to a server. The server or the network was not connected to a backbone or any other networks. In other words, the clients were not connected to the internet. Then, by themselves, the clients were not able to generate traffic. Because of the fact that we wanted to generate traffic for representing a saturated and unsaturated network so we could measure the variation of performance for several security mechanisms, a traffic generator was needed. This traffic

generator needed to have certain characteristics such as: suitable for wireless networks, capable of overloading an 802.11 WLAN, allow the user to change the size and inter-packet delay and provide him/her, the option to select the generation algorithm.

IP traffic [24] was chosen because it met the requirements needed for the experiment and based on the fact that it was used in the previous work [3] being used as the base of our research. Below is a brief description of the *IP traffic-Test & Measure* tool.

5.4.1 IP Traffic-Test & Measure

IP Traffic is a software testing tool that can run on any PC with windows 98, 2000 or XP. It can generate, receive, capture, replay IP traffic, measure end-to-end performance and quality of service over any IP fixed or mobile network. This traffic generator can be set with a large set of different parameters and has the capability to manage 32 simultaneous IP connections. It allows generating traffic using one of the three traffic types protocol: TCP, UDP and ICMP. During our experiment, we only used two traffic types: TCP and UDP.

5.4.1.1 Client Side

For every client, only one active connection was used. The option “IP Generator-Parameters” was selected. Then, we entered the IP address of the server in the IP address field. The number 2010 was collected into the port number and TCP or UDP was added into the protocol field. Figure 5.3 shows a representation of the IP Traffic software on the client side.

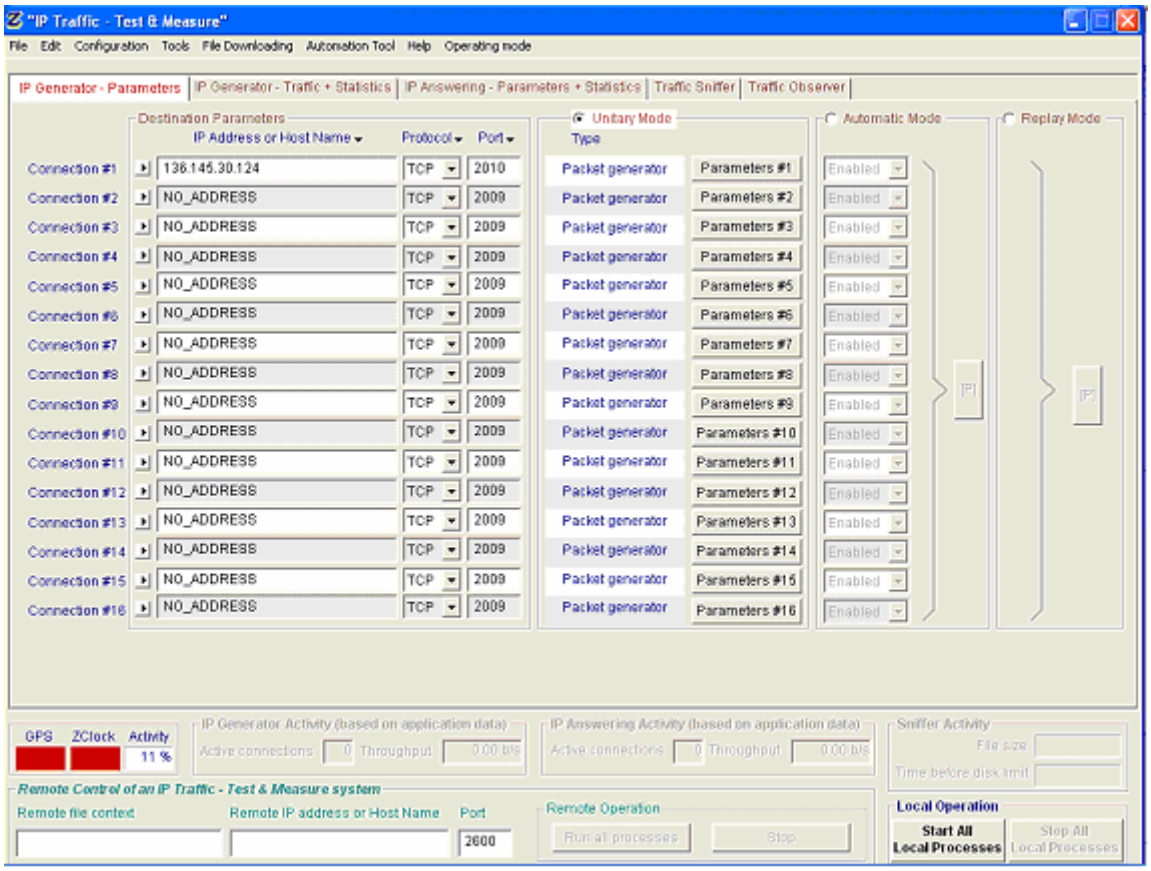

Figure 5.3: IP Traffic – Client

From the interface of the software shows in Figure 5.3, once we clicked on the button Parameters #1, a window popped up. In this window, we entered the assumptions or the characteristics for the traffic that the IP Traffic tool would be generated. Just like for any other research work, we had made some assumptions for our experiment and they would be entered in the popup window. The assumptions made for our experiments were as followed:

- Range for Packets Stream: 10000 – 60000
- The maximum bandwidth: 12 Mbps
- Traffic types being used: TCP and UDP
- Packet length: random over range 40 – 1500

5.4.1.2 Server Side

On the server side, the IP answering option needed to be selected because the server was only receiving traffic generated by the clients. Three different numbers were entered in the port fields which were the port numbers assigned to the clients so they could communicate with the server.

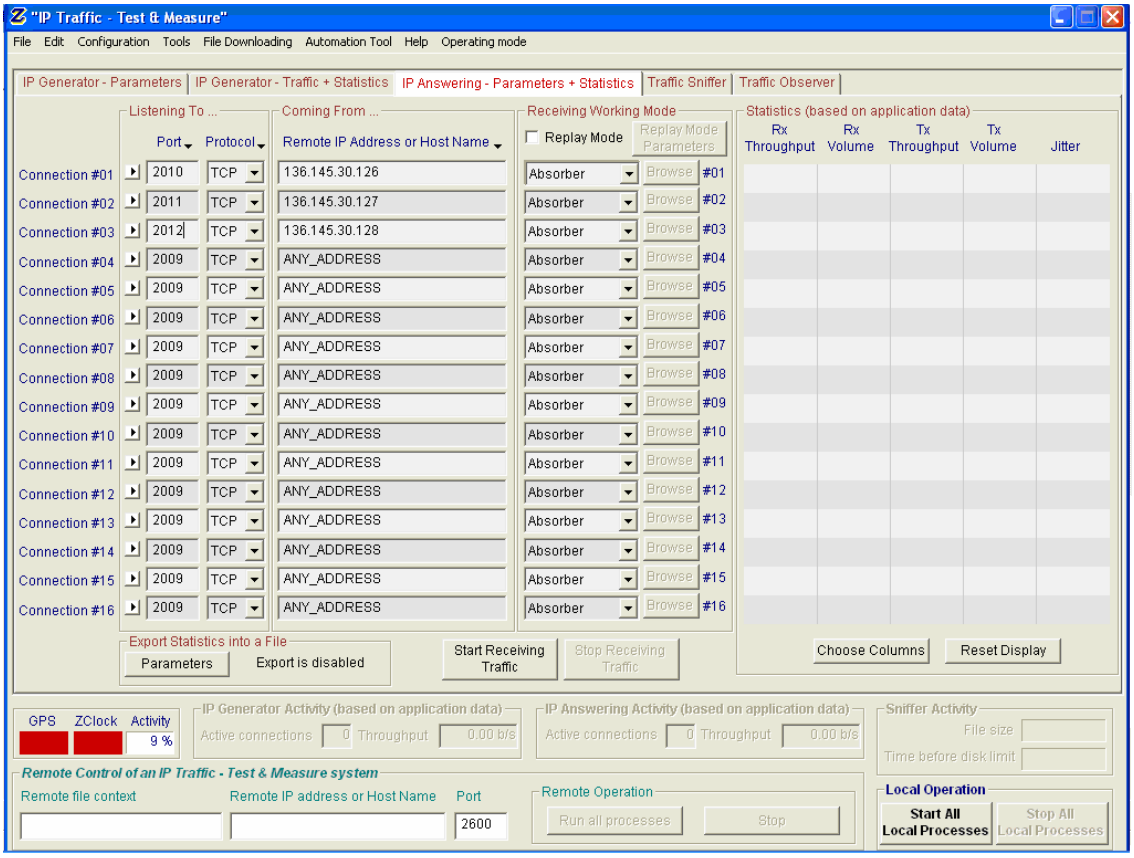

Figure 5.4: IP Traffic – Server

In fact, three static IP address were assigned to the clients and they were entered into the IP address field. Three connections were used for the clients and they all setup as absorber

because the server only absorbed the traffic generated by the clients. Figure 5.4 shows a graphical representation of the configuration of the fields on the server side.

We had done the configuration on the client and server side before we started generating traffic. The next section provides information about the tool being used to capture traffic and generate statistical results.

5.5 Measurement Tool "Ethereal"

Ethereal was used as the measurement tool to capture traffic and measure the throughput and response time for traffic generated by the IP Traffic Generator. Ethereal is an open source network packet analyzer and sniffer that capture network packets and display the data into the packets as detailed as possible. It is a kind of measuring tool or software that allows network managers or researchers to examine and analyze what is going on inside a wired or a wireless LAN. A graphical representation of the ethereal software capturing packets or traffic on the server during our experiment is showed in Figure 5.5.

The ethereal software does provide some statistics about traffic being captured for a specific amount of time or number of packets. In Figure 5.5, the pop up window in the middle is what display the statistics numbers about the traffic captured. In that window, the throughput and the response time at a message and packets level are provided. In our experiment, the measurements were taking at packets level.

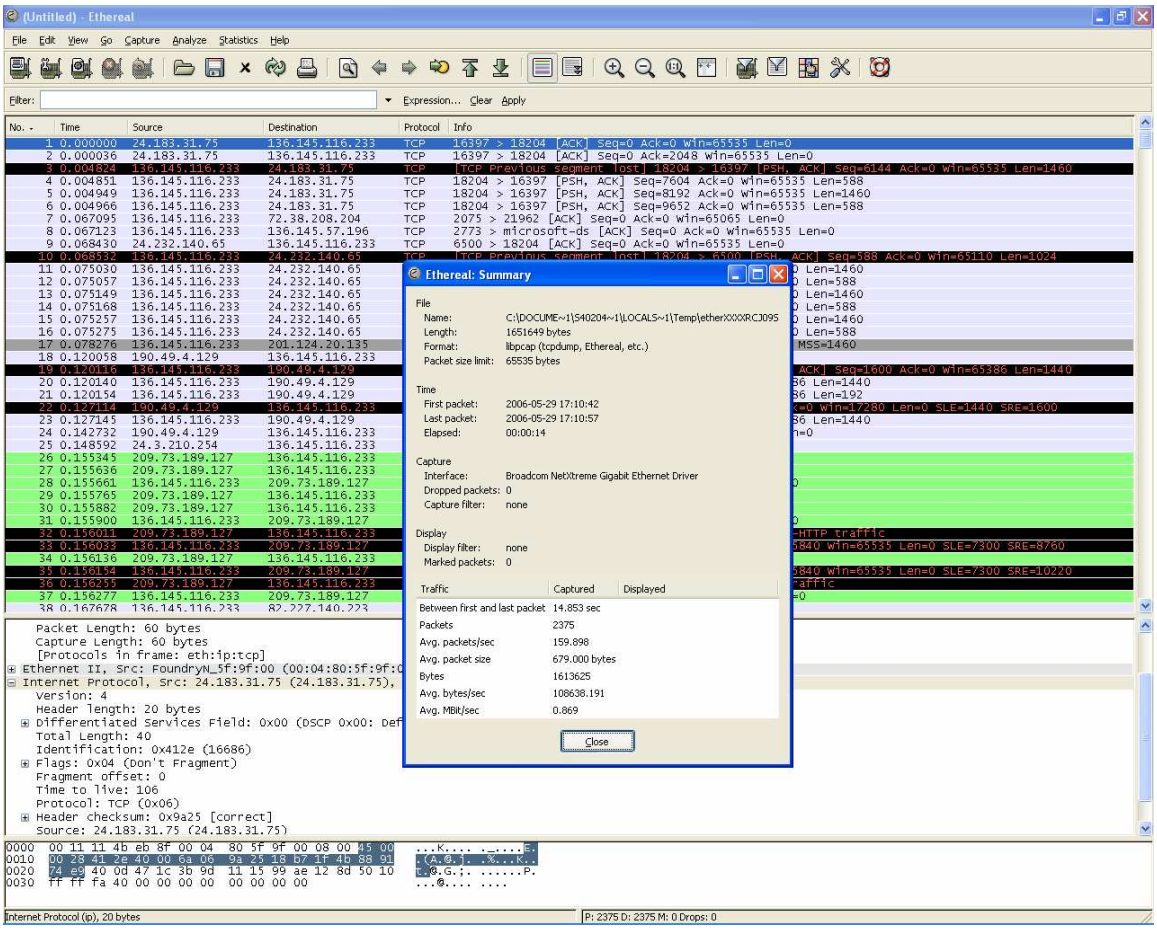

Figure 5.5: Ethereal Capturing Traffic and Display Statistics

5.6 Procedures

As mentioned earlier, this research study has for objective, the evaluation of the impact of different security mechanisms and packet sizes on the performance of saturated or unsaturated WLANs with multiple clients. To make it really simple, we divided our experiments in two parts.

In the first part of the experiment, we measured the throughput and response time of two traffic types: TCP and UDP, against different security mechanisms. Then, we repeated the

experiment for three clients to study and understand the impact of adding more clients into network. Two different bandwidths were chosen: 12000 Kb/s to represent a saturated network and 500 Kb/s to represent an unsaturated network. Appendix B provides more information about how to setup the WLAN for the experiment.

In the second part of the experiment, the throughput was studied as a function of different packet sizes, for different security mechanisms. The packet sizes were divided into four fixed numbers: 250, 500, 1000 and 1500 bytes. The experiments were conducted using one client and three different security mechanisms; the throughput was measured for both TCP and UDP traffic types.

Ten repetitive tests were conducted but only the last five were documented just to be sure about the accuracy of the results.

5.7 Summary

In this chapter, the methodologies and procedures that were being followed to conduct the experiment were presented. An IP traffic generator software was used on both clients and server side to generate a saturated and unsaturated network. The ten security mechanisms being used for our experiment were presented. In fact, the configuration methods for these security mechanisms were also given. The first six security mechanisms were easier to configure than the last four. The Ethereal software was being used to capture packets and to get the statistical results.

CHAPTER 6

Results and Analysis

This chapter presents the results of the impact of the security mechanisms presented in chapter 5 on the performance of the wireless Local Area Network and a brief analysis about the results is also conducted. Firstly, the impact of the traffic types on the performance of the network is presented. Then, we go over the results of the effect of the security mechanisms on the performance of the wireless LAN. Results referring to the impact of adding more clients to the system are also presented. At last, the impact of some fixed packets sizes on the performance of the WLAN is also quantified. We use Minitab 14 as statistic tools or software to perform statistical analysis of our results. The section that is followed gives an overview of the experimental results.

6.1 Experimental Results and Analysis

The experiments were conducted for a saturated and unsaturated 802.11g wireless LAN. As mentioned earlier in chapter 5, ten security mechanisms were used in our experiments. A single cell and an infrastructure operation mode were used to setup the wireless LAN. Firstly, the experiments were running for a single client. Then, the experiments were repeated for two and three clients. The experiments were also repeated for different fixed packet sizes. The experiments conducted for UDP were separated from the ones conducted for TCP traffic type. Over than ten tests were running, but only five results were used. Then, the performance measures were obtained from those five repetitive tests for each security mechanisms. The traffic of the network was generated by IP Traffic generator software and

results were collected from the *Ethereal* monitoring tool. The Data results were analyzed at 95 % confidence interval. The subsections that followed present several results of our experiments and the analysis of them.

6.1.1 Impact of Traffic Types on Performance

The IP Traffic generator software being used allowed us to set up the traffic model types. UDP and TCP are the two traffic models that were used in our experiments. Both of the traffic types affect the performance of the network in different ways. If we take into consideration the results obtained for the mean throughput and response time from both the saturated and unsaturated network provided in Table 6.1, we understand and conclude that UDP performed better than TCP.

Table 6.1: Mean Throughput and Response Time for the two types of WLAN

WLAN	Unsaturated		Saturated	
Mean	Throughput (KB/s)	Response Time (ms)	Throughput (KB/s)	Response Time (ms)
TCP	53.243	15.546	337.863	5.500
UDP	54.842	14.361	439.566	2.980

The UDP traffic type sends and receives packets with faster response time and greater throughput than the TCP. Even in the cases of fixed packet sizes, the UDP traffic type performed better than TCP. Figure 6-1 presents the mean throughput for TCP and UDP for a saturated and unsaturated wireless LAN. Figure 6-1 proves that the UDP as traffic type generates better throughput or performance than the TCP. It also shows that the saturated WLAN produces higher throughput than the unsaturated one.

