

WIRELESS NETWORK SECURITY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ÇANKAYA UNIVERSITY

BY

ALİ KAHRAMAN

IN PARTIAL FULFILLMENT OF THE REQUIREMENT
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
COMPUTER ENGINEERING

APRIL 2006

Title of the Thesis : **Wireless Network Security**

Submitted by **Ali Kahraman**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University



Prof. Dr. Yurdahan GÜLER
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.



Prof. Dr. Mehmet R. TOLUN
Chairman of the Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.



Assist. Prof. Dr. Reza Hassanpour
Supervisor

Examination Date : 28 April 2006

Examining Committee Members


Prof. Dr. Hayri Sever (Başkent Univ.) 

Assist. Prof. Dr. Reza Hassanpour (Çankaya Univ.) 

Dr. Abdulkadir Görür (Çankaya Univ.) 

STATEMENT OF NON-PLAGIARISM

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Ali Kahraman
Signature : 
Date : 26.05.2006

ABSTRACT

Wireless Network security

Kahraman, Ali

M.S.c., Department of Computer Engineering

Supervisor : Dr. Reza Hassanpour

April 2006, 54 pages

Wireless Local Area Network, the most famous Wireless technologies have become increasingly popular in recent decade and has important role in our daily life and business. Wireless communications offer users and organizations many benefits like flexibility and portability, increased productivity and lower installation cost. But because of transmission media and weaknesses in wireless protocols there are many security risks and threat. Some of these risks are like wired networks some are exacerbated by wireless connectivity.

The architecture of a network defines the protocols and components necessary to satisfy application requirements. Like wired network the seven-layer Open System Interconnect (OSI) is the model for representing the various standards and interoperability of a wireless network.

The main goal of this thesis is to consider WLAN security and different type of WLAN security protocols produced for deploying in different layers and their weaknesses against security threats.

Key Words: WLAN Network, Security, Security Protocols, Layers, Weaknesses

ÖZ

Telsiz Ağ Güvenliđi

Kahraman, Ali

Yüksek Lisans, Bilgisayar Mühendisliđi Bölümü

Tez Yöneticisi : Dr. Reza Hassanpour

Nisan 2006, 54 sayfa

WLAN, en ünlü telsiz ağ teknolojisidir. Son yıllarda büyük hızla artarak yaygınlaşmakta ve günlük iş hayatımızda önemli rol oynamaktadır. Telsiz haberleşme kullanıcılarına esneklik, serbest dolşım, düşük montaj maliyeti ve yüksek verimlilik gibi çok sayıda fayda sağlamaktadır. Fakat telsiz ağların, gönderim ortamı olarak havayı kullanmasından ve güvenlik protokollarındaki yetersizliklerden dolayı bir çok güvenlik sorunu mevcuttur. Bu sorunların bir kısmı telli ağlarda mevcut olan sorunların aynısı olup fakat diđer kısmı sadece telsiz ağlara özgüdür.

Bir ađın mimarı, gereken uygulama ihtiyalarını gidermek iin ihtiya duyulan protokol ve birimleri tanımlar. Telli ađlarda olduđu gibi, OSI modelinin yedi katmanı, farklı gvenlik standartlarını temsil eder.

Bu tezin esas amacı WLAN teknolojisinin gvenliđi ve farklı katmanlarda uygulanan gvenlik protokollerini ve bu protokollerin varsa gvenlik aıklarını incelemektir.

Anahtar Kelimeler: WLAN Ađ. Gvenlik, Gvenlik Protokol, Katmanlar, Zayıflık

ACKNOWLEDGEMENTS

I express sincere appreciation to my supervisor Dr. Reza Hassanpour for his directorship and guidance throughout the research. I offer my great thanks to my wife for her unlimited support and insight.

TABLE OF CONTENTS

STATEMENT OF NON-PLAGIARISM	iii
ABSTRACT	iv
ÖZ	vi
ACKNOWLEDGEMENTS	viii
TABLE OF CONTENTS	ix
CHAPTERS:	
1- INTRODUCTION	1
1.1 Threat and Vulnerabilities	2
1.2 Contribution of Thesis.....	3
1.3 Outline of Thesis	4
2- WIRELESS LOCAL AREA NETWORK	5
2.1 Wireless LAN Overview	5
2.1.1 IEEE 802.11	6
2.1.2 HiperLAN.....	8
2.2 WLAN Architecture.....	9
2.3 WLAN Technology.....	10
2.3.1 RF Technology	11
2.3.1.1 Spread Spectrum Techniques.....	12
2.3.1.2 Frequency Hopping Spread Spectrum Technique ..	12
2.3.1.3 Direct Sequence Spread Spectrum Technique.....	14
2.4 WLAN Advantages and Disadvantages.....	15
3- SECURITY THREATS AND RISK MITIGATIONS.....	17
3.1 Security Vulnerability and Threats	18
3.2 Other Security Risks	20

3.3 Risk Mitigations.....	21
3.3.1 Software Solutions.....	22
3.3.1.1 Access Point Configuration	22
3.3.1.2 Software Upgrades.....	24
3.3.1.3 Secure the WLAN with Network Access Authentication.....	25
3.3.1.4 Encryption.....	25
3.3.1.5 Personal Firewalls.....	26
3.3.1.6 IDS	26
3.3.2 Hardware Solutions	28
4- COMPARISON OF SECURITY METHODS IN DIFFERENT LAYERS	31
4.1. Security Methods Used in Physical Layer	31
4.1.1 Spread Spectrum Methods.....	31
4.1.2 OFDM Method	32
4.2. Security Method Used in Data link Layer.....	33
4.2.1 The WEP Protocol.....	34
4.2.2 WPA and WPA2.....	38
4.2.2.1 Enterprise Mode Components for Authentication..	40
4.2.2.2. How WPA and WPA2 Authentication Works.....	41
4.2.2.3. How WPA Encryption with TKIP Works	42
4.2.2.4. How WPA2 Encryption with AES Works.....	43
4.2.2.5 Problem with 802.1x/EAP	43
4.2.2.6 Problem with WPA-PSK	44
4.3. Security Method Used in Network Layer	44
4.3.1. IP Security (IPsec).....	45
4.3.2. Mobile IP	46
4.4. Security Method Used in Transport Layer	48
4.4.1 How Does Secure Socket Layer (SSL) Work?.....	49
4.4.2 Limitation for SSL.....	50
5- CONCLUSION	52
REFERENCES	R1

LIST OF TABLES

TABLES:

Table 1 - The IEEE 802.11x Standards and General Specifications....	7
Table 2 - The IEEE 802.11x Improved Standards and General Specifications.....	8
Table 3 - The IEEE 802.11x Improved Standards and General Specifications.....	9
Table 4 - WPA and WPA2 Mode Types.....	40

LIST OF FIGURES

FIGURES

Figure – 1 : Converted of 802.11 to Wired Network by APs.....	10
Figure – 2 : Wireless ISM Bands.....	11
Figure – 3 : FHSS Technique	13
Figure – 4 : Bit Pattern in DSSS Technology.....	14
Figure – 5 : Coded Signal in DSSS Technology	14
Figure – 6 : The Parking Lot Attack.....	18
Figure – 7 : IDS Architecture	28
Figure – 8: OFDM Modulation.....	33
Figure – 9 : Wireless Security of 802.11 in Typical Network.....	34
Figure – 10 : Shared-key Authentication Message Flow.....	35
Figure – 11 : Encrypted WEP Frame.....	36
Figure – 12 : WEP Privacy Using RC4 Algorithm.....	36
Figure – 13 : WPA and WPA2 Components.....	41
Figure – 14 : Isec Transport and Tunnel Mode	46
Figure - 15 : Mobile IP Elements	46

ABBREVIATIONS

3DES	Triple DES
AES	Advanced Encryption Standard
AH	Authentication Header
AP	Access Point
ATM	Asynchronous Transfer Model
BSA	Basic Service Area
BSS	Basic Service Set
CCMP	Counter Mode CBC MAC Protocol
CDMA	Code Division Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CDPD	Cellular Digital Packet Data
CoA	Care of Address
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Control Protocol
DoS	Denial of Service
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESP	Encapsulated Security Payload
ESS	Extended Digital Assistant
ETSI	European Telecommunication Standard Institute
FA	Foreign Agent

FCC	Federal Communication Commission
FHSS	Frequency Hopping Spread Spectrum
GHz	Giga Hertz
GSM	Global System for Mobile communication
HA	Home Agent
HIDS	Host-base IDS
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association Key Management Protocol
ISM	Industrial, Scientific, Medical
LLC	Logical Link Control
MAC	Media Access Control
MIC	Message Integrity Check
MITM	Man In The Middle
MN	Mobile Node
OFDM	Orthogonal Frequency Division Multiplexing
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PMK	Pair wise Master Key
PSK	Pre-Shared Key
PTK	Pair wise Transient Key
RADIUS	Remote Authentication Dial-In User Service
RSA	Rivest-Shamir-Adelman
RSN	Robust Security Network
SSID	Service Set Identifiers
SSL	Secure Socket Layer
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
TPC	Transmission Power Control

VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network

CHAPTER 1

INTRODUCTION

Wireless network technologies enable one or more devices to communicate without physical connection. Wireless network technologies generally use radio frequency for transmitting data, whereas wired technologies use cables. Wireless technology cover a broad range of differing capabilities oriented toward different use and needs.

Wireless networks can be mainly categorized in three groups based on their coverage area: Wireless Wide Area Networks (WWAN), WLANs, and Wireless Personal Area Networks (WPAN). WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), and Mobitex. WLAN, representing wireless local area networks, includes 802.11, HiperLAN, and several others. WPAN, represents wireless personal area network technologies such as Bluetooth and IR [1].

Wireless technologies use wavelengths ranging from the radio frequency (RF) band up to the IR band. The frequencies in the RF band cover a significant portion of the EM radiation spectrum, extending from 9 kilohertz (kHz), the lowest allocated wireless communications frequency, to thousands of gigahertz (GHz). As the frequency is increased beyond the RF spectrum, EM energy moves into the IR and then the visible spectrum.

Wireless network (WLAN) technology is the fastest growing segment of the communications market. According to Gartner research [2], worldwide shipments of WLAN units are forecasted to grow at an annual rate of 42% through 2007.

The major reason of this growth is the strong return on investment afforded by much lower installation costs, higher availability, and mobile data connectivity. Another significant advantage of WLAN technology is that there is no so many effort required to deploy wireless networks.

However, there are serious concerns about the security of wireless networks, source of risks in wireless networks is that the communications medium, the airwave, is open to intruders.

The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks typically associated with wireless communications. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

1.1 Threat and Vulnerabilities

Specific threats and vulnerabilities to wireless networks and handheld devices include the following:

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- DoS attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.

- Malicious entities may be able to violate the privacy of legitimate users and be able to track their movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Malicious entities may, through wireless connections, connect to other agencies or organizations for the purposes of launching attacks and concealing their activities.
- Malicious entities may use third-party, insecure wireless network services to gain access to an agency's or other organization's network resources.

1.2 Contribution of Thesis

The purpose of this thesis covers details specific to WLAN technology and the security protocols deploy on different WLAN layers to mitigate the threats and vulnerabilities. Advantages and disadvantages of security protocols will be explained individually and will be compared to each other.

Also the most common implementation requiring security is infrastructure mode, most security measures center around this design, so securing an infrastructure mode wireless network will be focused.

This document does not address the WWAN and WPAN and their security protocols

1.3 Outline of Thesis

Following pages of this thesis is organized as follows:

- Chapter 2 provides an overview of wireless Local Area Network technology.
- Chapter 3 discusses the wireless security threats and risk mitigations
- Chapter 4 explains the different security methods and shows their weaknesses.
- Chapter 5 summarizes the conclusion of this thesis

CHAPTER 2

WIRELESS LOCAL AREA NETWORK

2.1 Wireless LAN Overview

WLAN history back to the mid-1980 when the Federal Communications Commission (FCC) first made the RF spectrum available to industry. During first ten years there was a relatively slow growing. WLAN start to growth sharply when the bandwidth increased by the IEEE 802.11 standards.

Wireless Local Area Networks (WLAN), supply high speed duplex broadband data communication and use radio frequency or infra-red instead of cables for data communications within a relatively small geographical area with compared to their wired counterparts. Congress halls, Hotels, Airports and university campuses are the places mostly use the WLANs.

WLAN systems; supplies different availability like wideband internet service, programming over servers, files sharing and electronic mail service between the users in the same network. Also because of wireless technology WLAN can be successfully used in streets, parks and similar open places. But its coverage is very limited around 25-100 meter.

Wireless LANs have become widespread with providing standards by Institute of Electrical and Electronics Engineers (IEEE). Also cost of wireless equipments came down with accepting these standards. IEEE 802.11 and HiperLAN are two types of WLAN technology and standard that are available for consumers. IEEE 802.11 is American based and HiperLAN was developed by European Telecommunication Standards Institute (ETSI). These two types of technologies are considered below.

2.1.1 IEEE 802.11

The IEEE initiated the 802.11 project in 1990 with a scope “to develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within an area.” Later, in 1997 the first IEEE 802.11 standard was published. Then, in 1999, the IEEE ratified the 802.11a and the 802.11b wireless networking communication standards.

The 802.11a standard currently operates at the bandwidth of 300MHz in the 5GHz band using Orthogonal Frequency Division Multiplexing (OFDM) technology [3], and the 802.11b standard operates at 2.4 GHz and 2.5GHz Industrial, Scientific and Medical (ISM) frequency band using Direct Sequence Spread-Spectrum technology (DSSS). The 802.11b WLAN technology permits transmission speeds of up to 11 Mbps. This means that 802.11b and 802.11a are not compatible; however, these two standards are able to coexist due to the fact that there is no signal overlap.

Summary of the various 802.11 standards is provided in table 1.

Table 1 - The IEEE 802.11x Standards and General Specifications

Standard Name	Frequency Band and Link Rate	Modulation Technique -- Number of Channel	Security	Description
802.11	2.4 GHz ISM with rate of 2 Mbps	FHSS or DSSS -- 3 radio channel	WEP or WPA	First standard
802.11a	5 GHz with rate of 54 Mbps	OFDM -- It specifies eight available radio channels	WEP or WPA	This is a physical layer standard. For multiple users applications and high data communication
802.11b	2.4 GHz ISM with rate of 11 Mbps	DSSS -- 3 radio channel	WEP or WPA	This is a physical layer standard. Widespread use and low cost systems
802.11g	2.4 GHz ISM with rate of 54 Mbps	DSSS or OFDM -- 3 radio channel	WEP or WPA	This standard is the 802.11b for high speed rate transmissions.