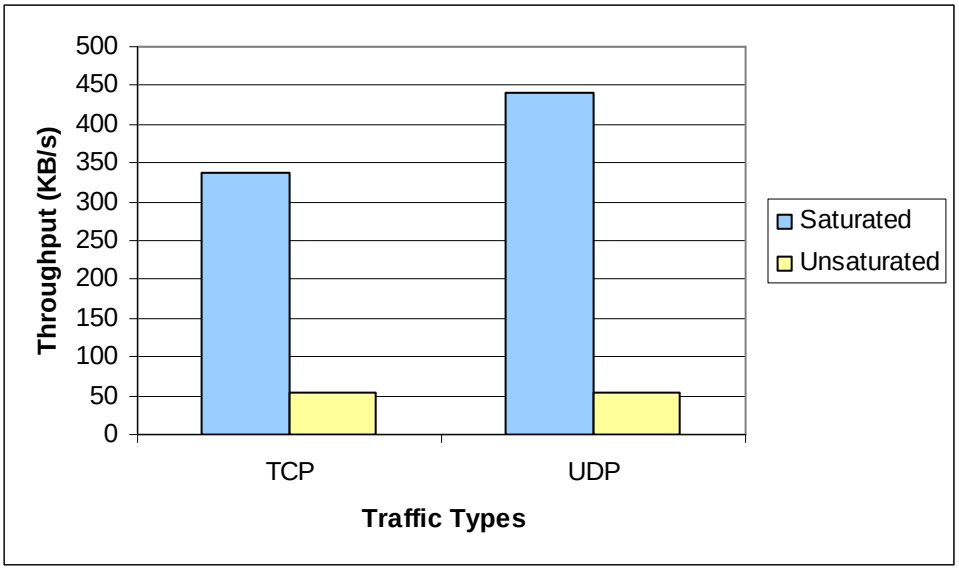

Figure 6.1: Mean TCP and UDP Throughput

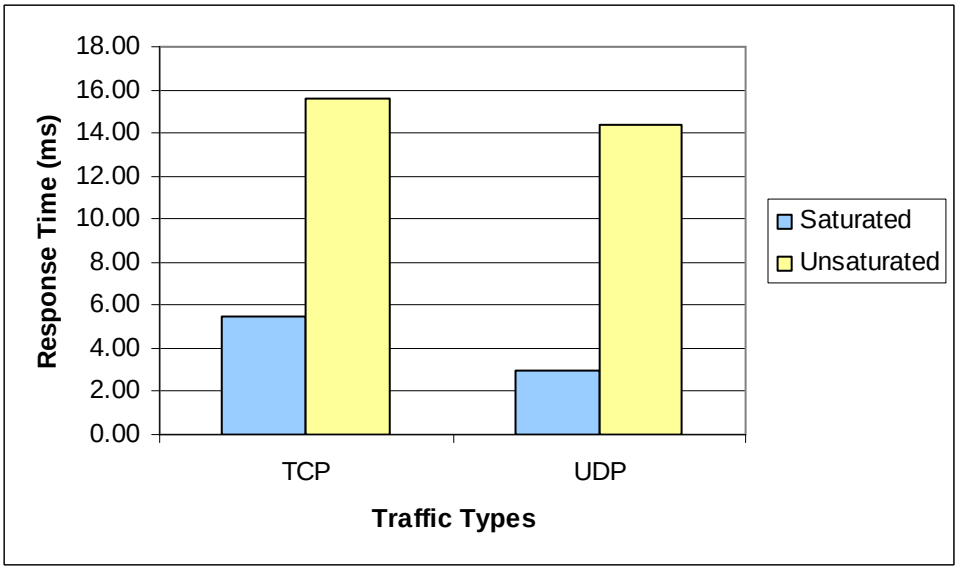

Figure 6.2: Mean TCP and UDP Response Time

In figure 6-2, the mean response time for TCP and UDP for a saturated and unsaturated wireless LAN is presented. It shows that the unsaturated network generates higher response

time than the saturated one. For both saturated and unsaturated network, the UDP generates lower response time than the TCP as traffic types. UDP transfers data faster than TCP.

6.1.2 Impact of Security Mechanisms on Performance

The security mechanisms being used for our experiments affect the performance of the wireless LAN in different ways. As mentioned earlier, several set of experiments were taking place to identify the impact of these security mechanisms on the performance of the network. During the first set of experiments, the throughput limit or bandwidth was set to 500 Kb/s to represent an unsaturated or non congested network and the data were collected using only one client that sends and receives traffic from the server. Figure 6.3 shows the results for the throughput of TCP and UDP traffic types for ten different security mechanisms for an unsaturated wireless LAN. The results show that the stronger the security mechanism, the lower the performance of the network and the weaker the security mechanism, the greater the performance of the network. These results definitely confirmed the general trends reported or documented in [44 and 3].

Certainly, some of the security mechanisms affect the performance of the wireless LAN more than others. For example, if we consider the security mechanisms from the 802.1X standard such as: security mechanisms 7 to 10, they decrease more the performance of the network than the others.

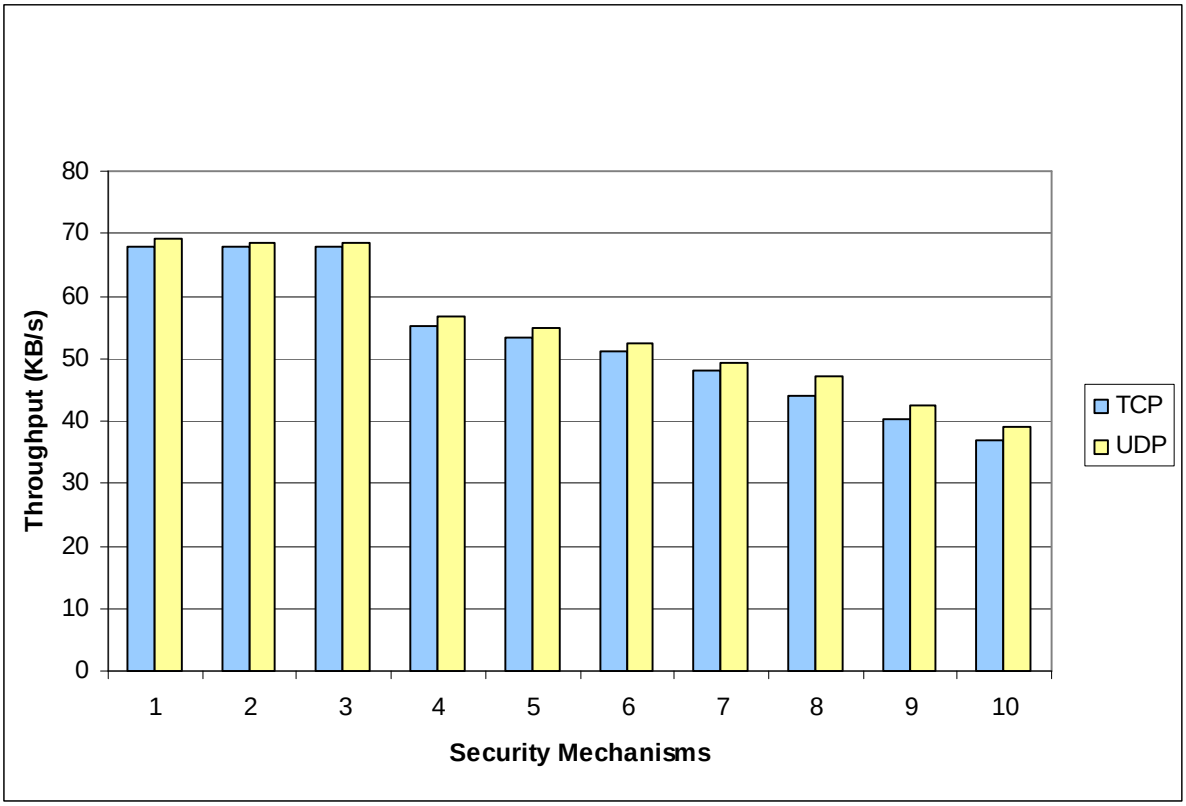

Figure 6.3: Throughput for TCP and UDP in an unsaturated WLAN

For the unsaturated network, the security mechanisms also affect the response time of the wireless LAN. Figure 6.4 shows the results for the response time of the network when throughput limit was set up to 500 Kb/s or when the WLAN is unsaturated. The results show that the more secure the network, the higher the response time and the weaker the security mechanisms; the lower the response time. Thus, the network takes more time to transfer a packet when security is higher while it takes less time to transfer the same packet when the security of the network is lower.

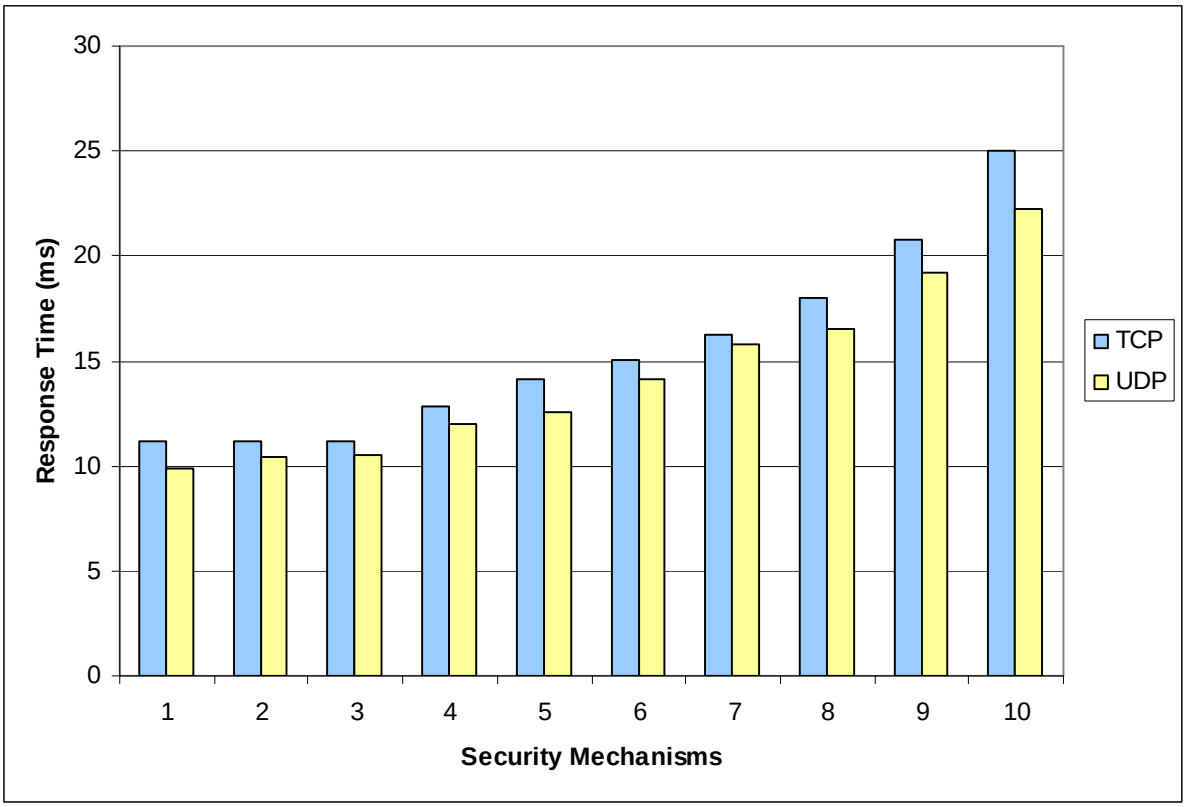

Figure 6.4: Response time for TCP and UDP in an unsaturated wireless LAN

In other set of experiments, the throughput limit or bandwidth was set to 12000 Kb/s or 12 Mb/s to represent a saturated or congested network. The results were still collected by using one client and one server into a single cell. Figure 6.5 illustrates the throughput results of TCP and UDP traffic types for different security mechanisms into a congested network. In fact, the results are completely different from the ones obtained while the network was non congested.

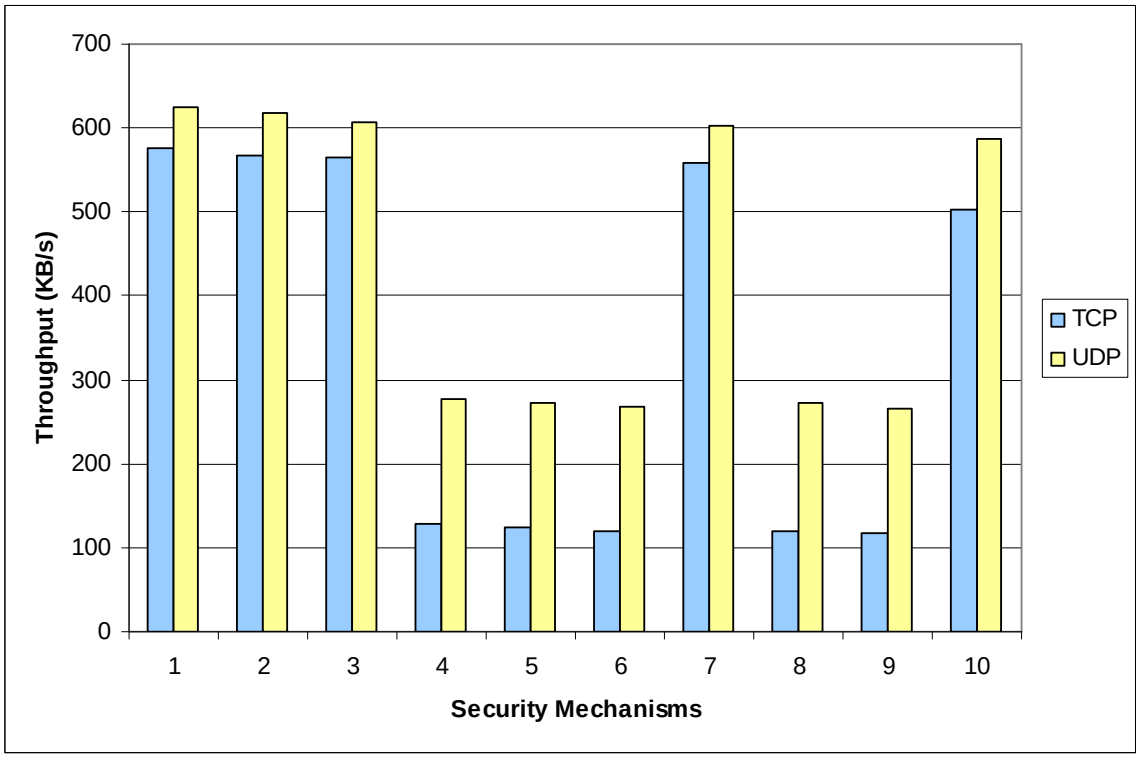

Figure 6.5: Throughput for TCP and UDP in a Congested Wireless LAN

Surprisingly, the results show that the performance for a congested wireless LAN under security mechanisms 4, 5, 6, 8 and 9 is extremely less than while using 1, 2, 3, 7 and 10 as security mechanisms. This contradicts the fact that the more secure the system, the lower the performance of the network. In fact, the security mechanism 7 is more secure than 4, 5 and 6 but it still provides better performance than they do. The security mechanism 10 is more secure than the security mechanisms 4, 5, 6, 8 and 9; but still the security mechanism 10 generates better performance than them. We understand that the use of the key option provides by the WEP algorithm at 40 or 128 bits is the cause of serious performance degradation for security mechanisms 4, 5, 6, 8 and 9. Then, the key of the WEP algorithm definitely has a significant impact on the performance of the network. The results show that,

the fact of encrypting each single packet using security mechanisms 4, 5, 6, 8 and 9 with a 40 or 128 bits WEP key decrease more the performance of the network than some other more secure mechanisms such as EAP-TLS and PEAP.

The same way they affect the throughput of the wireless LAN, the security mechanisms 4, 5, 6, 8 and 9 also increase considerably the response time of the network. Figure 6.6 illustrates the response time of TCP and UDP traffic types for different security mechanisms into a congested network.

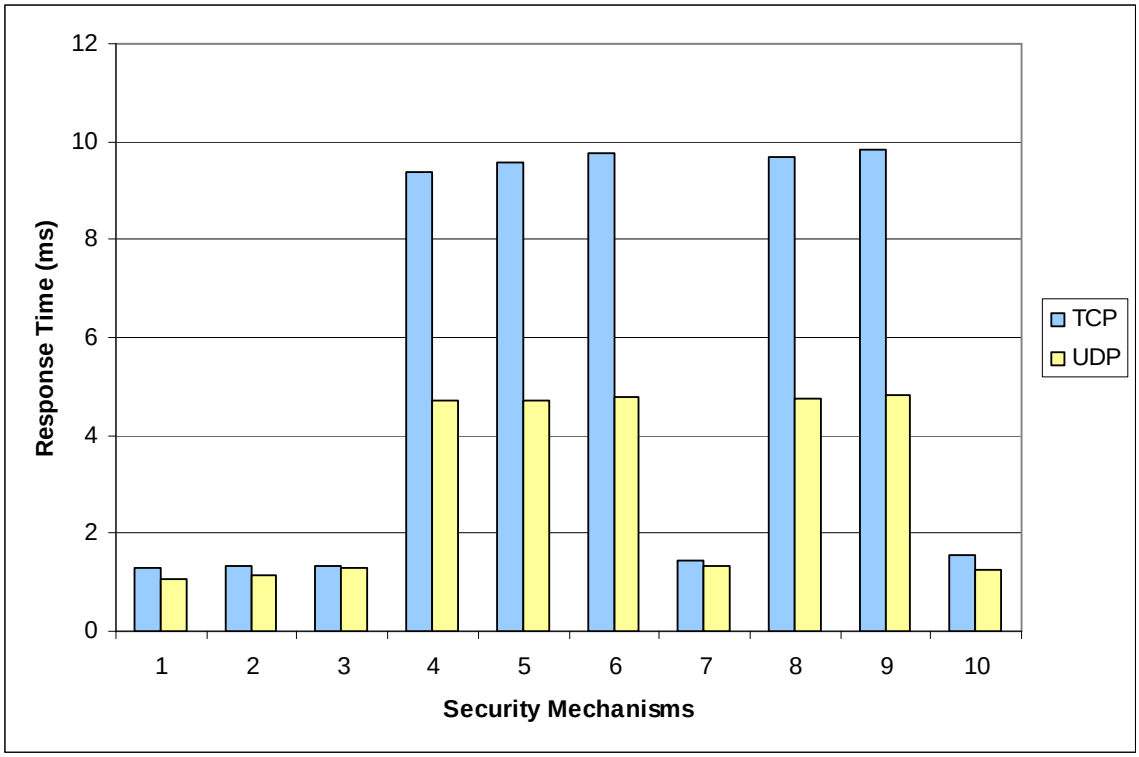

Figure 6.6: Response Time for UDP and TCP in a Congested Wireless LAN

When the security mechanisms 4, 5, 6, 8 and 9 are being used in a congested network, the wireless LAN transfer data slower than when 1, 2, 3, 7 and 10 are used; vice versa. This speed reduction is caused by the use of the WEP keys as security and encryption measures.

6.1.3 Impact of Adding more Clients

After conducting the experiments for one client, the experiments were also repeated for two and three clients just to evaluate the impact of adding more clients to the wireless LAN. Figure 6.7 presents the average per-station throughput for TCP traffic type and Figure 6.8, the average per-station throughput for UDP traffic types for a congested network.