For improving WLAN implementation and solving the problems exist in 802.11 first standards, other standards of 802.11x were published by IEEE. Summary of these 802.11x standards is given in table 2.

Table 2 - The IEEE 802.11x Improved Standards and General Specifications

802.11d	This standard is supplementary to the MAC layer in 802.11 to promote worldwide use of 802.11 WLANs. The 802.11 standards can not legally operate in some countries; the purpose of 802.11d is to add features and restrictions to allow WLAN to operate within the rules of these countries.
802.11h	This standard is supplementary to the MAC layer to comply with European regulations with transmission power control (TPC) and dynamic frequency selection (DFS) for 5 GHz WLANs at the rate of 54 Mbps.
802.11i	This standard is supplementary to the MAC layer to improve security. It will apply to 802.11 physical standards a, b and g. It provides an alternative to WEP with new encryption methods and authentication procedures.
802.11e	This standard is supplementary to the MAC layer to provide QoS. It will apply to 802.11 physical standards a, b and g. The purpose is to provide classes of service with managed levels of QoS for data, Voice, and video applications.
802.11f	The standard defines the registration of access points within a network and the interchange of information between access points when a user is handed over from one access point to another.

2.1.2 HiperLAN

HiperLAN (High Performance Radio LAN), has high communication rate, was developed as a WLAN standard by European countries. It has two types, HiperLAN1 and HiperLAN2. Both types were defined by ETSI and use OFDM method to work in 5 GHz frequency band. HiperLAN's have the same characteristic and capacity as 802.11 standards [4, 5]. Unlike IEEE 802.11, which was based on products, HiperLAN was based on certain functional requirements specified by

ETSI. HiperLANs have coordinated with the 802.11a in the PHY layer specification and current work on the MAC to support QoS.

HiperLAN1, started in 1992 and completed in 1997, works in 5 GHz unlicensed band at the rate of 20 Mbps. HiperLAN2 use the same frequency but support the data rate of up to 54 Mbps with this PHY layer opens an environment for innovative wireless video applications [6].

802.11a restrict especially the multimedia application. However HiperLAN2 provide good performance in transferring video with high data rate, although it is a more expensive solution. HiperLANs are ATM technology based and have better service quality with respect to 802.11. It can be said that within present WLAN applications, HiperLANs are the best alternative technology, but HiperLANs are not as prevalent as 802.11. Table 3 shows the comparison between HiperLAN and 802.11a standard.

Table 3 - The IEEE 802.11x Improved Standards and General Specifications

Specifications	HiperLAN2	802.11a
Data Rate	54 Mbps	54 Mbps
Throughput	32 Mbps	32 Mbps
Frequency Band	5 GHz	5 GHz
Frequency Selection	Single Carrier	Single Carrier
Media access	TDMA/TDD	CSMA/CA
Encoding	DES, 3DES	40 bit RC4
Modulation Method	OFDM	OFDM

2.2 WLAN Architecture

WLAN networks exist in either *infrastructure* or *ad hoc* mode. Ad hoc networks have multiple wireless clients talking to each other as peers to share data among themselves without the aid of a central Access Point. An infrastructure WLAN consists of several clients talking to a central

device called an Access Point (AP), which is usually connected to a wired network like the Internet or a corporate.

The Basic Service Area (BSA) is the coverage area one access point. The Basic Service Set (BSS) is a set of stations controlled by one access point. The distribution system (DS) is the fixed (wired) infrastructure [7] used to connect a set of BSS to create an extended service set (ESS). By deploying multiple APs with overlapping coverage areas, organizations can achieve broad network coverage.

Wireless equipments can be a laptop, PDAs or notebook personal computer (PC) with a wireless NIC. The card in the laptop and the AP support the MAC and PHY layers of the IEEE 802.11, the rest of the AP device acts as a bridge to convert the 802.11 protocol to MAC and PHY layer of the backbone DS, that is typically an IEEE 802.3 Ethernet LAN (Figure -1). Laptops connect to the LAN through the AP to communicate with other devices, such as the servers.

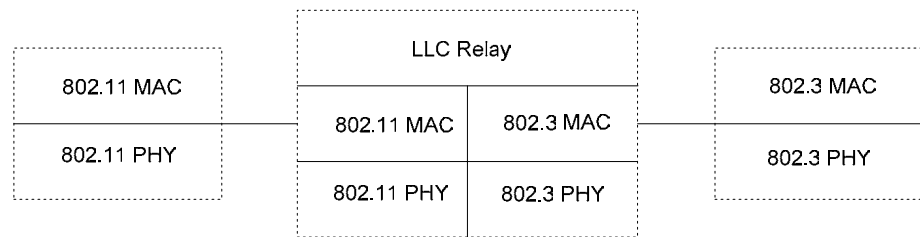


Figure – 1 : Converted of 802.11 to Wired Network by APs

2.3 WLAN Technology

There are several technologies available for data transmission in wireless networks. The most important technologies are the electromagnetic signals using RF and infra-red [8]. RF and Infra-red technologies are used in wireless LANs and each with its own set of benefits and compromises. Organization can select the right technology with respect to their requirements to improve system productivity and satisfaction. Nowadays, as a result of improvement in multimedia applications, high data rate need become a very important criterion for

competition between technologies. The coverage area and sensitivity against interference are the other important subjects. RF technology is used in practice due to high data rate and passing through obstacle.

2.3.1 RF Technology

RF technology use electromagnetic signals to provide communications. There is a widespread use of this technology in wireless LANs. But the frequency spectrum is limited and should be used productively. Also frequency band requirement rise with increasing the number of users and systems. Intensive use of frequency band, increase the frequency pollution and interference risk. For that reason RF technologies which use frequency spectrum productively and do not affected from interferences, were improved in last years.

The ISM band has become popular for wireless communications because it is available worldwide and free for all RF users. ISM bands assigned in 13560 kHz, 27120 kHz, 40.6 MHz, 915 MHz, 2450 MHz, 5800 MHz and 24.125 GHz for central frequency all over the world by ITU. The bands that are technically suitable for WLAN are shown in figure – 2 [9,10].

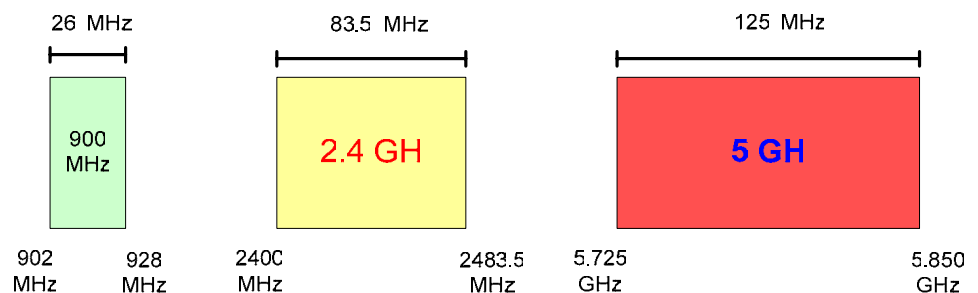


Figure – 2 : Wireless ISM Bands

ISM band was assigned first to other radio users, so the WLAN systems accept the probable interference from the beginning. This condition make absolutely necessary to improve and use a technology with resistant to interference for WLAN systems. Spread spectrum is one of basic techniques used in RF technology. The main difference between

the spread spectrum transmission and traditional radio modem technologies which are using narrow band is that the transmitted signal in spread spectrum systems occupies a much larger bandwidth than the traditional radio modems where the transmitted signal has a bandwidth of the same order as the information signal at base band.