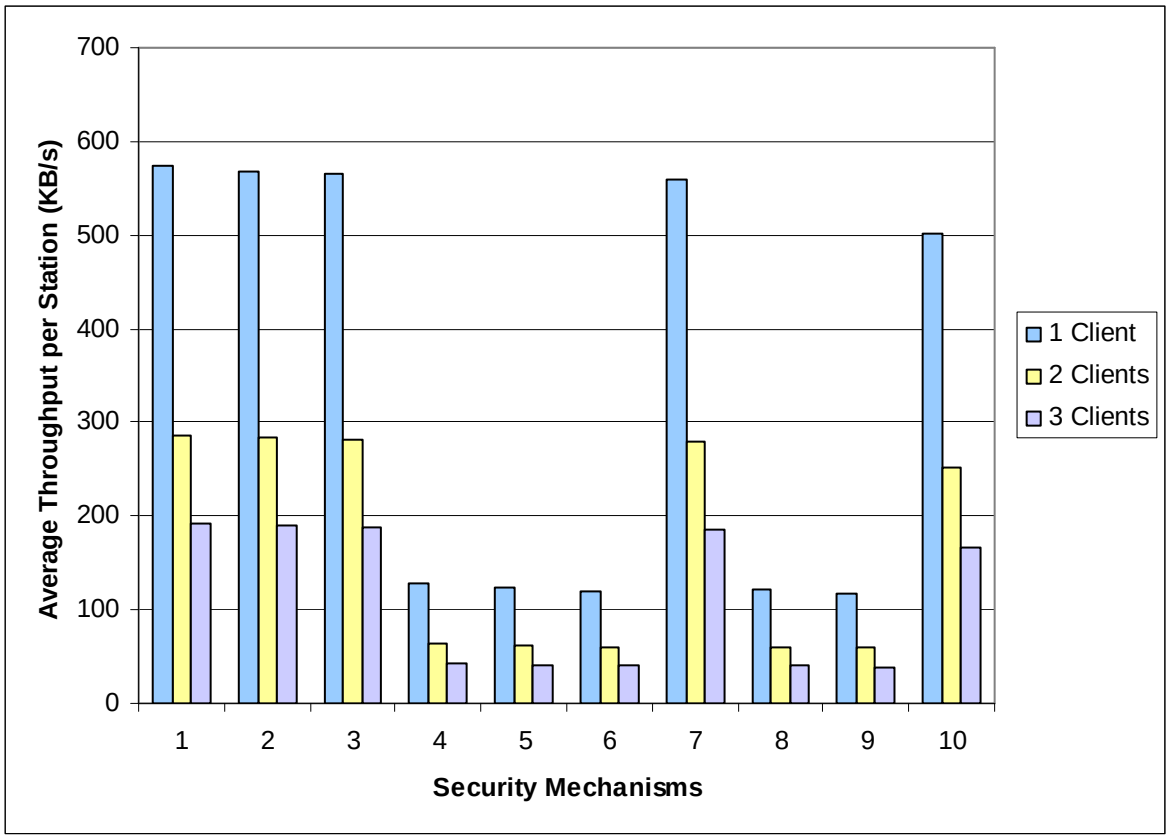

Figure 6.7: TCP Average Per-Station Throughput in a Congested Wireless LAN

The results indicated that, for every security mechanism, the average throughput per-station was decreased by 49.7 % when the experiments were conducted for two clients and by 66.7 % when three clients were used.

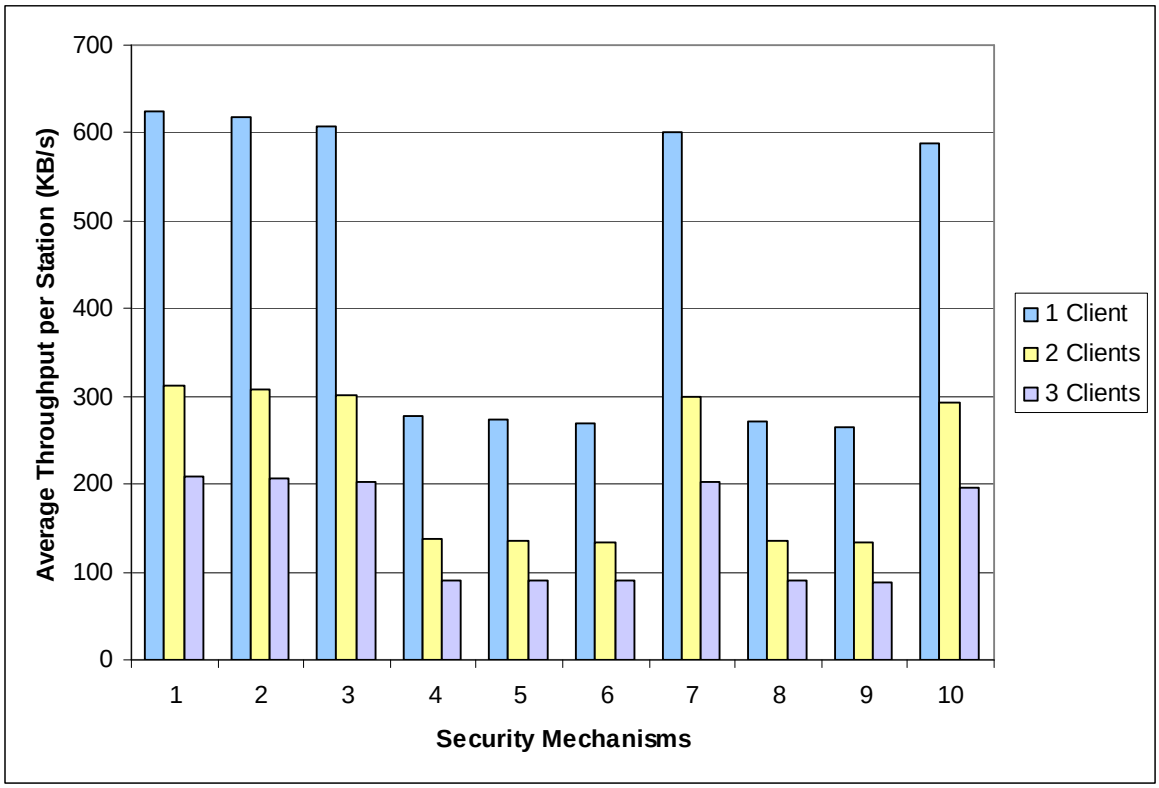

Figure 6.8: UDP Average Per-Station Throughput for a Congested Wireless LAN

In fact, based on our results, we realize that each additional client added to the network decreases considerably the performance of the network. Our experimental work and findings approved the results published in [42] that conclude, when the number of stations increases into a wireless LAN, the overall throughput decreases and its variance increases. Our work also rejoined the conclusions of [3] that assume the average throughput of the network decreases when the number of clients in the system is being increased.

6.1.4 Impact of Fixed Packet Sizes on Performance

As mentioned earlier, other set of experiments were also performed for four fixed packet sizes: 250, 500, 1000 and 1500 just to evaluate their impacts on the performance of a wireless

LAN while using three different security mechanisms. Those three security mechanisms were used to run the experiments: MAC authentication, WEP encryption with a key of 128 bits and WEP security protocol combined with EAP-TLS. Figure 6-9 shows the throughput results obtained from TCP as traffic type and the three security mechanisms mentioned earlier for a non congested wireless LAN.

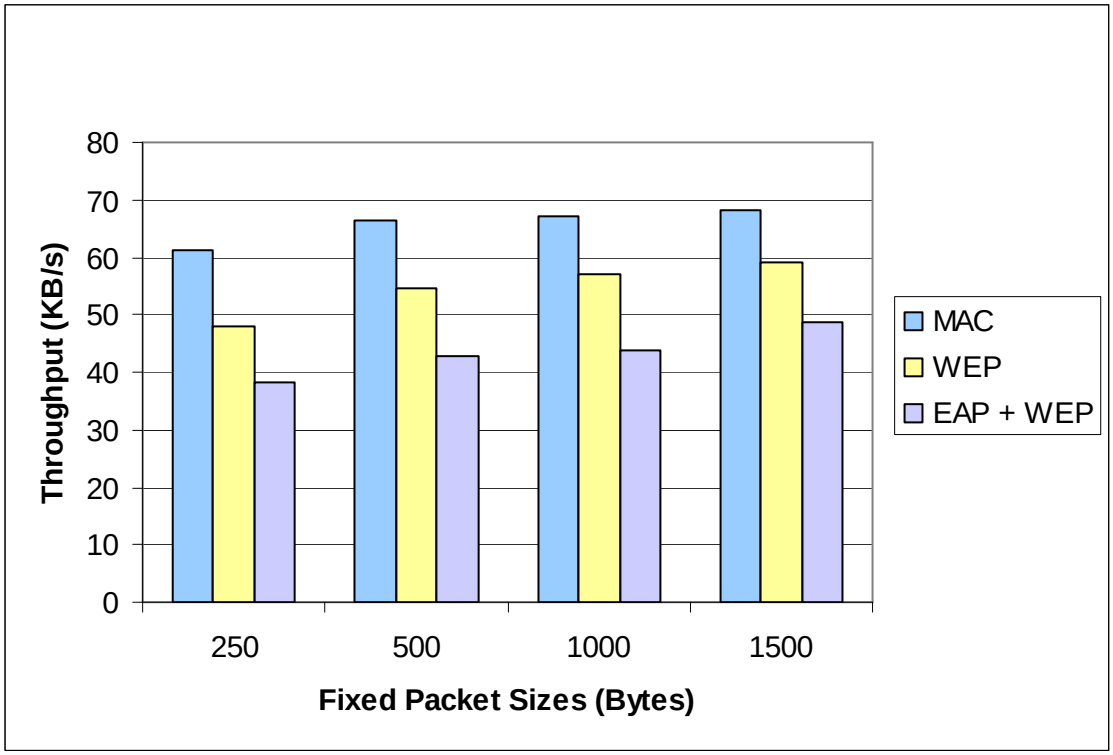

Figure 6.9: TCP Fix Packet Sizes Throughput for non Congested WLAN

The results prove that 1500 bytes which is the biggest packet size produce greater throughput than the other packet sizes. The results also prove that the lower is the security; the greater is the throughput (performance).

Figure 6-10 presents the throughput results when UDP is used as traffic type under the three security mechanisms for a non congested wireless LAN. The results show that the highest

packet size (1500 bytes) generates higher throughput. The results illustrate in Figure 6-10 also prove that the higher the packet size, the higher the throughput and the stronger the security mechanism, the lower the performance of the network.

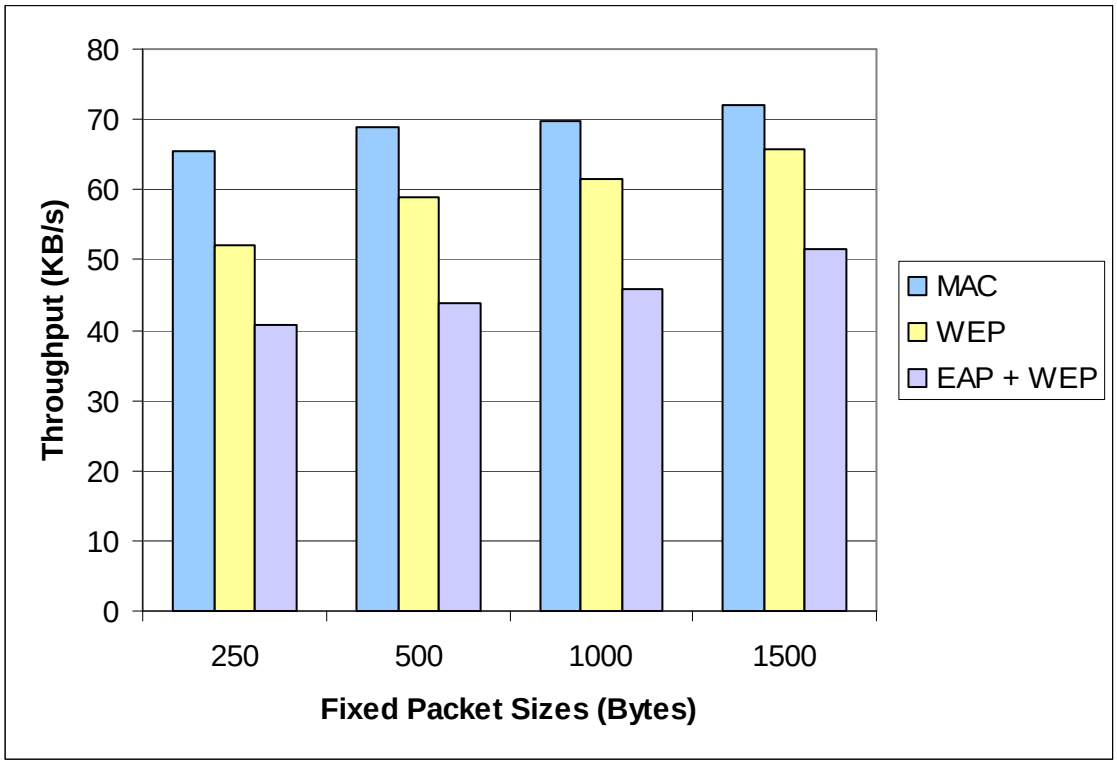

Figure 6.10: UDP Fix Packet Sizes Throughput for non Congested WLAN

In the case of a congested wireless LAN, the results were different from the non congested one. Figure 6.11 illustrates the throughput results for TCP traffic types for different fixed packet sizes (250, 500, 1000 and 1500 bytes). The results show that for 1000 bytes, the throughput is higher or maximum than it is for the other packet sizes. The MAC authentication which is the weaker security mechanism generates higher throughput than the other security mechanisms for all the packet sizes.

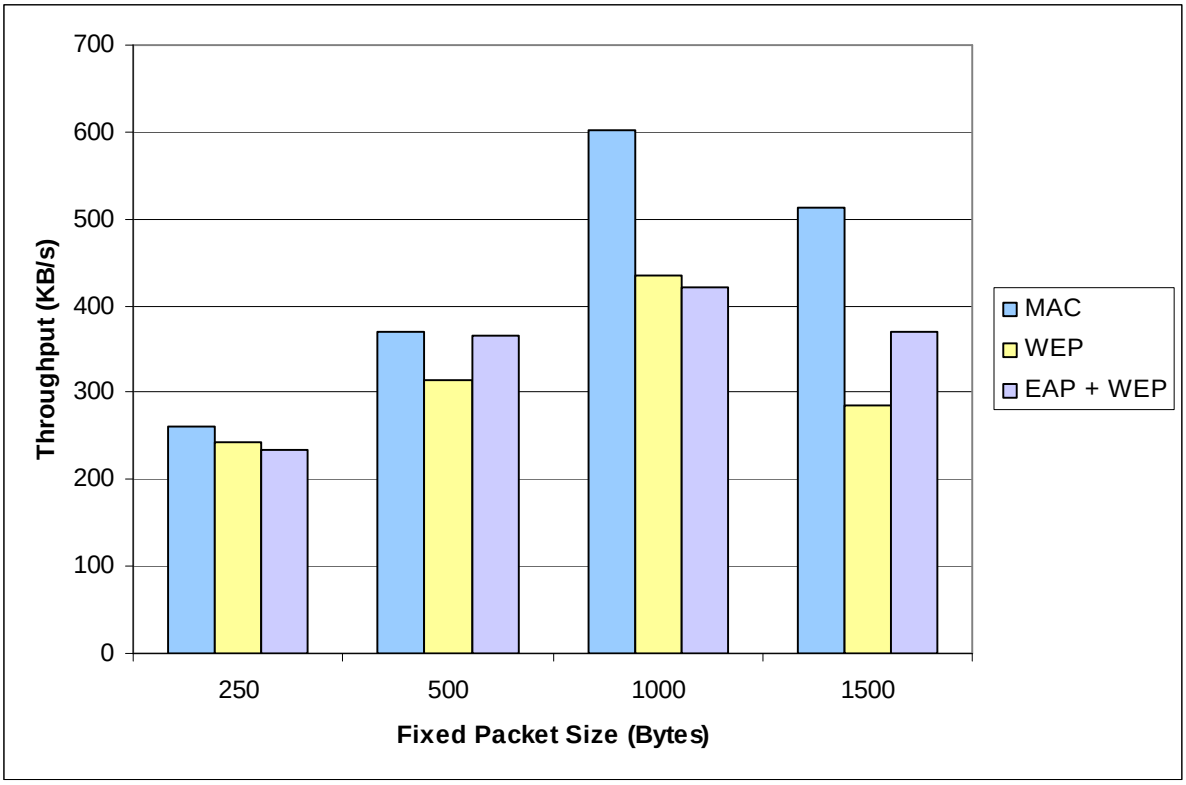

Figure 6.11: TCP Fix Packet Sizes Throughput for Congested WLAN

The same set of experiments was repeated by using the same fixed packet sizes, the same security mechanisms and UDP as traffic types. Figure 6.12 presents the results obtained for the experiments. The results show that when the WEP is used as security mechanism, 500 bytes produce higher throughput than the others packet sizes. For the other two security mechanisms (MAC and WEP + EAP), the throughput is higher when the packet size is equal or set to 1000 bytes. Figure 6.12 also shows that the weaker security mechanism which is MAC still produces a higher throughput for three of the four fixed packet sizes (500, 1000 and 1500).

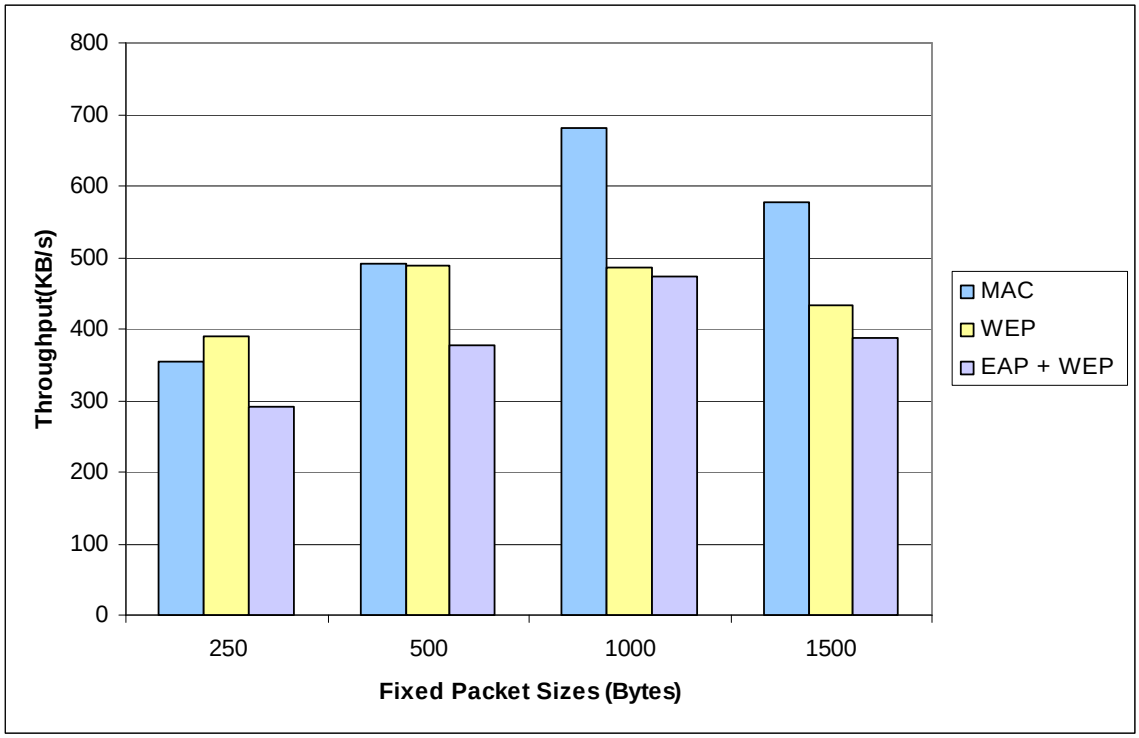

Figure 6.12: UDP Fixed Packet Sizes Throughput for 12000

In fact, both the security mechanisms and the packet sizes affect the performance of the network in different ways.