2.3.1.1 Spread Spectrum Techniques

Spread spectrum technology was first introduced about 50 years ago by the military who was seeking ways to prevent radio signals from being monitored or blocked by hostile parties. It was designed to be resistant to noise, interference, jamming, and unauthorized detection. Spread spectrum transmitters send their signals out over a multiple range of frequencies at very low power, in contrast to narrow band radios that concentrate all of their power into a single frequency. There are several ways to implement spread spectrum transmission, the techniques specified in the IEEE 802.11 Wireless LAN standard are frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS).

2.3.1.2 Frequency Hopping Spread Spectrum Technique

Some wireless local-area network products use the frequency hopping method of spreading their signals. In order to avoid jamming, the transmitter shifts the center frequency of the transmitted narrow band signal at random but in known order. FHSS technique is shown in figure – 3.

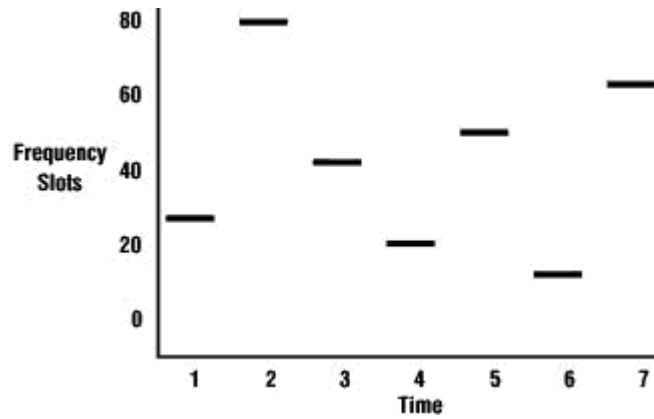


Figure – 3 : FHSS Technique

The range of available frequencies in the ISM (Industrial Scientific Medical) band of 2.400 - 2.483 GHz is divided into a series of 1MHz channels up to 79 separate and distinct channels. Transmissions are sent over each of these channels in what appears to be a random sequence (called a “pseudo-random sequence”) such as channel 1, channel 32, channel 3, channel 56, etc. The radio switches frequencies many times a second, transmitting on each channel for a fixed amount of time, and then proceeding on to the next channel in its sequence, covering all of the channels before repeating the sequence. Without knowing how long to stay on each channel (the “dwell time”) and what the hopping pattern is, it is impossible for a non-participating station to receive and decipher the data. The frequency hopping physical layer has 22 hop patterns to choose from. The frequency hopping physical layer is required to hop across the 2.4GHz ISM band covering 79 channels. Each channel occupies 1 MHz of bandwidth and must hop at the minimum rate specified by the regulatory bodies of the intended country. A minimum hop rate of 2.5 hops per second is specified for the United States.

FHSS systems may have data speed limitations and be shorter in range. FHSS designs are easier to build and therefore cost less. They are very good at avoiding narrow band interference and unauthorized user access due to their frequency hopping nature. They are also scalable in the many separate networks can be co-located in the same area without interfering with each other.

2.3.1.3 Direct Sequence Spread Spectrum Technique

The DSSS physical layer uses an 11-bit Barker Sequence to spread the data before it is transmitted. Each bit transmitted is modulated by the 11-bit sequence. This process spreads the RF energy across a wider bandwidth than would be required to transmit the raw data. The receiver disspreads the RF input to recover the original data. The undefined receiver in the network can perceive the DSSS signal as a low power wide band noise. The advantage of this technique is that it reduces the effect of narrowband sources of interference. DSSS technique provides a bit patterns for each data bit as shown in figure 4. This bit pattern is called “chip” or “chipping code”. The actual signal and coded signal can be seen in figure – 5.

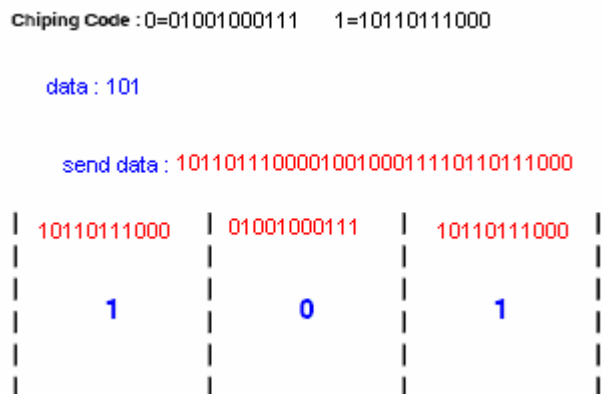


Figure – 4 : Bit Pattern in DSSS Technology

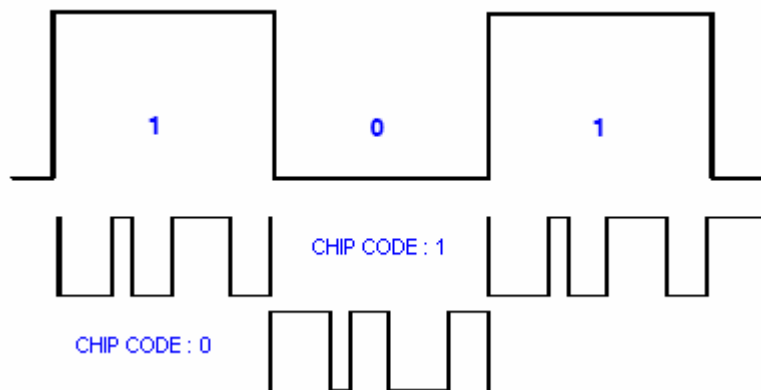


Figure – 5 : Coded Signal in DSSS Technology

The spreading architecture used in the direct sequence physical layer is not to be confused with CDMA. All 802.11 compliant products utilize the same PN code and therefore do not have a set of codes available as is required for CDMA operation.

DSSS systems are harder to build, have high user density limitations and typically costs more to build. It should always have a slight data speed advantages over frequency hopping systems and will have a range advantage.

2.4 WLAN Advantages and Disadvantages

Wireless local area network (WLAN) has some general advantages and disadvantages with compared to their wired counterparts.

Some advantages of WLANs are:

- **Mobility and Flexibility:** Within radio coverage, nodes can communicate from everywhere and without further restriction.
- **Planning:** It does not need for wiring planning. For wired networks, additional cabling with the right plugs have to be provided
- **Designing:** Wireless networks allow for the design of small, independent devices which can for example be put into a packet like PDA.
- **Robustness:** Wireless network can survive disasters like earthquakes.
- **Cost:** After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a wireless network will not increase the cost.

WLANs also have several disadvantages:

- **Quality of service:** Wireless typically offer lower quality than their wired counterparts. The reasons are lower bandwidth due to

limitation in radio transmission and higher error rates due to interference.

- Proprietary solution: Lack of standards and compatibility between wireless products.
- Restrictions: Wireless LAN coverage area is limited to AP and antenna coverage.
- Data rate: Data rate transmission in wireless LAN is very low with respect to wired network.
- Safety and security: the free-space wireless link is more susceptible to eavesdropping, fraud and unauthorized transmission.

CHAPTER 3

SECURITY THREATS AND RISK MITIGATIONS

While wireless networking has several advantages over a traditional wired LAN, however it introduces security risks that a wired LAN is not susceptible to. Enterprises that deploy this technology must understand and deal with the security issues related to radio transmission. Radio waves cannot be controlled, and they travel freely through most physical barriers, easily spreading confidential data beyond the walls of an office or home. If it is not handling properly, this potentially creates a major security hole in a network.

Using of wireless access points (APs) with very little configuration, one is able to set up a wireless network, and roam anywhere within a 300 foot or more region without the traditional network Ethernet. This makes the same network available to any other PC that is also equipped with a wireless network card. Without proper security precautions, intruders can freely access your network. The attacker can implement the “parking lot” attack, see figure – 6, where the attacker sits in the organization’s parking lot and accesses hosts on the internal network.

Unprotected wireless networks essentially “open the front door” of your network to intruders that can access shared drives and data, sniff every packet on your network, read emails, access web sites, and capture data

for further analysis, and take as long as they need to crack the rest of your system.

This chapter will review the threats and attacks in wireless LANs and also the specific techniques to mitigate these threats. Some of the wireless attacks are probably found similar to those mounted on wired networks with minor updates, Whereas the others are unique to wireless LANs.

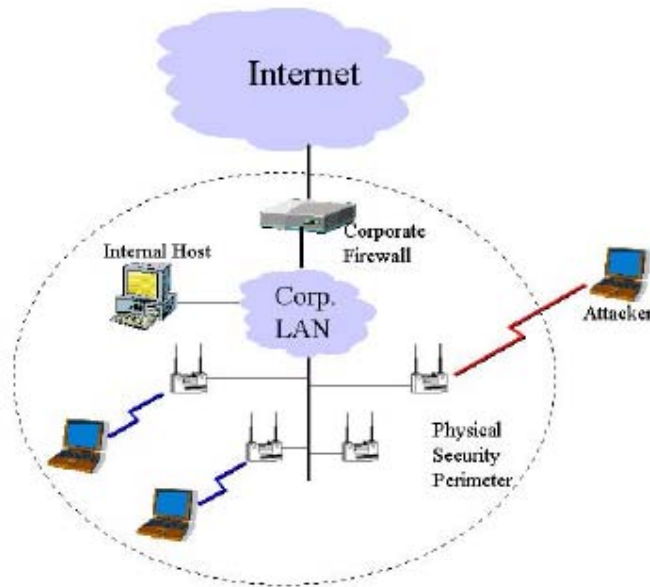


Figure – 6 : The Parking Lot Attack

3.1 Security Vulnerability and Threats

Like wide network wireless LANs are vulnerable to two types of attack: 1) active attacks; hackers gain access to the LAN to destroy or alter data and, 2) passive attacks; hackers gain access to the LAN, but can only eavesdrop to transmitted data.

Active Attacks: A direct attack by intruders to make modifications to message, data or file. It is possible to detect this type of attack but it may not be preventable these attacks are profiled below:

Spoofing: One of the most basic types of active attacks is that the intruder configures their wireless terminal to have the same MAC

address as an authorized access point or wireless terminal. When spoofing an access point, the intruder's terminal appears as the authorized access point, with the intent to associate with an authorized wireless terminal and access the data on that device. When spoofing a wireless terminal, the intruder's terminal appears as the authorized terminal, with the intent to gain unauthorized access to the wireless network.

Denial of Service (DoS): A denial of service attack disrupts a network by loading the bandwidth with meaningless data to bring the network to a halt. It can be done by sending continuous stream of meaningless information to APs or clients and shuts down all communications in a given area. This type of attack can required a significant amount of power if applied to a broad area. DoS attack on wireless network may be difficult to prevent and stop [11].

Replay Attacks: The intruder monitors and captures transmitted packets between a wireless terminal and access point. This is achieved via a passive monitoring utility called a 'sniffer'; such as Air Snort, which is readily available on the Internet as freeware. Once the packet is captured, the hacker can do one of two things:

- Initiate a DoS attack by repeatedly transmitting through the access point. Because the packet contains valid data, the access point forwards it to the host server to process and respond with a data receipt message. The host server overloads if the packet is transmitted with enough frequency.
- Accelerate the data flow on the network to reduce the time required to collect enough data to crack a WEP encryption key.

Man-in-the -middle (MITM): In this form, the attacker intercepts the data traveling from one device to another device and alters the contents, intelligently. The intruder may drop packets, replay packets, modify packets or even completely change the contents.

Passive Attacks:

An attack in which an unauthorized party gains access to an asset and does not modify its content. These types of attack are nearly impossible

to detect and even hard to prevent. Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below

Eavesdropping: Anytime two (or more) computers communicate over a network the data packets can be intercepted, copied, stored or analyzed by attacker. With a little modification on any wireless device it can be captured all traffic on a particular network channel or frequency [11].

Traffic analysis—The attacker gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

3.2 Other Security Risks

In addition to abovementioned attacks there are other vulnerabilities that are unique for wireless network because of wireless equipments and its physical environment. We briefly describe the techniques that unauthorized can used to access network.

Theft of Hardware

Device theft is the physical theft of the device by an attacker. It is common to assign a WEP key to a client. The possessor of a client can access to the wireless LAN by using the client's MAC address and WEP key. If multiple users share a client, then those effectively share the MAC address and WEP key. When a client is stolen, the unintended users have access to MAC address and WEP key. After informing administrator by proper owner, administrator must change the MAC address and WEP key of all clients that use the same keys as stolen client.

Following methods may bring limited security against device thief:

- Bases wireless LAN authentication on device-independent items such as usernames and passwords, which users use regardless of clients on which they operate;

- Uses WEP keys that generated dynamically on user authentication, not static keys that are physically associated with a client.

Rogue Access Point

Rogue access points are those connected to network without permission from the network administrator. They could be used to allow unauthorized users to access to the network. Also they can be configured as a legitimate AP to wireless client.

Many rogue access point are placed by employees looking for additional freedom to move about at work and brings their APs from home and plug them directly into the corporate LAN without authorization. In addition, it is not always well-intentioned employees who deploy rogue access points. Attacker also can deploy an access point on your network and then connect to it later at night [12].

Open Access Points: Many wireless networks are set up as “open”, that is without keys or authentication mechanisms, as this is often the factory default. For such networks, anyone with a wireless client can gain access to the Internet. Not only that, the intruder can gain access to the network (often inside a firewall) and can access data and other resources available on the network.

High Gain Antennas: Low power wireless networks such as the 802.11b network seems to be secure from any intruder not in the vicinity. However, this has been shown not to be true. It has been demonstrated, that using high-gain antennas, an intruder can access a 802.11b network from up to 15 miles away, even though the network is designed for a maximum operational range of about 300 feet.

3.3 Risk Mitigations

For mitigation risks and to help secure the wireless LANs, two technical solution, software and hardware, are put into practice. Software solutions include proper access point configuration, software patches and upgrades, authentication, encryption, and intrusion detection

systems (IDS). Hardware solutions include smart cards, VPNs, Public key infrastructure (PKI) and biometrics. It should be noted that hardware solutions which generally have software components, are listed simply as hardware solutions.

3.3.1 Software Solutions

3.3.1.1 Access Point Configuration

Network administrators need to configure APs in accordance with established security policies and requirements. Properly configuring default setting, encryption settings, SSID, Ethernet MAC Address Filtering, and shared keys, will help eliminate many of the vulnerabilities inherent in a vendor's software default configuration.

Update Default Setting

Each WLAN device comes with its own default settings. If the security features are left with their default settings, the network is still vulnerable. The default IP address will be easy for hackers to guess and thus gain access to the AP. Also many APs are set up with "admin" as the administrative login name and without a password, which is like leaving the door open for a burglar [13].