6.2 Statistical Analysis

A statistical analysis is conducted using Minitab 14, a statistical software package. Just like for most of the statistical analysis, our statistical tests and analysis were based on some null and alternatives hypotheses. The hypotheses being studied are:

- The traffic types TCP and UPD do not affect the performance of the network. The alternative hypothesis is that, the traffic types do affect the performance of the network.

- The security mechanisms do not have any impact on the performance of the network. The alternative hypothesis is that, the security mechanisms have a significant impact on the performance of the network.
- If the network is saturated or unsaturated, it does not affect the performance of the network. The alternative hypothesis is that, the traffic intensity does have an impact on the performance of the network.
- There are no interactions between the traffic types, security mechanisms and traffic intensity. The alternative hypothesis is that, there are some interactions between the factors (traffic types, security mechanisms and traffic intensity).

One way to report the results of a hypothesis test is to state that the null hypothesis is or is not rejected at a specified α-value or level of significance. Usually, the α-value is equal to 0.05 and it is being compared to the p-value to decide if the null hypothesis is rejected in favor of the alternative hypothesis. If p-value is less than 0.05 (α-value), the null hypothesis is rejected. An *analysis of variance* (ANOVA) is conducted to obtain some statistical results and to identify significant affects on the performance of the network. A correlation test is also performed between the throughput and the response time just to verify if both of the variables are related one to each other. A polynomial regression analysis is also performed to investigate the relationship between the response time and the throughput which are the two response variables of our study. The following subsection presents the results of our statistical analysis.

6.2.1 Descriptive Statistical Results

The experiments consider three factors: security mechanisms (10 possibilities), traffic types (TCP and UDP) and traffic intensity (saturated versus unsaturated). Tables 6-2 and 6-3 present the mean and standard deviation for throughput (KB/s) and response time (ms) for unsaturated versus saturated wireless LAN, respectively.

Table 6.2: Descriptive Statistical Results for an Unsaturated WLAN

Security Mechanisms	Throughput (KB/s)				Response Time (ms)			
	TCP		UDP		TCP		UDP	
	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.
1	67.970	0.304	69.230	0.820	11.134	0.021	9.935	0.938
2	67.838	0.047	68.622	0.486	11.145	0.005	10.426	0.719
3	67.888	0.229	68.454	0.608	11.137	0.010	10.558	0.787
4	55.134	1.683	56.576	1.724	12.853	0.946	12.068	0.654
5	53.458	7.831	54.972	3.136	14.137	2.830	12.762	1.249
6	51.116	1.953	52.382	1.595	15.075	0.739	14.131	0.695
7	47.940	2.346	49.382	2.588	16.238	0.960	15.790	0.741
8	44.062	0.974	47.262	0.701	17.986	0.534	16.485	0.324
9	40.170	3.129	42.482	1.901	20.748	2.488	19.226	1.533
10	36.850	1.013	39.064	1.250	25.006	1.861	22.224	1.244

Table 6.3: Descriptive Statistical Results for a Saturated WLAN

Security Mechanisms	Throughput (KB/s)				Response Time (ms)			
	TCP		UDP		TCP		UDP	
	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.
1	574.870	2.800	624.690	2.560	1.281	0.009	1.069	0.016
2	567.930	3.940	617.490	2.290	1.319	0.022	1.139	0.013
3	564.750	2.390	606.400	2.800	1.338	0.006	1.289	0.010
4	128.880	2.440	277.820	1.840	9.379	0.029	4.689	0.019
5	123.270	2.460	273.170	1.600	9.559	0.024	4.726	0.007
6	120.600	2.770	272.260	1.500	9.558	0.211	4.735	0.017
7	558.810	3.130	601.810	1.500	1.431	0.069	1.315	0.013
8	119.530	3.740	268.510	1.460	9.765	0.121	4.778	0.021
9	118.170	1.050	265.870	1.940	9.834	0.017	4.810	0.021
10	501.820	3.190	587.640	2.050	1.539	0.018	1.247	0.011

The results also prove that the performance for a congested wireless LAN under security mechanisms 4, 5, 6, 8 and 9 is extremely less than the performance of the network while using 1, 2, 3, 7 and 10 as security mechanisms. Just like Figure 6-5 and 6-6, the results show in table 6-3 also contradict the fact that, the stronger the security mechanism; the lower the performance because the security mechanism 10 is stronger than 4, 5, 6, 8 and 9 but it produces greater performance than them.

6.2.2 Analysis of Variance

An analysis of variance (ANOVA) is conducted by using the *General Linear Model* option to test if the factors (traffic types, security mechanisms and traffic intensity) have a significant impact on the response time which is the response under consideration. The results in Table 6-4 show that the three factors have a significant effect on the response time given that their respective p-value are much smaller than 0.05. Thus, we reject the null hypotheses and support the alternatives ones.

Table 6.4: *ANOVA* Analysis Results

Source	DF	Seq SS	Adj SS	Adj MS	F-Stat	p-value
Traffic Types	1	171.66	171.66	171.66	23.68	0.000
Security Mechanisms	9	1483.66	1483.66	164.85	22.74	0.000
Traffic Intensity	1	5738.36	5738.36	5738.36	791.67	0.000
Error	188	1362.71	1362.71	7.25		
Total	199	8756.39				

In this analysis of variance, it also shows up that the percentage of data variability explained by the model (R-Sq) is equal to 84.44 % which is a good indication for the ANOVA model. Notice that, the analysis of variance conducted is a simple ANOVA test that does not

consider the interactions between the factors (traffic types, security mechanisms and traffic intensity) that can affect the response time.

6.2.3 ANOVA 2-Way Interactions

Another analysis of variance is conducted to test the effect of the traffic types, security mechanisms and traffic intensity on the response time. In this model, we also test the significant interactions between the factors. Table 6-5 presents the results obtained from the ANOVA test. The results prove that the three factors have a significant impact on the response time given that their respective p-values are less than 0.05. The results also show that the factors have some significant interactions one on each other because the p-values for all the interactions are way much smaller than 0.05. Then, we can reject the null hypothesis that claims there are no interactions between the factors in favor of the alternatives ones.

Table 6.5: *ANOVA* 2-Way Interactions Analysis Results

Source	DF	Seq SS	Adj SS	Adj MS	F-Stat	p-value
Traffic Types (A)	1	171.66	171.66	171.66	153.85	0.000
Sec. Mechanisms (B)	9	1483.66	1483.66	164.85	147.75	0.000
Traffic Intensity (C)	1	5738.36	5738.36	5738.36	5143.08	0.000
Interaction (A * B)	9	77.92	77.92	8.66	7.76	0.000
Interaction (A * C)	1	22.28	22.28	22.28	19.97	0.000
Interaction (B * C)	9	1073.94	1073.94	119.33	106.95	0.000
Error	169	188.56	188.56	1.12		
Total	199	8756.39				

An important value that does not include in Table 6-5 is the R-Sq which represents the percentage of data variability. The ANOVA test reveals that the R-Sq is equal to 97.46 % which is an indication that confirms the ANOVA as a great statistical model.

6.2.4 Models Validation

In fact, two different analysis of variance tests are being conducted, a simple ANOVA and a 2-way interactions ANOVA that consider the interactions between the factors: traffic types, security mechanisms and the intensity of the network (saturated and unsaturated). In the subsections that followed, we validate both of the models and decide which one is better.

6.2.4.1 Simple ANOVA Validation Model

The simple ANOVA statistical model is validating by performing an analysis of the residual plots for the response time of the WLAN. Four different graphics have been provided to illustrate the residual plots but they have been combined or placed into one graphic. Figure 6-13 illustrates the residual plots for the response time that can help to validate the model. The validation of the statistical or ANOVA model can be performed by using any of those fours graphics.

Certainly, there are some assumptions or rules that the model has to follow so we can consider it as a great statistical model that fulfills the assumptions of the analysis of variance (ANOVA). Model assumptions ANOVA procedures make these assumptions about the errors:

- The errors are normally distributed with mean zero.
- The error variance does not change for different levels of a factor or according to the values of the predicted response. The variance needs to have a constant value.
- Each error is independent of all other errors.

Our main goal is to check the validity of these assumptions in our analysis. Residuals are the best estimates of error. Therefore, we can check each of these assumptions graphically by using the residual plots.

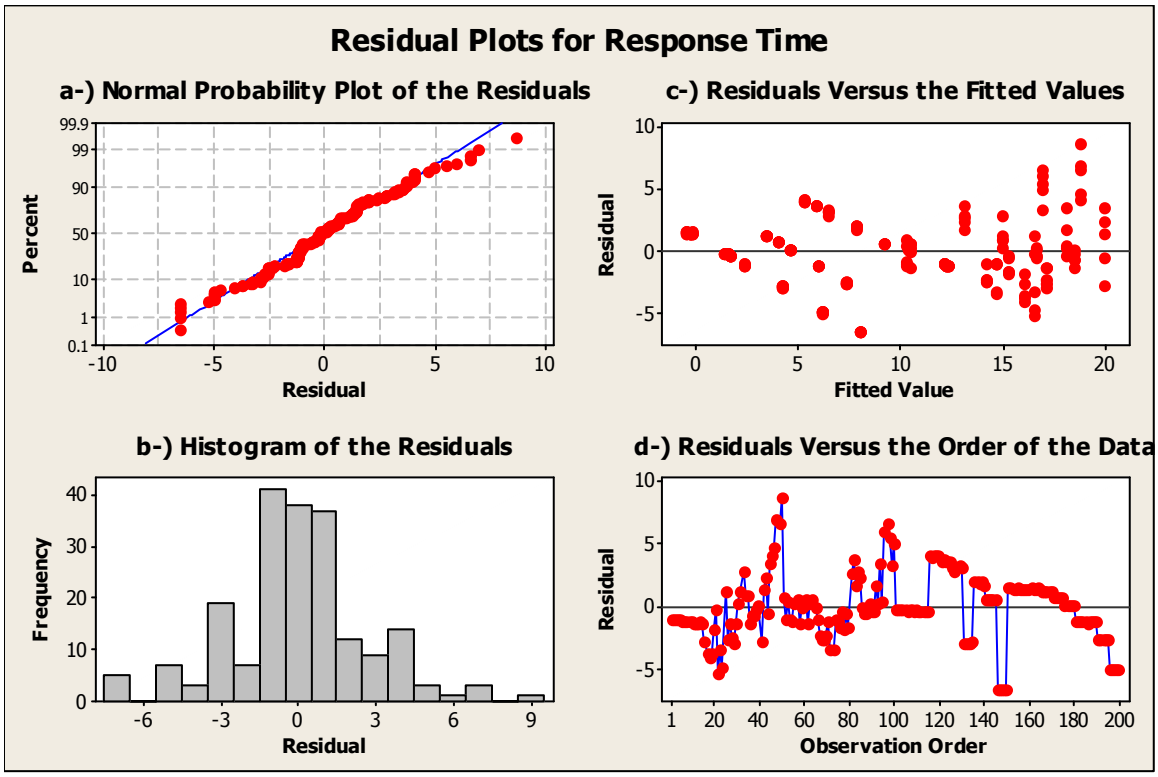

Figure 6.13: Residual Plots of the simple ANOVA Model for Response Time

Figure 6-13a presents the normal probability plot of the residuals. Based on this graphic, we can conclude that the ANOVA model follows the assumptions and rules of a great statistical model because the data are normally distributed. The majority of the point shows in the graph falls onto the fitted line and the one that are not being placed on the line is really close to it, that is why we conclude that the data follows a normal distribution.

Figure 6-13b illustrates the graphical representation of a histogram of the residuals. Based on this graphic, we conclude that the residuals follow a normal distribution because the data of the histogram have a bell-shaped. Then, the graphic follows the analytical assumptions. The errors are normally distributed with mean zero.

In Figure 6-13c, the graphical representation of the residuals versus the fitted values is given. When analyzing this type of graphic, the model is correct and the assumptions are satisfied if the residuals are structureless and also the variance of the errors is constant. After analyzing the graphic, we realize that the data are randomly scattered around the fitted line and they are not following any particular pattern. The errors have a constant variance because the residuals are randomly distributed. Based on Figure 6-13c, we can admit that the ANOVA model fulfills the assumptions of our analysis and it is a great statistical model.

The last figure (Figure 6-13d) provides a graphical view of the residuals versus the order of the data. From this figure, we deduct that the residuals do not follow any particular patterns because the data were randomly scattered around zero or the fitted line. Then, we conclude that the errors are independent from each other and their variance is constant. This model definitely follows all of our assumptions being used for the analysis or the validation of a great model.

6.2.4.2 ANOVA 2-Way Interactions Validation Model

Figure 6-14 shows a graphical representation of the residuals plots for the response time obtained from the ANOVA 2-way model that considers the interactions between the statistical factors (traffic types, security mechanisms and traffic intensity) during the analysis.

There are four different graphics including in that figure. In overall, the graphics look nice for a statistical analysis and the validation of the model but the ones present in Figure 6-13 are better. Then, if we are taking in considerations only the graphics, we will conclude the simple ANOVA model is better than the ANOVA 2-Way Interactions model.

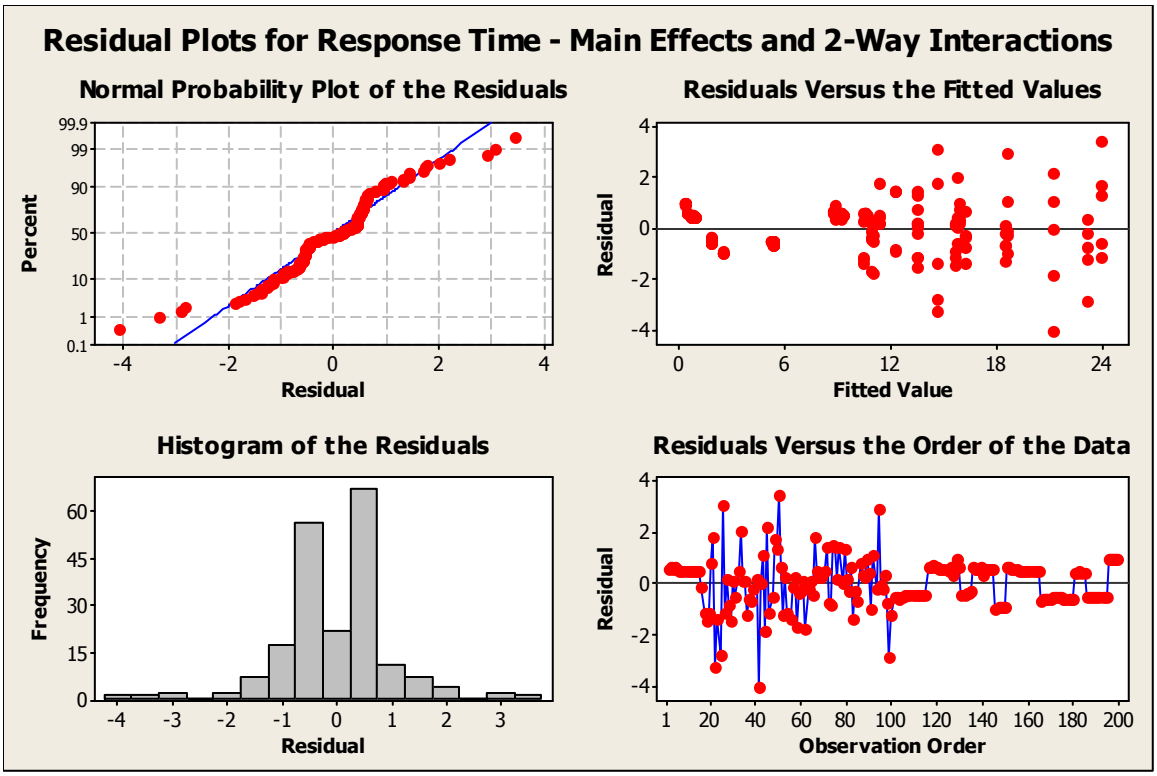

Figure 6.14: Residual Plots of the ANOVA 2-Way Interactions Model for Response Time

However, our validation model is based on the R-Sq values. For the simple ANOVA model, R-Sq is equal to 84.44 % while it is equal to 97.46 % for ANOVA 2-Way interactions model. Based on the R-Sq values, we conclude that the ANOVA 2-Way interactions model is a better statistical model than the simple one. However both of the models fulfill the analysis of variance (ANOVA) presumptions.

6.2.5 Correlation Test

A correlation coefficient test is performed for the response time and the throughput just to measure the degree of linear relationship between the two response variables. Usually, the correlation coefficient has for result a value between -1 and +1. If the correlation coefficient is negative, the variables are negatively correlated, that is mean one of the variables tends to increase as the other one decreases. Conversely, when the correlation coefficient is positive, both of the variables tend to increase at the same time. For our correlation test, we obtain a negative value for the correlation coefficient which is equal to – 0.859 and a p-value equal to 0.000 which is less than α. Then, the coefficient correlation value is statistically significant. The throughput and the response time are negatively correlated; whenever one increases, the other deceases and vice versa.

6.2.6 Fitted Line Plot Regression Analysis

A regression analysis is also conducted to analyze the relationship between the response time and the throughput. As results, we obtain a p-value less than 0.05 or α for the regression test. Thus, the regression test is statistically significant. Table 6.6 shows the results obtain from the regression analysis.

Table 6.6: Regression Analysis Results

Source	DF	SS	F-stat	p-value
Regression	3	9557158	8180.36	0.000
Linear	1	556.90	556.90	0.000
Quadratic	1	1170.74	1170.74	0.000
Cubic	1	738.52	738.52	0.000
Error	196	76329		
Total	199	9633487		

The cubic polynomial regression model is a significant statistical model because we find out that the p-value is lower than α. Figure 6-15 shows a graphical representation of the relationship between the throughput and response time. The model generates a cubical equation that estimates the value of the throughput in function of the response time.

$$\text{Throughput} = 718.2 - 118.4\ \text{Response Time} + 6.802\ (\text{Response Time})^2 - 0.1266\ (\text{Response Time})^3$$

This is a third degree equation that represents the regression analysis model for the response time and the throughput. This equation allows us to determine the different throughput values by replacing the response time by its value.

The graph (Figure 6-15) also validates the polynomial regression model as a great and significant statistical model because the data or the points included in it falls onto the curve or the fitted line and they follow a normal distribution.

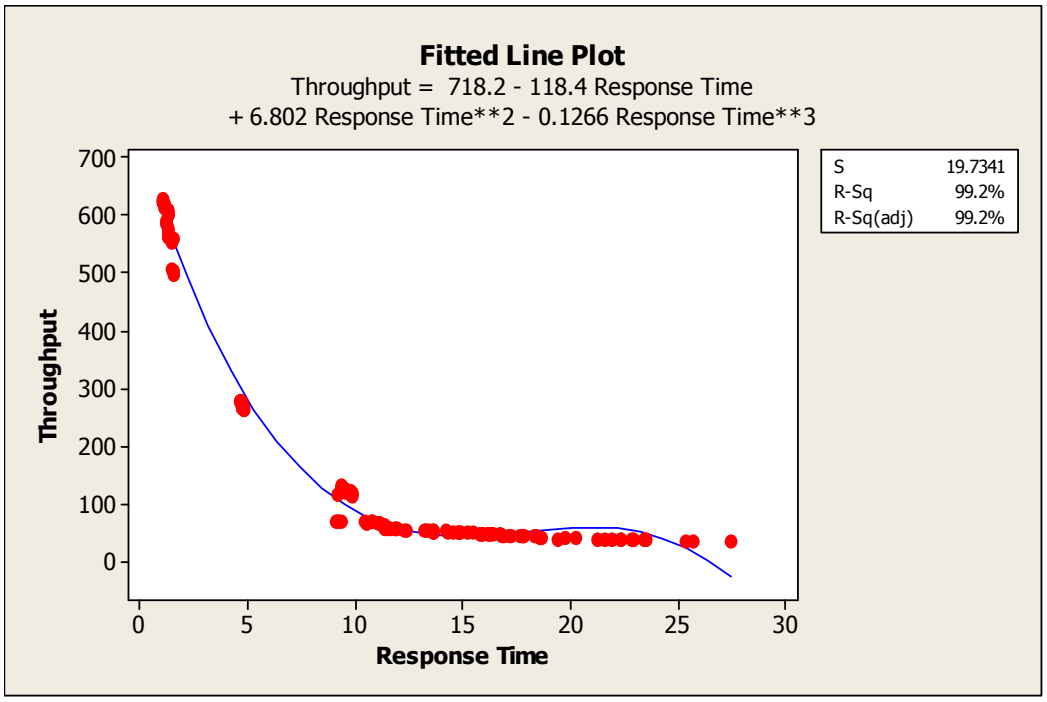

Figure 6.15: Fitted Line Plot for Throughput and response Time

From Figure 6.15, we also observe that, when the response time falls into the interval 10 to 25, the value of the throughput is constant while for the interval 0 to 10, the throughput varies considerably.

6.3 Limitations

There are several different limitations applicable to our experiments. Firstly, the experiments were conducted in an area in which there were several other devices such as microwaves and other access points that were probably operated in the same frequency range as our access point. Then, there might be some radio interferences signal between our wireless LAN and other devices. These interferences once they occurred definitely affect and degrade the performance of our wireless LAN.

During our experimental work, we realize that electricity can affect the performance of the network. We actually run some tests when the client computer was connected to an outlet electricity plug and then turn the power off and run the same tests with the same characteristics while the client was using battery. The results were different for both tests; the throughput of the network was lower when the power was off. Then, we conclude that the electricity has a significant impact on the performance of the network.

The experiments evaluated the impact of the security mechanisms on the performance of the wireless LAN for the 802.11g standard only. We know that they are other important 802.11 standards such as 802.11b and 802.11a but our study does not take in consideration these standards.

Due to the limitations of equipment, our experimental work was only conducted for three clients using a single cell.

6.4 Retesting

A lot of retesting has been taking place because of the fact that any simple factors can affect our results. Certain factors that can affect the performance of our wireless LAN are: the other devices operating in the same frequency range, power and the types of equipment that are being used for the experiment. Certainly, for our experiment we do repeat certain tests several times for accuracy. During our experiment, most of the tests being repeated are the one conducted for congested network because in this type of network, our experiment proves that anything can happen. This type of network even rejects our assumptions that pretend the more secure the WLAN, the lower the performance. Then, the retesting is very essential during measurement type experimentation.

6.5 Summary

This chapter presents the results of our experimental work. Some briefs explanations on how and why we obtain the results are also provided. For the non congested wireless LAN, we find out that the stronger the security mechanism, the lower the throughput and the higher the response time. The weaker the security mechanism, the greater the throughput and the lower the response time. For a congested network, the impact of the WEP key algorithm decreases a lot more the performance of the network than other considered more secure mechanisms such as EAP-TLS, LEAP and PEAP. When we add two and three clients to the wireless LAN,

we find out that each additional client decreases significantly the performance of the network. In the cases of the measurement of the impact of the fix packet sizes on the network, we find out as results that the fixed packet sizes affect the performance of the network in different ways depend on the security mechanism being used. A statistical analysis is conducted by taking in considerations some null and alternatives hypotheses. Because of the fact that the p-values obtained from the two ANOVA models were smaller than 0.05, we reject the null hypotheses for the alternatives ones.

CHAPTER 7

WLAN Security Recommendations

When it comes to set up the security of a wireless LAN, some security guidelines or recommendations need to be followed. During the set up of the wireless LAN security, one of the most important factors that needs to be considered is the performance of the network. Basically, the designer or the administrator of the network needs to establish a tradeoff between performance and the security mechanism that he/she is planning to use. This chapter, based on our experimental results provides some recommendations about the traffic types and the security setting of a wireless LAN based on a tradeoff between performance and security means.

Firstly, we provide some recommendations or guidelines based on the traffic types; one of the factors that have a significant impact on the performance of the wireless LAN when using any security mechanisms. Then, we go over some recommendations based on the wireless LAN security mechanisms and the performance of the network.

7.1 Recommendations Based on Traffic Types

During our experiments, beside the security mechanisms, one of the factors we observe that affect the wireless LAN is the traffic types being used. We used two traffic types, the UDP (User Datagram Protocol) and TCP (Transfer Control Protocol). Our results prove that, for all the security mechanisms the UDP provides better performance than the TCP as traffic type. Based on our results, we recommend the use of the UDP as traffic type instead of the

TCP under the used of any security mechanisms for the improvement of the performance of the network.

7.2 Recommendations - Performance Tradeoff & Security

This section provides some recommendations or guidelines for wireless LAN security setup based on tradeoff between performance and security taking in consideration both the saturated and unsaturated wireless LANs.

7.2.1 Unsaturated Wireless LAN

The results of our experiment for an unsaturated WLAN with only one client shows that the stronger the security of the network, the lower the performance. When we added two more clients to the network under the impact of the same security mechanisms, we find out that each additional client decreases considerably the performance of the network but still the stronger the security mechanism, the lower the performance. In the case of the fixed packet sizes, all the security mechanisms do have a different and significant impact on the performance of the network. Then, for an organization to use the more secure mechanism, it has to pay a price which is the decrease of the performance of its wireless LAN. However, the organization can still use a trade off between performance and security mechanisms. The organization can use the MAC address which provides better performance than the WEP and the 802.1x security mechanisms, but the problem to that is that the MAC authentication protocol can compromise to some attacks. An organization can also use the WEP protocol as basic security because based on our results, the WEP does not affect the performance that

much comparing to the 802.1x security mechanisms. The drawback is that the WEP algorithm is not really secure (Chapter 3). Then, better security is needed because no organization wants to compromise its information. Based on our results, the security mechanism until now that does not compromise to a known attack and that provides better performance is the EAP (Extensible Authentication Protocol). It does not mean that it is not vulnerable to attacks. Based on our results, an organization can also choose to use the EAP or mix it with WEP to provide better security for its wireless LAN.

7.2.2 Saturated Wireless LAN

In the case of a saturated network, our results prove that the 40 and 128 bits WEP key affect considerably the performance of the network. The WEP keys even affect the performance of the network more than other stronger security mechanisms such as EAP and PEAP. Additionally to that, the WEP protocol is not really secure. In that case, an organization does not need to use the WEP protocol with keys. The organization can choose to use EAP or PEAP as security mechanisms. Because of the fact that EAP provides better performance than PEAP, when it comes to a saturated wireless LAN, we recommend the EAP (Extensible Authentication Protocol) as the best security mechanism that provides better tradeoff between performance and security means.

7.3 Summary

In this chapter, we provide some recommendations or guidelines that need to be followed to protect a wireless LAN. When it comes to traffic types, the use of the UDP is selected as

recommendation to provide better performance under any security mechanisms. Based on a tradeoff between performance and security, the use of EAP or the combination of it with WEP is recommended for unsaturated wireless LAN and the use of EAP by itself is recommended in the case of a saturated network.

CHAPTER 8

Conclusions and Future Work

This chapter concludes our experimental research and thesis work. An overview and presentation of the future work that can be performed in the same area is also provided.

8.1 Conclusions

This research quantifies the impact of the security mechanisms on the performance of the network for congested and non congested wireless LAN. The experiments were first running for a single client and then they were repeated for multiple clients to evaluate the effect of adding more clients to the network. Another set of experiments were also conducted for fixed packet sizes just to analyze their impacts on performance.

Our finding and results lead us to conclude that the UDP traffic type provides better performance than the TCP. It provides greater throughput and faster response time than the TCP. For an unsaturated wireless LAN, the results prove that, the stronger the security of the WLAN, the lower the performance and the greater the response time. In the case of a congested wireless LAN, the encryption of each single packet by the WEP algorithm keys extremely decreases the performance of the wireless LAN. It even decreases the performance of the network more than very well known stronger security mechanisms (EAP and PEAP). When adding multiple clients to the network, we find out that, when the number of clients in the system is increasing, the overall throughput of the network is decreasing. When several fixed packet sizes were used, we find out that they affect the performance of the network differently depend on the security mechanisms being used.

A statistical analysis was also conducted by considering several null and alternatives hypotheses. Two different ANOVA models were used: a simple and all-interactions ANOVA models. Based on the results obtained from both of the models, we reject the null hypotheses in favor of the alternatives ones because p-value is lower than 0.05 or α. We conclude that the all-interactions model is a better statistical model than the simple one because the all-interactions model generates an R-Sq value equal to 97.46% while the simple model only generates 84.44%. A correlation test was also performed to study the linear relationship between the response time and the throughput; we find out that, they are negatively correlated. So, whenever one of the variable increases, the other one decreases. Finally, we performed a fitted line plot regression analysis; we realize that, there is a great relationship between the response time and the throughput.

8.2 Future Work

Further research work can be carried out by studying the effect of the WPA and WPA2 on the performance of an unsaturated and saturated wireless LAN. Other work can be also performed by repeating the same experiments with multiple access point. Our experimental is based on 802.11g; then it will be interesting in the future to conduct a similar research for others 802.11 standards. Additional research can be also conducted by studying the impact of the electrical power on the performance of a wireless LAN.

References

[1] Arbaugh, W.A. *Wireless security is different*. Computer, Volume: 36, 9 – 101, Issue: 8, Aug. 2003.

[2] Arbaugh, W.A. *Your 802.11 wireless network has no clothes.* Wireless Communications, IEEE Volume 9, Issue 6, Dec. 2002 Page(s):44 - 51

[3] Baghaei, N.; Hunt, R *IEEE 802.11 wireless LAN security performance using multiple clients.* Networks, 2004. (ICON 2004). Proceedings. 12th IEEE International Conference on Volume 1, 16-19 Nov. 2004 Page(s):299 - 303 vol.1

[4] Balachandran, A., Voelker, G., Bahl, P. and Rangan V. Characterizing user behavior and network performance in a public wireless LAN. *In Proceedings of ACM SIGMETRICS*, 2002.

[5] Bing, B., & Subramanian, R. A Novel Technique for Quantitative Performance Evaluation of Wireless LANs. *Computer Communications*, 21. Elsevier. Pages: 833-838, 1998.

[6] Bing B. Measured performance of the IEEE 802.11 wireless LAN. *In Proceedings Conference on Local Computer Networks*, pages 34-42, 1999.

[7] Borisov, B., I. Goldberg, & D. Wagner. *Intercepting Mobile Communications: The Insecurity of 802.11*. Seventh Annual International Conference on Mobile Computing and Networking. ACM, 16-21 July 2001

[8] Brown, B.; *802.11: the security differences between b and I*. Potentials, IEEE Volume 22, Issue 4, Oct-Nov 2003 Page(s):23 – 27

[9] Brown, G.; Jones, D. *802.11 Security Checkpoint.* Wireless Oracle, Light Reading Volume 2, NO 3 March 2003

[10] Burr, W.E. *Selecting the Advanced Encryption Standard.* Security & Privacy Magazine, IEEE. Volume 1, Issue 2, Mar-Apr 2003. 43 – 52.

[11] Carli, M.; Rosetti, A.; Neri, A. *Integrated security architecture for WLAN.* Telecommunications, 2003. ICT 2003. 10th International Conference on Volume 2, 23 Feb.-1 March 2003 Page(s):943 - 947 vol.2

[12] Chen, J. C. Measured Performance of 5-GHz 802.11a Wireless LAN Systems. Atheros Communications, Inc. August 27, 2001.

[13] Cisco. Deployment Guide: Configuring the Cisco Wireless Security Suite. Cisco Systems Inc. April 2004.

[14] Cisco. *Performance Management: Best Practices White Paper*, Cisco Systems, Inc. 1998, http://www.cisco.com/warp/public/126/perfmgmt.htm.

[15] Convery, S., & D. Miller. *SAFE: Wireless LAN Security in Depth, version 2*. White paper. Cisco Systems, Inc. 2003
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf

[16] Crow, B.P.; Widjaja, I.; Kim, L.G.; Sakai, P.T. IEEE 802.11 Wireless Local Area Networks. Communications Magazine, IEEE. Volume 35, Issue 9, Sept. 1997 Page(s):116 – 126

[17] Davies, J. Deploying Secure 802.11 Wireless Networks with Microsoft Windows. Microsoft Press, ISBN 0-7356-1939-5, 2004

[18] Duchamp D. and N.F. Reynolds. Measured performance of a wireless LAN. In *Proc. of the 17th IEEE Conference on Local Computer Networks*, pages 494–499, September 1992.

[19] Ethereal, www.ethereal.com

[20] Fluhrer, S., I. Mantin, & A. Shamir. *Weaknesses in the Key Scheduling Algorithm of RC4.* Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

[21] Fortier, P.J. & Michel, H.E. Computer Systems Performance Evaluation and Prediction. First Edition, Digital Press, ISBN 1-55558-260-5, 2003.

[22] G. Xylomenos and G.C. Polyzos. TCP and UDP performance over a wireless LAN. In *Proceedings of INFOCOM*, pages 439-446, 1999.

[23] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang. *Security in mobile ad hoc networks: challenges and solution.* Wireless Communications, IEEE, Volume: 11, Issue: 1, Feb 2004, 38 – 47.

[24] IP traffic, www.zti-telecom.com/pages/iptraffic-test-measure.htm

[25] Kamerman, A., & G. Aben. Net throughput with IEEE 802.11 wireless LANs. *Wireless Communications and Networking Conference*, WCNC, IEEE. Volume: 2, Page(s): 747 -752 vol. 2. 23-28 September, 2000.

[26] Karygiannis, T., & L. Owens. (2002). *Draft: Wireless Network Security - 802.11, Bluetooth and Handheld Devices.* USA. National Institute of Standards and Technology.

[27] Marincic, A.; Milovanovic, D. Wireless Local Area Networks. Telecommunications in Modern Satellite, Cable and Broadcasting Services, 1999. 4th International Conference on Volume 1, 13-15 Oct. 1999 Page(s):291 - 299 vol.1

[28] Microsoft. Certificate requirements when you use EAP-TLS or PEAP with EAP-TLS. http://support.microsoft.com/default.aspx?scid=kb;en-us;814394. Article ID: 814394, Last Review: June 7, 2005.

[29] Microsoft. Configure PEAP and EAP methods.
http://technet2.microsoft.com/WindowsServer/f/?en/Library/ecb5c750-9917-48eb-b33b-8404a57e396b1033.mspx. Updated: January 21, 2005.

[30] Microsoft: How to install a certificate for use with IP Security. http://support.microsoft.com/default.aspx?scid=kb;EN-US;253498.
Article ID: 253498, Last Review: December 9, 2005June 7, 2005.

[31] Microsoft IIS Team, Internet Information Services 6.0 Resource Kit. Microsoft Press, ISBN 0-7356-1420-2, 2004.

[32] Nayak, D.; Rajendran, N.; Phatak, D.B.; Gulati, V.P. *Security Issues in Wireless Local Area Networks.* Electrical and Computer Engineering, 2004. Canadian Conference on Volume 3, 2-5 May 2004 Page(s):1637 - 1640 Vol.3

[33] Orinoco. (2002). *Principles of 802.1x Security*. Orinoco Technical Bulletin 048/B. Lucent. April 2002

[34] Potter, B. *Wireless security's future*. Security & Privacy Magazine, IEEE, Volume: 1, Issue: 4, July-Aug. 2003, 68-72.

[35] Russell, S.F**.** *Wireless network security for users.* Information Technology: Coding and Computing, 2001. Proceedings International Conference on 2-4 April 2001 Page(s): 172 - 177

[36] Stallings, W. *Cryptography and Network Security: Principles and Practices*. Pearson Education, Inc., NJ, Third Edition, 2003.

[37] Stallings, W. IEEE 802.11: Moving Closer to Practical Wireless LANs. IT Professional IEEE, Volume 3, Issue 3, May-June 2001 Page(s):17 – 23

[38] Stallings, W. IEEE 802.11: Wireless LANs from a to n. IT Professional, Volume 6, Issue 5, Sept.-Oct. 2004 Page(s):32 – 37

[39] Stevens W. TCP slow start, congestion avoidance, fast retransmit, and fast recovery algorithms. Internet Request for Comments, January 1997. RFC 2001.