SSID

Network access control can be implemented using an SSID associated with an AP or group of APs. The SSID provides a mechanism to "segment" a wireless network into multiple networks serviced by one or more APs. Each AP is programmed with an SSID corresponding to a specific wireless network. To access this network, client computers must be configured with the correct SSID. A building might be divided into multiple networks by floor or department. Typically, a client computer can be configured with multiple SSIDs for users who require access to the network from a variety of different locations.

Because a client computer must present the correct SSID to access the AP, the SSID acts as a simple password and, thus, provides a measure of security. However, this minimal security is compromised if the AP is

configured to “broadcast” its SSID. When this broadcast feature is enabled, any client computer that is not configured with a specific SSID is allowed to receive the SSID and access the AP. In addition, because users typically configure their own client systems with the appropriate SSIDs, they are widely known and easily shared. Therefore it is suggested to disable broadcast SSID features and configure the SSIDs with a value that is not easy to capture.

MAC Address Filtering

While an AP or group of APs can be identified by an SSID, a client computer can be identified by the unique MAC address of its 802.11 network card. To increase the security of an 802.11 network, each AP can be programmed with a list of MAC addresses associated with the client computers allowed to access the AP. If a client's MAC address is not included in this list, the client is not allowed to associate with the AP.

MAC addresses may provide some level of security and it is effective against casual eavesdropping but will not be effective against determined adversaries. Because they are transmitted in the clear from a wireless NIC to an AP, the MAC can easily be captured. Also MAC addresses are best suited to small networks. Each AP must be manually programmed with a list of MAC addresses, and the list must be kept up-to-date. This administrative overhead limits the scalability of this approach.

Using DHCP

Automatic network connections involve the use of a Dynamic Host Control Protocol (DHCP) server. The DHCP server automatically assigns IP addresses to devices that associate with an AP when traversing a subnet. For example, a DHCP server is used to manage a range of IP addresses for client laptops or workstations. After the range of IP addresses is established, the DHCP server dynamically assigns addresses to workstations as needed. The server assigns the device a dynamic IP address as long as the encryption settings are compatible with the WLAN. The threat with DHCP is that a malicious user could

easily gain unauthorized access on the network through the use of a laptop with a wireless NIC. Since a DHCP server will not necessarily know which wireless devices have access, the server will automatically assign the laptop a valid IP address. Risk mitigation involves disabling DHCP and using static IP addresses on the wireless network, if feasible.

3.3.1.2 Software Upgrades

Vendors generally try to correct known software security vulnerabilities when they have been identified. These corrections come in the form of security patches and upgrades.

An example of a software or firmware patch is the RSA Security WEP security enhancement. In November 2001, RSA Security, Inc., developed a technique for the security holes found in WEP. This enhancement, referred to as “fast packet keying,” generates a unique key to encrypt each network packet on the WLAN. The Fast Packet Keying Solution uses a hashing technique that rapidly generates the per packet keys.

Another example of a software or firmware patch that will be available as early as late 2002 is WiFi Protected Access (WPA). WPA does not need hardware upgrades and use TKIP to enhance the security of 802.11 [14]. It is a quickly enhanced protection for some of the WPA problems, but was not a perfect solution. In 2004, the Wi-Fi Alliance introduced Wi-Fi Protected Access 2 (WPA2), the second generation of WPA security. Like WPA, WPA2 provides enterprise and home Wi-Fi users with a high level of assurance that their data will remain protected and that only authorized users can access their wireless networks. WPA2 need new hardware and uses the Advanced Encryption Standard (AES) for data encryption [15].

3.3.1.3 Secure the WLAN with Network Access

Authentication

A network access authentication system restricts network access to authorized entities. To enter to a LAN, network access authentication is being used. After the system authenticates the entity, it should also authorize the particular session. After the entity is authenticated and the session authorized, the system should ideally authenticate each packet to prevent the session from being “hijacked” midstream [16]. Network access authentication can be accomplished at every layer of the wireless networking model – PHY, MAC, IP and UDP/TCP.

In IEEE 802.11 link layer, WEP provides authentication service and only entities with the shared key are permitted “physically” access to the network. However, WEP protocols has its flaws, the IEEE 802.1x standard is adopted as well as Point-to-Point protocol. This addition provides a facility for mutual authentication via an authentication server, such as RADIUS [17].

With mutual authentication between the client and an authentication server, the rouge AP can not successfully convince wireless client to its legitimacy and cause them to send traffic through it.

3.3.1.4 Encryption

The content of the data in wireless LANs is also visible if the data is sent unencrypted. Encryption converts the data into a no readable form that requires effort to reconvert to its readable form. If encryption is used properly, it should protect data from eavesdropping attacks.

The 802.11 standard specifies WEP for encryption. But WEP has two major weaknesses: Initialization Vector (IV) and the CRC-32 checksum algorithm. For eliminating these weaknesses, new encryption techniques was developed by IEEE 802.11 group. Advanced Encryption Standard (AES) Rijndael algorithm [15, 16] is a newer encryption method that was selected by the U.S. government to replace DES.

3.3.1.5 Personal Firewalls

Resources on public wireless networks have a higher risk of attack since they generally do not have the same degree of protection as internal resources. Personal firewalls offer some protection against certain attacks. Personal firewalls are software-based solutions that reside on a client's machine and are either client-managed or centrally managed. Client-managed versions are best suited to low-end users because individual users are able to configure the firewall themselves and may not follow any specific security guidelines. Centrally managed solutions provide a greater degree of protection because IT departments configure and remotely manage them. Centrally managed solutions allow organizations to modify client firewalls to protect against known vulnerabilities and to maintain a consistent security policy for all remote users. Some of these high-end products also have VPN and audit capabilities. Although personal firewalls offer some measure of protection, they do not protect against advanced forms of attack. Depending on the security requirement, agencies may still need additional layers of protection. Users that access public wireless networks in airports or conference centers, for example, should use a personal firewall. Personal firewalls also provide additional protection against rogue access points that can be easily installed in public places.

3.3.1.6 IDS

An intrusion detection system (IDS) monitor real-time network traffic to discover whether an unauthorized users are attempting to access, have already accessed, or have compromised the network. IDS for WLANs can be host-based, network-based, or hybrid, the hybrid combining features of host- and network-based IDS.

A host-based IDS (HIDS) is normally a piece of software that monitors the system for suspicious activity. This involves monitoring system files for changes or the installation of new software, drivers, or kernel modifications [18]. A host-based agent is installed on an individual

system (for example, a database server). In some cases, an agent can halt an attack on a system, although a host agent's primary function is to log and analyze events and send alerts.

A network-based IDS (NIDS) is installed on network and has capability to monitors the network traffic, as shown in figure 7. The NIDS either monitors for suspicious activity by comparing network traffic to signatures of known attacks or monitoring anomalies. The network monitor will recognize packets that conform to this pattern and take action such as killing the network session, sending an e-mail alert to the administrator, or other action specified.

One of the benefits of using NIDS over HIDS is that a single NIDS sensor can monitor a network containing many hosts, thus simplifying the installation and configuration of the IDS. Some HIDS can dramatically decrease the performance of the host operating system.

Host-based systems have an advantage over NIDS when encrypted connections—e.g., SSL Web sessions or On-VPN connections—are involved. Because the agent resides on the component itself, the host-based system is able to examine the data after it has been decrypted. In contrast, a NIDS is not able to decrypt data; therefore, encrypted network traffic is passed through without investigation.