[40] Tanenbaum, A.S. Computer Networks, Fourth Edition. Prentice Hall PTR, ISBN: 0-13-066102-3, 2003

[41] TGi. (2002). Task Group 802.11i: IEEE, Inc. http://www.ieee802.org/11.

[42] Vasan, A., &. A. U. Shankar. An Empirical Characterization of Instantaneous Throughput in 802.11b WLANs. Department of Computer Science, University of

[43] Walker J. R. *IEEE 802.11 Wireless LANs: Unsafe at any key size; an analysis of the WEP encapsulation.* Document Number: IEEE 802.11-00/362. 27 October 2000 Maryland. http://www.cs.umd.edu/~shankar/Papers/802-11b-profile-1.pdf

[44] Wong, J. Performance Investigation of Secure 802.11 Wireless LANs: Raising the Security Bar to Which Level? Master's Thesis, University of Canterbury, Christchurch, NZ, 2002.

APPENDIX A. DATA CAPTURED

1. Data Captured for Unsaturated Network

Security Mechanisms	TCP		UDP	
	TCP Throughput(KB/s)	TCP Response Time (ms)	UDP Throughput(KB/s)	UDP Response Time (ms)
1	67.880	11.140	67.910	11.134
1	67.810	11.150	69.780	9.270
1	68.340	11.110	68.950	10.763
1	67.600	11.155	69.670	9.381
1	68.220	11.114	69.840	9.129
2	67.920	11.136	68.810	10.765
2	67.800	11.147	67.960	11.093
2	67.820	11.148	69.280	9.210
2	67.830	11.146	68.630	10.485
2	67.820	11.148	68.430	10.578
3	67.850	11.143	67.900	11.136
3	68.130	11.117	69.260	9.230
3	67.980	11.132	68.820	10.761
3	67.520	11.158	67.830	11.140
3	67.960	11.133	68.460	10.523
4	54.050	13.328	54.070	13.217
4	55.810	12.357	56.280	11.892
4	57.030	11.976	58.730	11.651
4	55.970	12.318	57.480	11.664
4	52.810	14.287	56.320	11.917
5	47.010	16.432	52.800	13.675
5	63.740	11.357	58.250	11.427
5	54.110	13.279	58.520	11.361
5	57.830	11.858	52.170	13.687
5	44.600	17.758	53.120	13.662
6	52.370	14.576	53.440	13.678
6	48.870	15.895	49.870	14.936
6	51.930	14.828	53.870	13.524
6	53.200	14.263	51.850	14.841
6	49.210	15.812	52.880	13.675
7	50.360	15.267	49.240	15.873
7	47.630	16.285	45.500	16.854
7	44.130	17.825	52.100	14.815
7	49.020	15.878	48.720	15.921
7	48.560	15.936	51.350	15.487
8	45.190	17.248	46.890	16.728
8	44.250	17.889	47.750	16.256
8	44.460	17.816	48.120	16.179
8	43.860	18.321	46.340	16.924
8	42.550	18.654	47.210	16.338
9	45.500	17.203	44.780	17.694
9	39.160	21.280	41.580	19.785
9	38.640	22.370	43.570	18.442
9	40.100	19.405	39.810	21.618
9	37.450	23.482	42.670	18.589
10	38.230	22.895	38.250	22.957
10	37.520	23.465	37.940	23.531
10	36.050	25.773	38.750	22.420
10	36.630	25.384	41.110	20.267
10	35.820	27.513	39.270	21.943

2. Data Captured for Saturated Network

Security Layer	TCP		UDP	
	TCP Throughput(KB/s)	TCP Response Time (ms)	UDP Throughput(KB/s)	UDP Response Time (ms)
1	571.220	1.294	622.310	1.082
1	576.640	1.278	621.940	1.087
1	578.430	1.270	626.880	1.058
1	573.420	1.283	627.540	1.049
1	574.650	1.280	624.800	1.072
2	570.770	1.301	618.690	1.136
2	569.820	1.323	614.070	1.158
2	565.780	1.338	616.430	1.145
2	571.270	1.293	618.310	1.135
2	562.030	1.341	619.940	1.123
3	561.880	1.345	605.350	1.293
3	567.230	1.332	607.480	1.286
3	565.630	1.335	609.430	1.279
3	562.570	1.343	602.110	1.304
3	566.450	1.337	607.650	1.282
4	128.850	9.381	280.370	4.663
4	131.670	9.345	277.920	4.691
4	127.060	9.414	275.480	4.712
4	130.900	9.356	276.800	4.704
4	125.930	9.402	278.550	4.678
5	121.820	9.576	275.320	4.716
5	119.960	9.584	272.910	4.728
5	124.760	9.542	273.850	4.724
5	123.560	9.567	270.930	4.735
5	126.250	9.527	272.840	4.729
6	120.730	9.581	272.510	4.730
6	116.920	9.242	273.040	4.726
6	123.650	9.558	270.340	4.764
6	118.870	9.836	274.170	4.719
6	122.820	9.574	271.250	4.738
7	562.230	1.344	603.750	1.302
7	559.460	1.388	601.080	1.318
7	556.310	1.437	599.780	1.336
7	554.890	1.464	602.590	1.309
7	561.170	1.522	601.850	1.313
8	114.980	9.855	270.650	4.740
8	119.260	9.803	266.940	4.792
8	122.870	9.788	268.760	4.786
8	116.880	9.826	267.350	4.789
8	123.670	9.554	268.870	4.783
9	118.560	9.838	265.830	4.815
9	119.230	9.805	267.780	4.788
9	118.380	9.839	264.810	4.827
9	116.420	9.848	267.700	4.788
9	118.250	9.839	263.240	4.832
10	506.190	1.508	590.510	1.227
10	501.670	1.543	587.670	1.249
10	499.960	1.548	584.870	1.256
10	497.870	1.539	588.230	1.253
10	503.430	1.556	586.920	1.250

APPENDIX B. EXPERIMENT CONFIGURATION

The following sections show briefly the configuration of the wireless LAN and the security mechanisms from the client and the server side. The modifications made to the equipments such as: access point, client devices and server during the experiment are also presented. The first section presents the changes made on the client side and the second one shows the setup on the server side.

B.1 Client Side

Firstly, we installed the wireless card software on the clients PCs. Because of the fact that we were using a single cell, we assigned a static IP address to the clients, access point, server and switch just to place them in the same segment. The subnet mask, default gateway and DNS server IP address were also entered (See Figure B.1.1).

The WEP security protocol was configured on the client side from the wireless properties to allow the client to be part of the network when WEP was being used (see Figure B.1.2).

Firstly, the method to assign an IP static address to the WLAN devices is presented, and then we show how to setup some of the security mechanisms on the client side. Finally, we show how to enter the assumptions data into the IP traffic generator and we also show the traffic generator setup on the client PCs.

Figure B.1.1 shows the assignment of a static IP address to a client which is part of the wireless LAN and Figure B.1.2 shows the setup of the WEP protocol on the client machines.

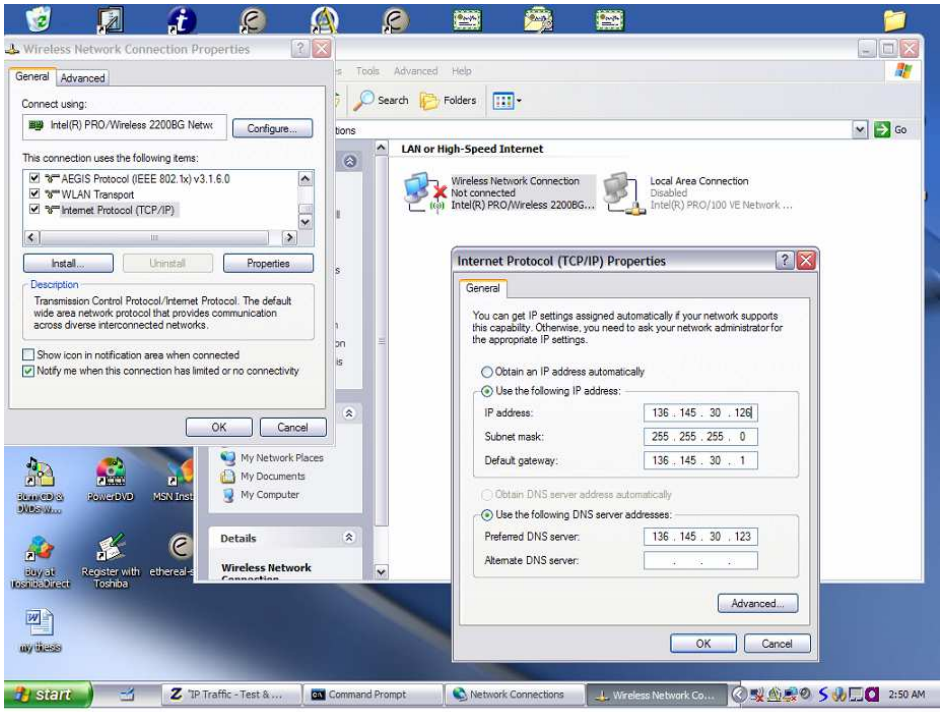

Figure B.1.1: Assigning a static IP address to a client

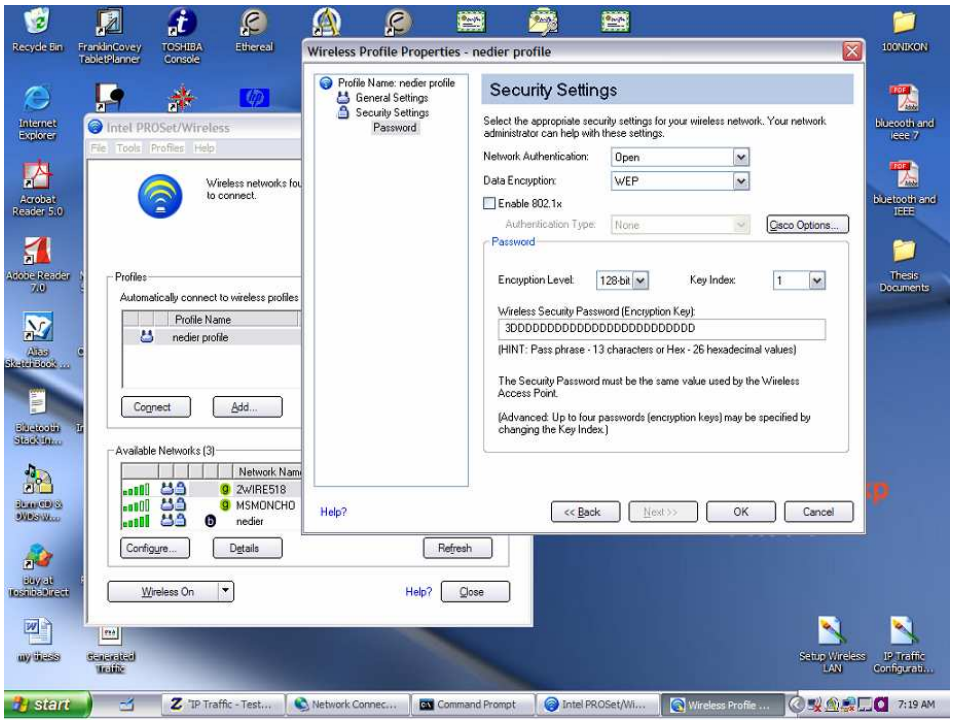

Figure B.1.2 Setup of the WEP Protocol with 128 bits

We configured the EAP-TLS to allow the client to authenticate to the network when it was being used (see Figure B.1.3) as security mechanism. Firstly, we right clicked on the wireless icon in the taskbar and we selected properties. A little window popped up in which we entered the profile name and the SSID setup on the access point and we clicked next. In the next window (Figure B.1.3), we enabled the 802.1x security method and we selected WEP as Data Encryption and TLS for EAP method. We also provided the certificate issuer from the server and specified the name of the radius server that authenticated the client.

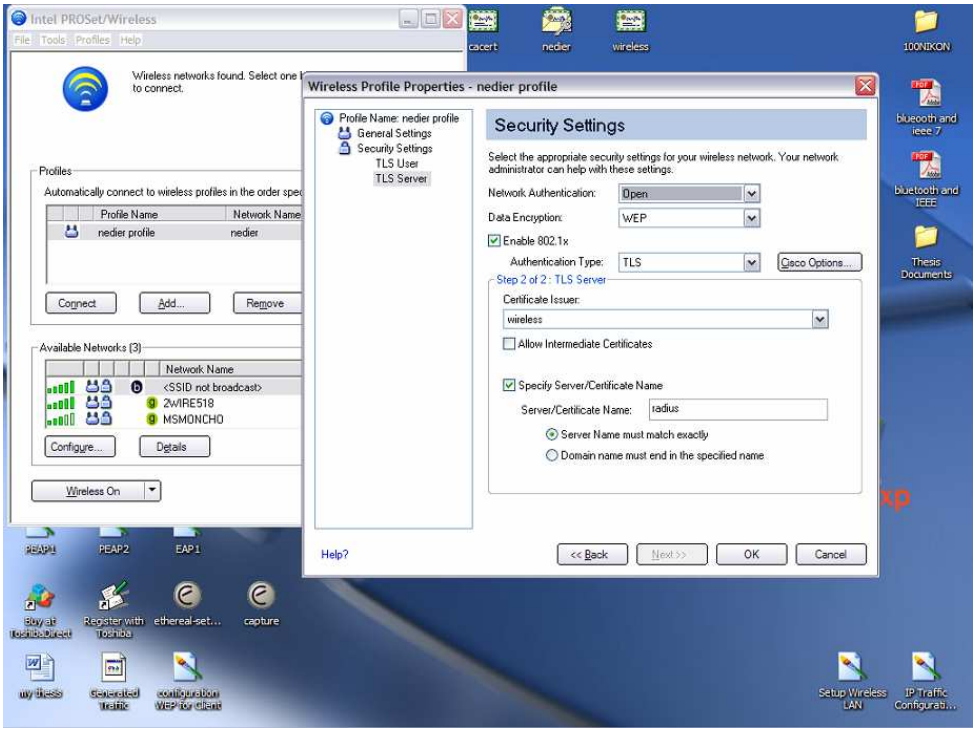

Figure B.1.3 Setup of the EAP-TLS

When the PEAP was used as security mechanism, we enabled the 802.1x security method and we selected PEAP as Authentication type. We also provided the authentication protocol

being used and we entered the user name and password for the client so he/she would be able to authenticate. Figure B.1.4 shows the configuration of the PEAP as security mechanism.

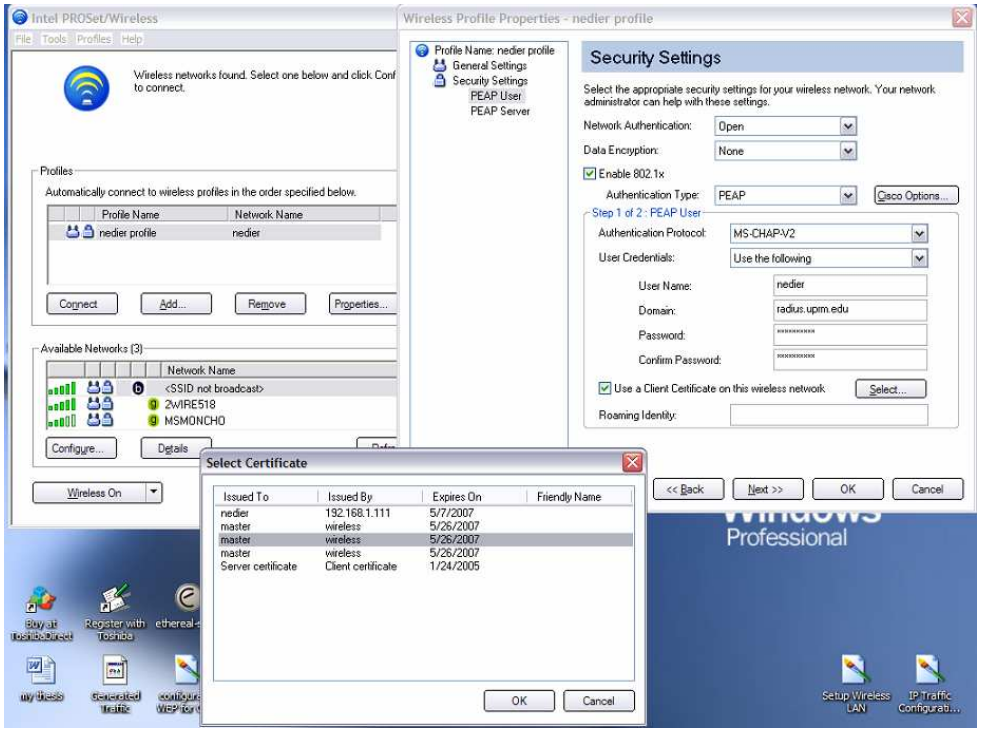

Figure B.1.4: PEAP Security Configuration

IP Traffic

The traffic generator uses in our experimental work has two operation modes, one for the clients and the other one for the server. Figure B.1.5 shows the traffic generator operating on the client side. Figure B.1.6 shows the parameters configuration window for entering the assumptions for the traffic being generated. To see that window and be able to enter information into it, we clicked on the parameters button.

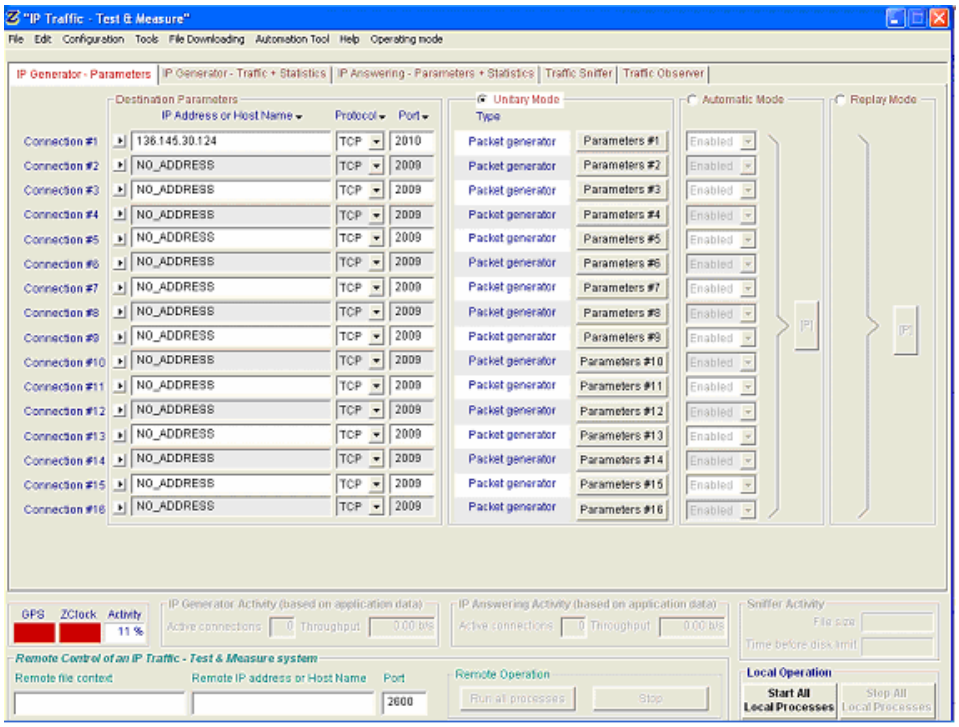

Figure B.1.5: IP Traffic Generator on client side

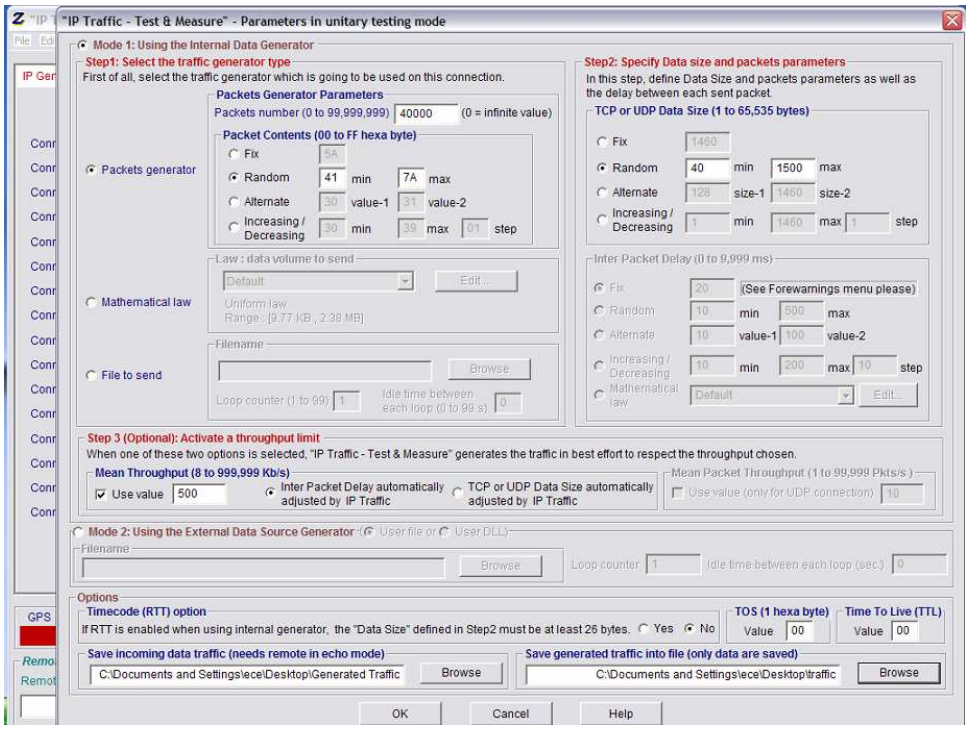

Figure B.1.6: IP Traffic Generator Parameters Window on client

B.2 Server Side

The setup of the security mechanisms was being done on the server using a web browser to access the interface of the access point. Once we accessed the interface of the access point, we used the security options provided by the manufacturer to setup the security mechanisms. We also used the Ethereal from the server side to capture packets and collected statistical results. The IP traffic was also used on the server side to receive traffic.

Access Point Configuration

Figure B.2.1 shows the configuration of the MAC authentication into the interface of the access point on the server side.

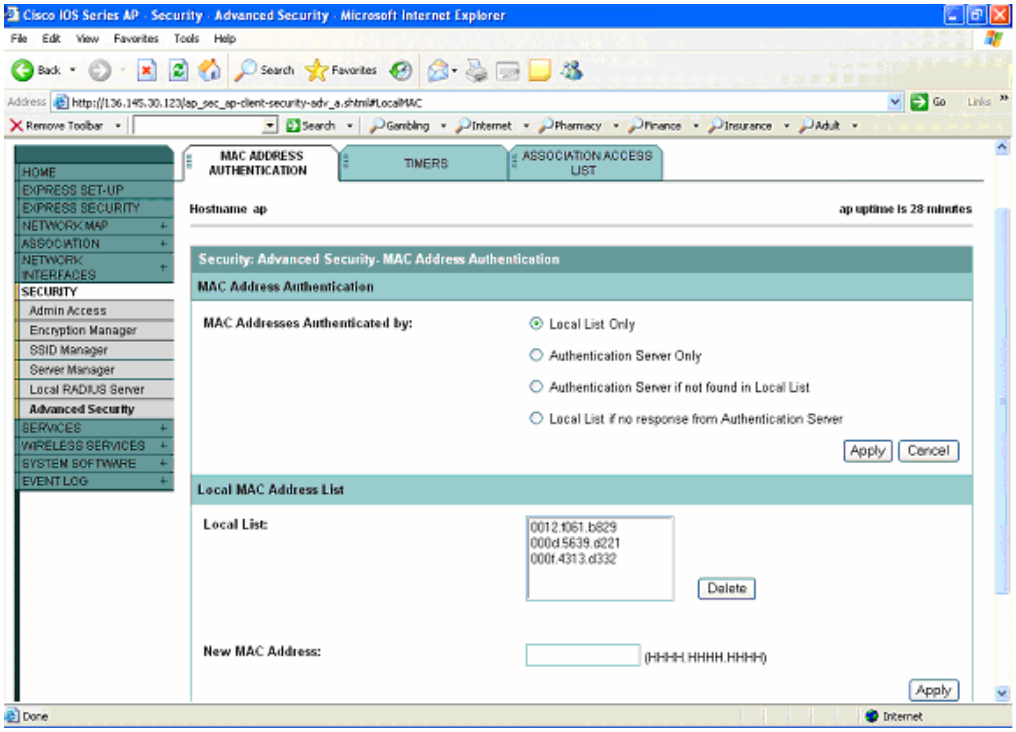

Figure B.2.1: MAC Authentication Configuration

Figure B.2.2 shows the setup of the WEP security protocol via the interface of the access point on the server side. We chose the “EXPREES SECURITY” option from the menu provided on the left part of the interface and then we selected the option: static WEP key. We selected the size of the key and we entered it.

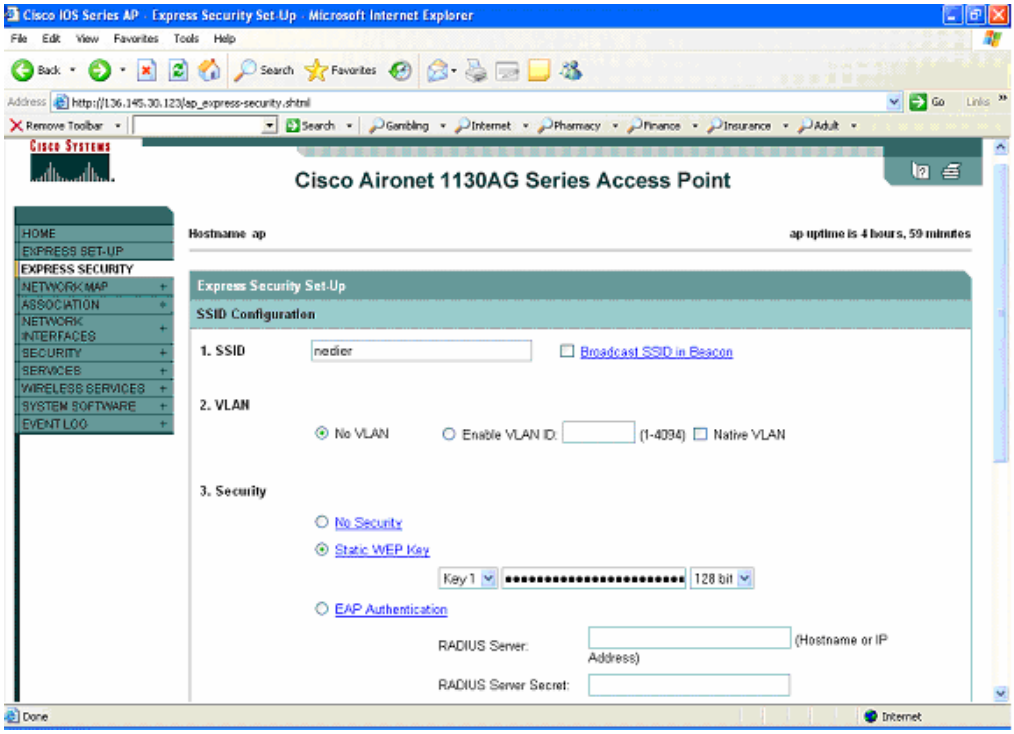

Figure B.2.2: WEP Security with 128 bits Setup

For the EAP-TLS configuration, we first clicked on security and then on encryption manager. It took us to the interface shows in Figure B.2.3. We created an SSID; we checked both “open authentication with EAP” and “Network EAP” options. We entered the IP address of our radius server in the EAP authentication customize box. The setup of the radius server into the access point interface is provided in Figure B.2.4.

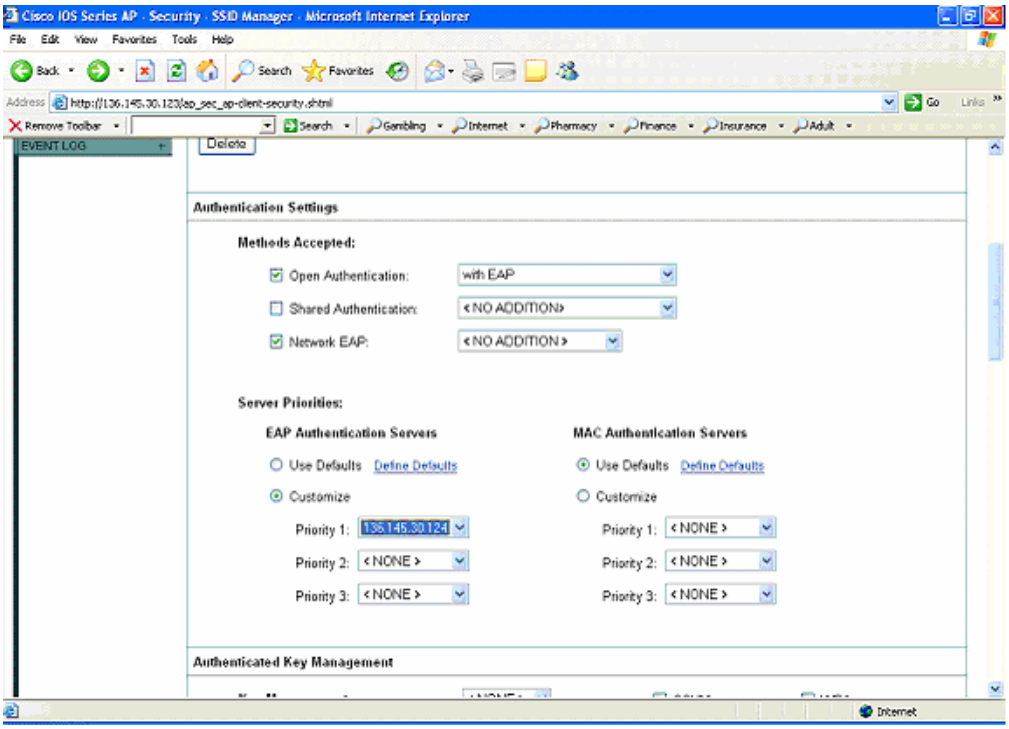

Figure B.2.3: EAP Authentication Setup in the Access Point Interface

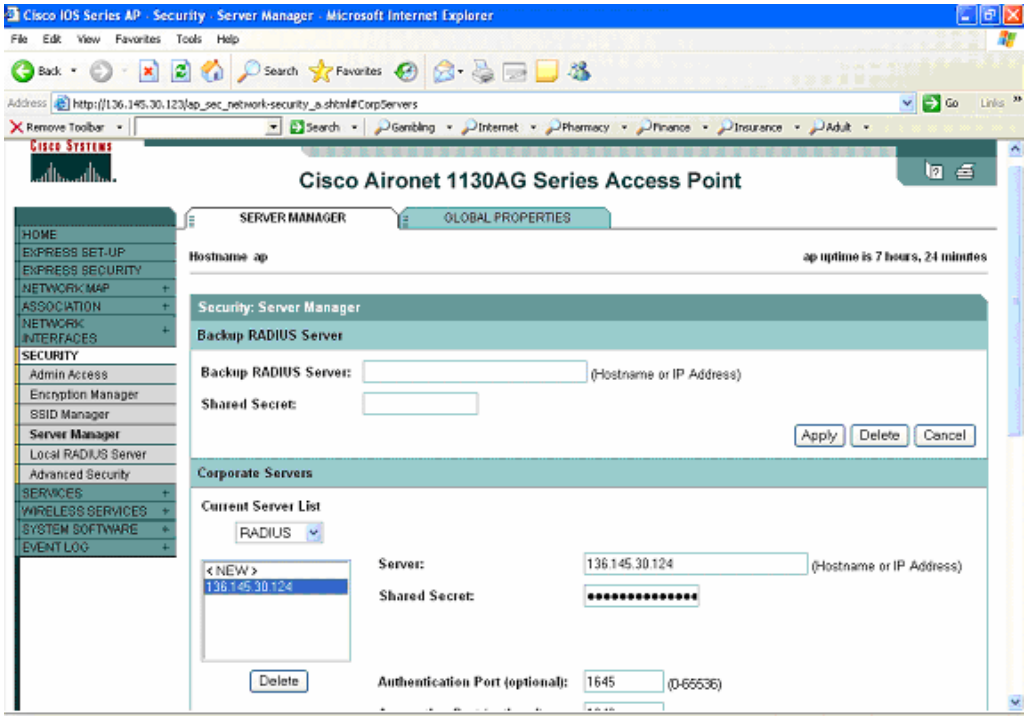

Figure B.2.4: Setup the Radius Server into the access point interface

Figure B.2.5 and B.2.6 show how to setup the PEAP security mechanism into the interface of the access point.

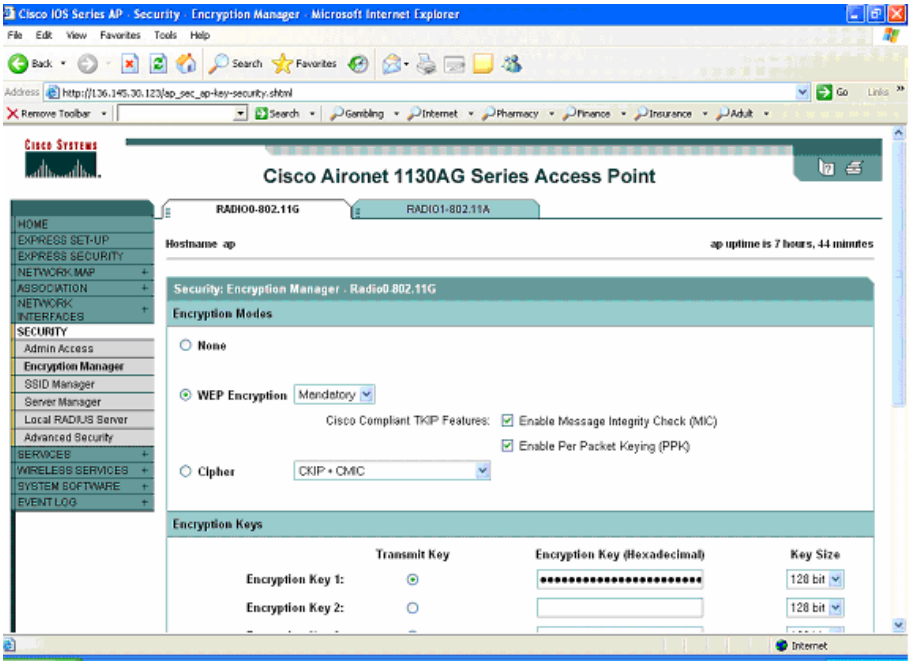

Figure B.2.5: First Part of Setting up PEAP into the Access Point

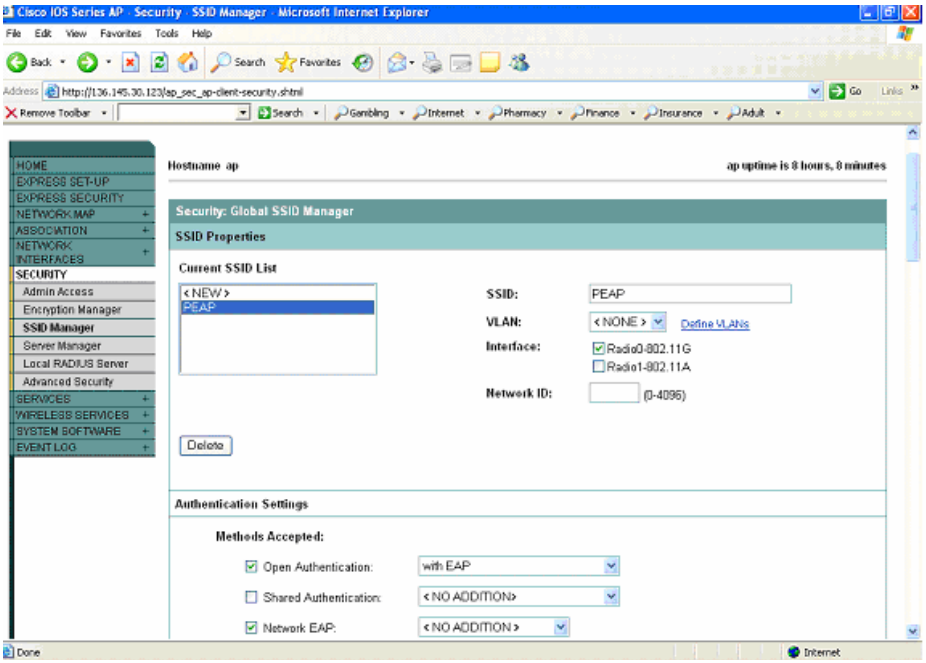

Figure B.2.6: Second Part of Setting up PEAP into the Access Point

Server Configuration

Figure B.2.7 shows the process of adding new clients to the Radius server. Under the Radius Server icon, we right clicked on the “Users” folder and we selected the “new user” option to create a new account on the server side.