Unlike HIDS, NIDS can be deployed in different locations in network to detect all traffic on the segment. It can be locate in front or behind of firewall, between organizational and partner networks, network background, critical servers, remote access server and wireless LAN backbone [24].

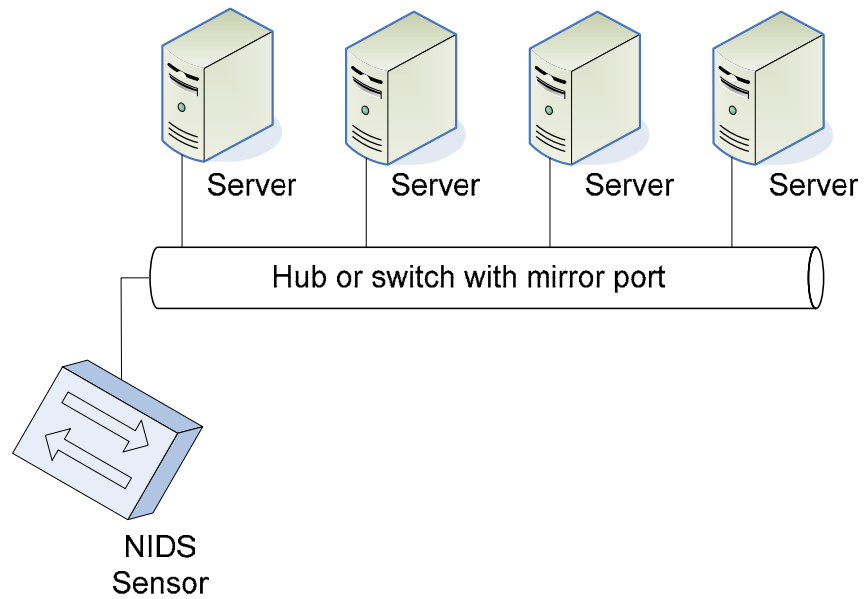


Figure – 7 : IDS Architecture

3.3.2 Hardware Solutions

Hardware solutions include implementing smart cards, VPNs, PKI, and other hardware solutions.

Smart card

Smart cards may add another level of protection. In wireless networks, smart cards provide the added feature of authentication. Smart cards are beneficial in environments requiring authentication beyond simple username and password. User certificate and other information are stored on the cards themselves and generally require the user only to remember a PIN number. Smart cards are also portable; consequently users can securely access their networks from various locations.

VPN

VPN technology provides the means to transmit data securely between two network devices over an insecure data transport medium. It is commonly used to link remote computers or networks to a corporate server via the Internet. However, it is also the ideal solution for protecting data on a wireless network. VPN works by creating a tunnel on top of a protocol such as IP. Traffic inside the tunnel is encrypted and totally isolated.

VPN technology provides three levels of security, user authentication, encryption and data authentication:

- Authentication ensures that only authorized user able to connect, send and receive data over the wireless network.
- Encryption offers more protection because it ensure that even if transmission are intercepted, they cannot be decoded without significant effort.
- Data authentication ensure integrity of data over wireless network and give guaranty that data send from authenticated devices only.

The benefits of VPN can be enhanced by combining it with other security features. VPN technology will be considered in detailed in fourth chapter.

PKI

PKI provides the framework and services for the generation, production, distribution, control, and accounting of public key certificates. It provides applications with secure encryption and authentication of network transactions as well as data integrity and non repudiation, using public key certificates to do so. WLANs can integrate PKI for authentication and secure network transactions. Third-party manufacturers, for instance, provide wireless PKI, handsets, and smart cards that integrate with WLANs.

Users requiring high levels of security should strongly consider PKI. It provides strong authentication through user certificates, which can be used with application-level security, to sign and encrypt messages. Smart cards provide even greater utility since the certificates are integrated into the card. Smart cards serve both as a token and a secure (tamper-resistant) means for storing cryptographic credentials. Users requiring lower levels of security, on the other hand, need to consider carefully the complexity and cost of implementing and administering a PKI before adopting this solution.

Biometric

Biometric devices include fingerprint/palm-print scanners, optical scanners (including retina and iris scanners), facial recognition scanners, and voice recognition scanners. Biometrics provide an added layer of protection when used either alone or along with another security solution. For example, for agencies needing higher levels of security, biometrics can be integrated with wireless smart cards or wireless laptops or other wireless devices and used in lieu of username and password to access the wireless network. Additionally, biometrics can combine with VPN solutions to provide authentication and data confidentiality.

CHAPTER 4

COMPARISON OF SECURITY METHODS IN DIFFERENT LAYERS

Like all IT-based security, WLAN security should be handled in layers. By building security in layers, protection can be provided at each layer in the network model. Each layer provides inherent protection against specific attacks for higher layers of security, correlating to the layers of the ISO network model.

4.1. Security Methods Used in Physical Layer

The bottom-most layer of the OSI reference model [19] is the Physical Layer. It describes the data that actually go into and out of the computer, how fast the data are transmitted and the method of communication such as radio, infrared, or wired.

4.1.1 Spread Spectrum Methods

There are different types of physical layer that are specified in 802.11. FHSS and DSSS are two types of radio layers which are explained in chapter 3 in detail. These two spread spectrum method prevent radio signals from being monitored or blocked by hostile parties.

Both FHSS and DSSS are resistant to interference from conventional radio transmitters. Because the signal doesn't stay in one place on the band, FHSS can elude a jammer – (a transmitter designed to block radio transmissions on a given frequency). DSSS avoids interference by configuring the spreading function in the receiver to concentrate the desired signal but spread out and dilutes any interfering signal.

Spread spectrum doesn't always do as well when there are other spread spectrum systems operating nearby, though. The more frequency-hopping transmitters operating on a band, the more likely it is that one or more of them will hop to the same frequency at the same time, garbling data that must be retransmitted. DSSS is better at resisting noise up to a certain point. However, if the combined interference throughout the band rises above a certain level, throughput dramatically drops-nearly to zero. Unfortunately, it only takes a few nearby FHSS systems to cripple a DSSS system. On the other hand, because a DSSS system is always transmitting on every frequency in the band, a nearby FHSS system may be unable to find any clear channel to hop to. In the presence of interference, FHSS usually degrades more gracefully than DSSS, but neither works well when competing at close range.

Directional antennas can sometimes help a node focus on the system with which it must communicate and ignore interference from others. However, as a general rule, when two transmitters compete for the same bandwidth, the one that expends more energy per bit of data wins the battle.

4.1.2 OFDM Method

Orthogonal Frequency Division Multiplexing (OFDM) modulation method is another type of physical layer. OFDM is a multi-carrier transmission technique, which divides the available spectrum into many carriers, each one being modulated by a low rate data stream. OFDM offers benefits over spread spectrum in channel availability and data rate. Channel availability is significant because the more independent channels that are available, the more scalable the wireless network

becomes. The high data rate is accomplished by combining many lower-speed sub carriers to create one high-speed channel. However, OFDM uses the spectrum much more efficiently by spacing the channels much closer together as shown in figure -8. This is achieved by making all the carriers orthogonal to one another, preventing interference between the closely spaced carriers. 802.11a with the highest data rate (54 Mbps) in WLAN systems, last standard 802.11g and HiperLAN2 use OFDM technique.