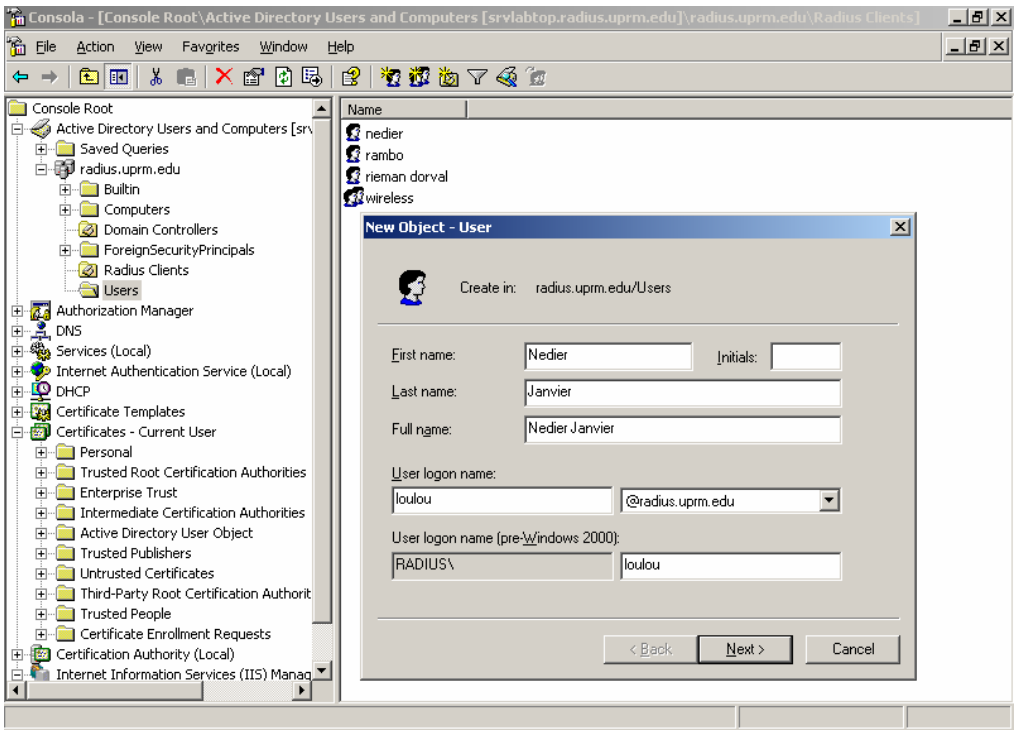

Figure B.2.7: Add a User or an Account to the Radius Server

Figure B.2.8 shows how to add a group policy for providing better security on the server side and B.2.9 shows the active directory of the users being added to the server.

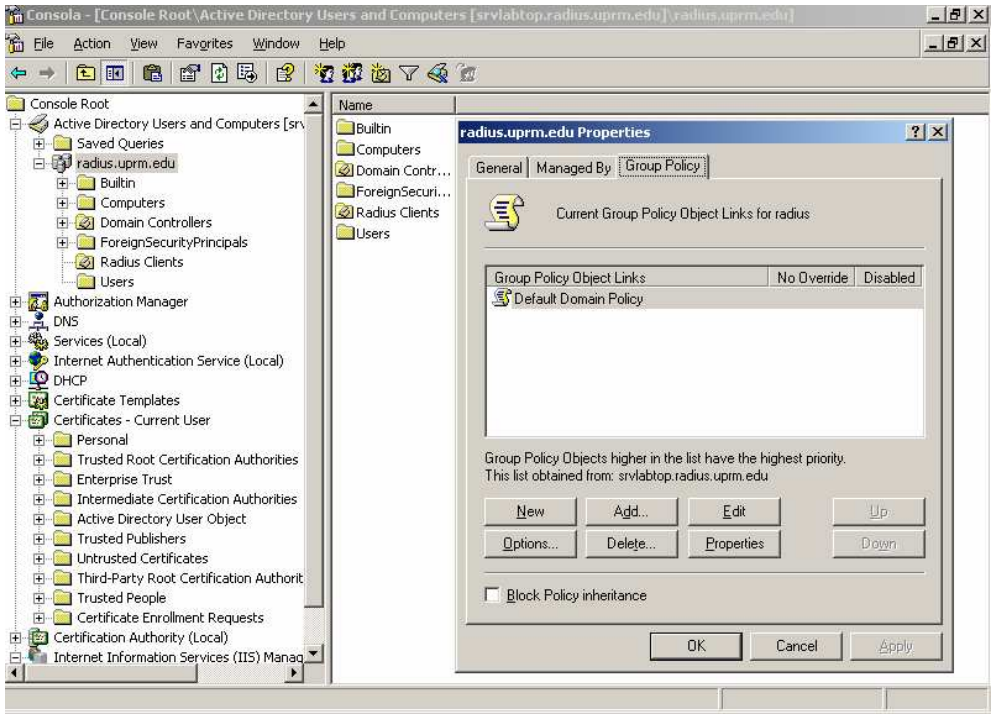

Figure B.2.8: Adding Group policy On the Server

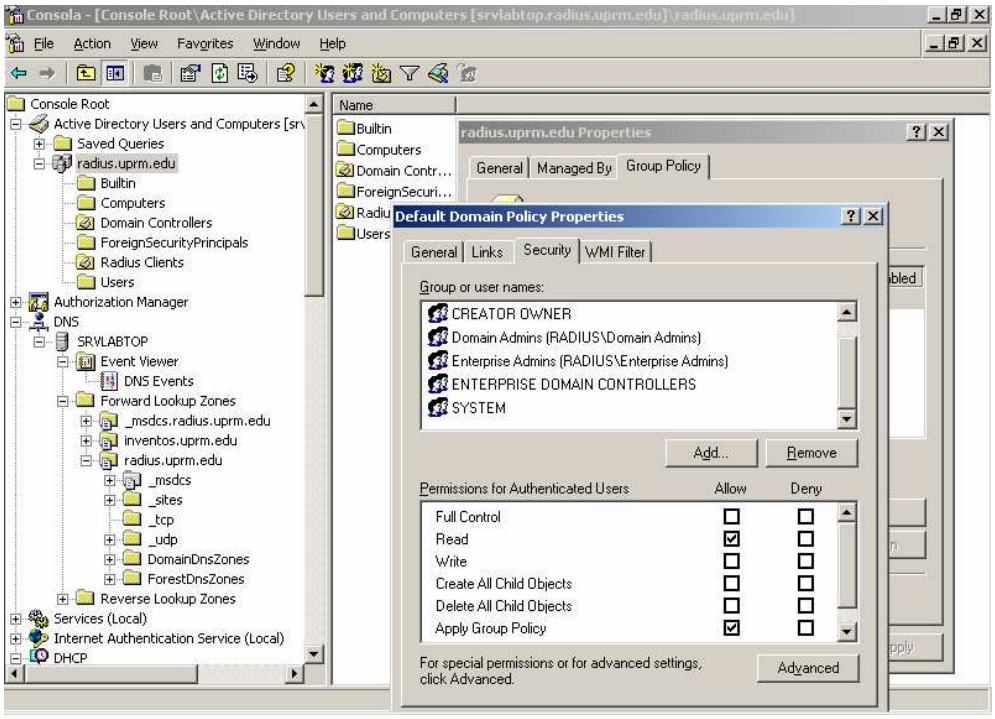

Figure B.2.9: Active Directory Users on the Server Side

A certificate was issued by the server for every client. Then, the client by using this certificate would be able to authenticate to the server every time he/she wanted to connect to the network. Figure B.2.10 shows a copy of the certificate issued by the server for the client with user name “rambo”.

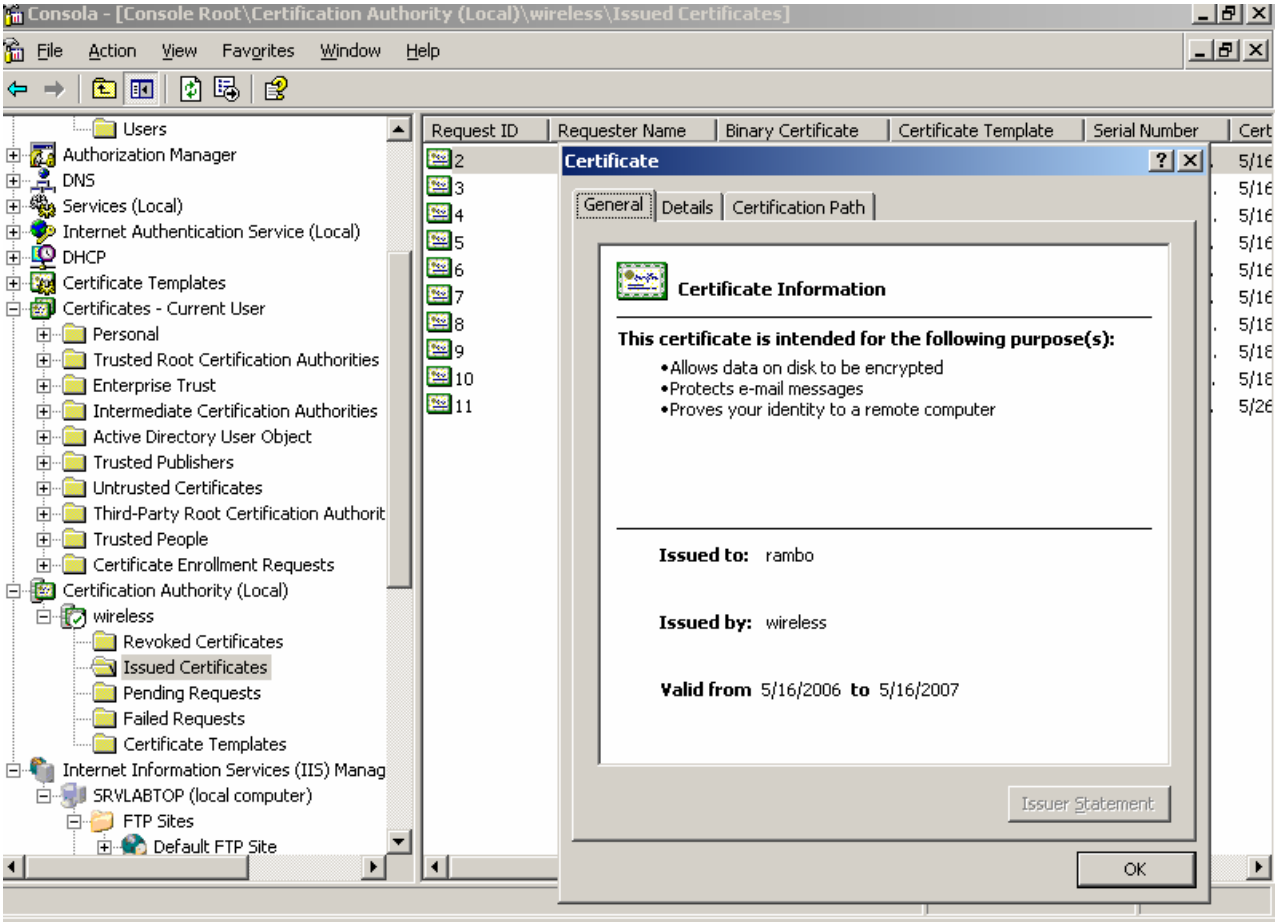

Figure B.2.10: User certificate Issued by the server

Ethereal

As mentioned in chapter 5, the ethereal software was used to capture packet and collect statistics results. In Figure B.2.11, we show the ethereal software displaying statistical results after capturing packets. We got the statistical popup window by choosing statistics from the main menu and by selecting summary from the popup menu.

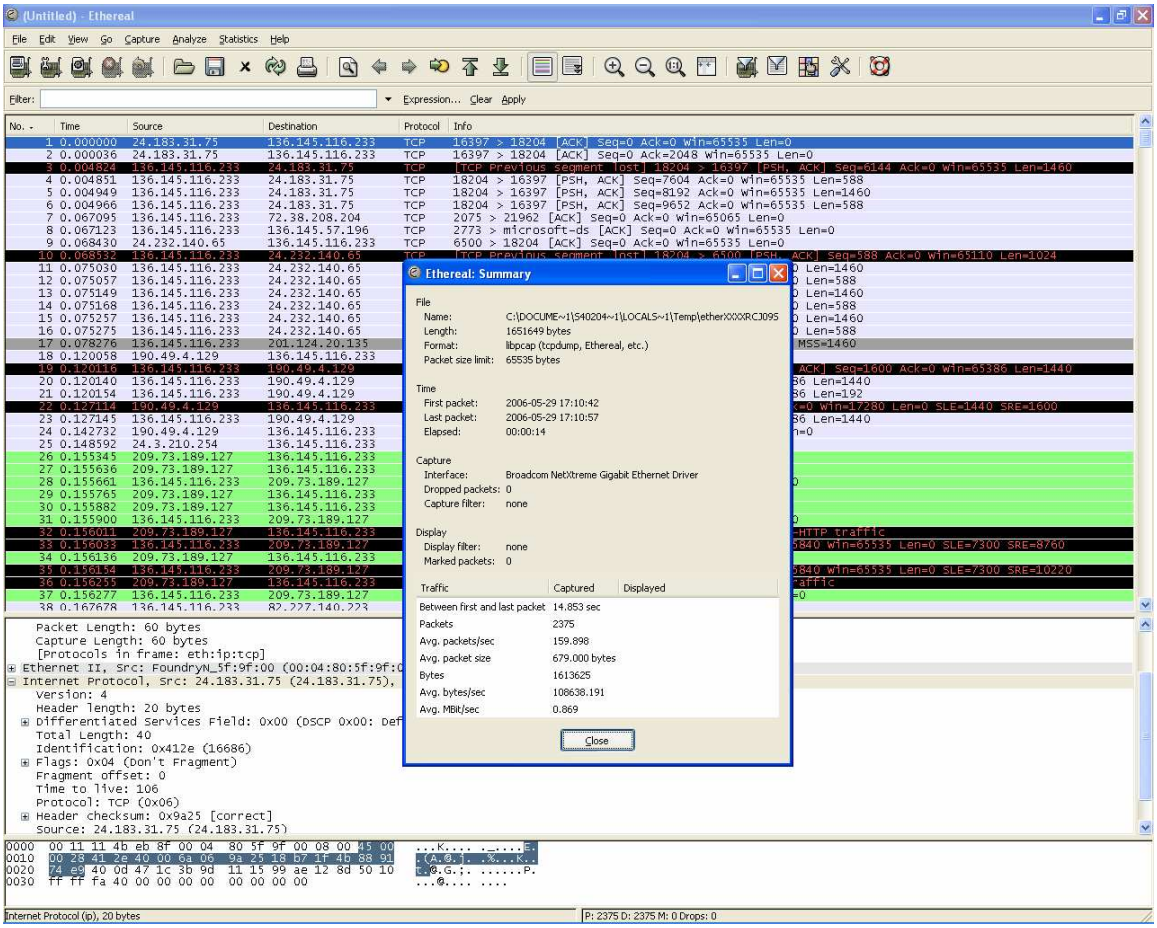

Figure B.2.11: Ethereal Software

IP Trafffic

The IP traffic generator software was also used on the server side. Figure B.2.12 shows the traffic generator running on the server side.

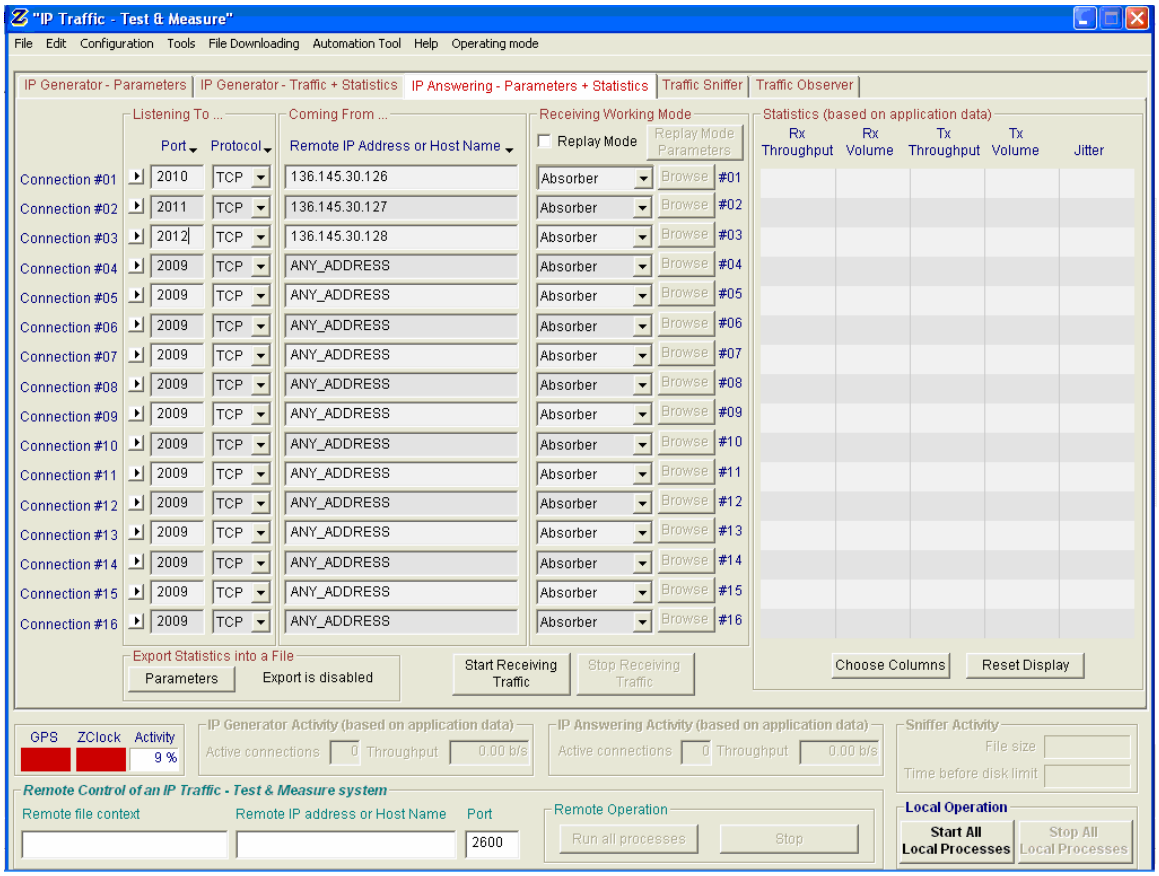

Figure B.2.12: Traffic Generator on the Server Side