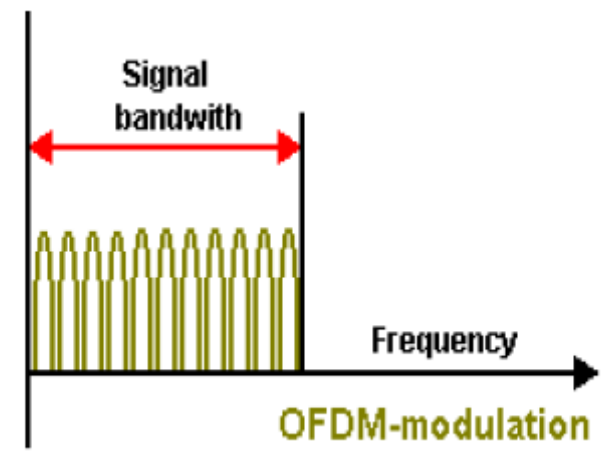


Figure – 8: OFDM Modulation

4.2. Security Method Used in Data link Layer

Link layers which is above physical layer deal with things such as how many bytes to send at a time, how to determine if a transmission fails, what to do if a transmission fails, and when to transmit.

Link layer security provides point-to-point security between directly connected network devices. In a wireless network, link layer protection defines a network that is secure to outsider intervention. Link layer protection starts with an authentication service and includes link layer encryption and integrity services. As a result, only authenticated users

can actively use the link layer, and all data traffic on the link layer is encrypted and authenticated.

Link layer protection secures wireless data only where it is most vulnerable, on the wireless link. Link layer security is also characterized by:

- Small footprint that can be easily integrated into network interface cards, access point devices, and mobile devices. Link layer security mechanisms are often integrated into the network hardware.
- Allows higher-level protocols, such as IP, IPX, etc., to pass securely. This provides security for all upper layer protocols.

4.2.1 The WEP Protocol

The Wired Equivalent Privacy (WEP) protocol is used in 802.11 networks to protect link-level data during wireless transmission between clients and access points. It is described in detail in the 802.11 standard [20]. WEP does not provide end-to-end security, but only for the wireless portion of the connection as shown in Figure 9.

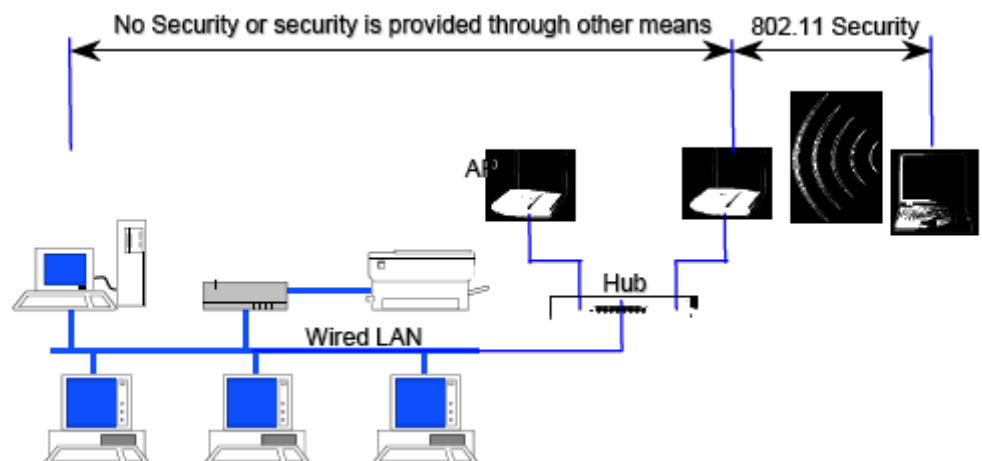


Figure – 9 : Wireless Security of 802.11 in Typical Network

First WEP use a share key for authentication and encryption applications. The standard key long in WEP is 40 bit. However,

numerous vendors offer nonstandard extensions of WEP that support key lengths from 40 bits to 104 bits [21].

Authentication can be done between an access point and a wireless client as depicted conceptually in figure-10. A random challenge is generated by the access point and sent to the wireless client. The client, using a cryptographic key that is shared with the AP, encrypts the challenge and returns the result to the AP. The AP decrypts the result computed by the client and allows access only if the decrypted value is the same as the random challenge transmitted.

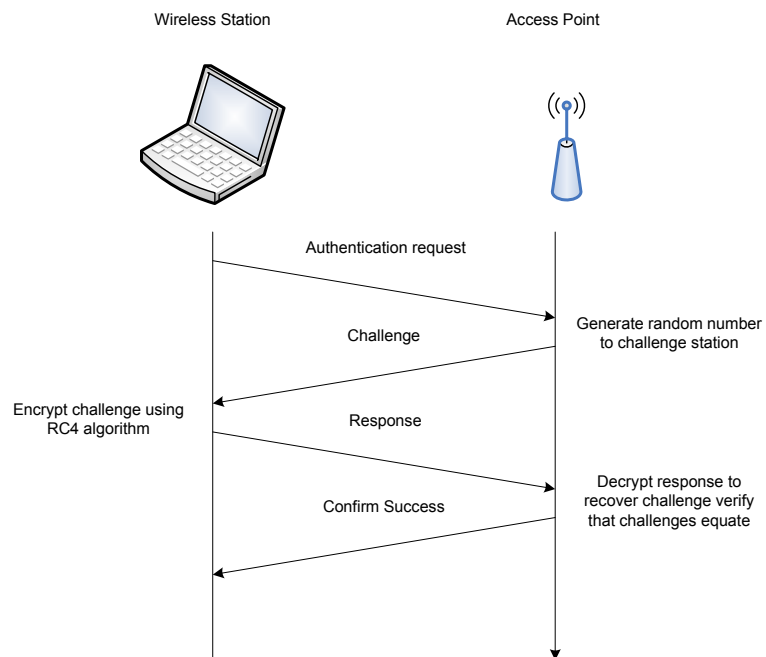


Figure – 10 : Shared-key Authentication Message Flow

To send a WEP encapsulated frame, the sender calculates the CRC of the frame payload and appends it to the frame. It then selects a new IV, appends this to the shared key to form a “per-packet” key, and uses the result to generate an RC4 key schedule. The sender then uses RC4 to generate a key stream equal to the length of the frame payload plus CRC. The sender XORs the generated key stream against the plaintext payload data and CRC. The sender also inserts the IV into the appropriate field in the frame header, and sets a bit indicating it are a

WEP encrypted packet. At this point, the WEP encapsulation is complete, and the frame can be sent to the peer as shown in figure 11.

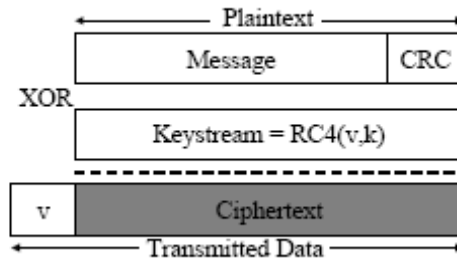


Figure – 11 : Encrypted WEP Frame

To process a WEP frame, the receiver checks the “encrypted” bit in the arriving frame. If it is set. The receiver extracts the IV from the frame, appends it to the BSS shared key, and generates the “per-packet” RC4 key schedule. RC4 is applied to the key schedule to produce a key stream the length of the packet’s encrypted payload. The receiver then XORs this key stream against the encrypted payload to extract plaintext. Finally the receiver verifies the CRC of the decrypted payload data to verify that the frame data correctly decrypted. The WEP privacy is illustrated conceptually in Figure 12.

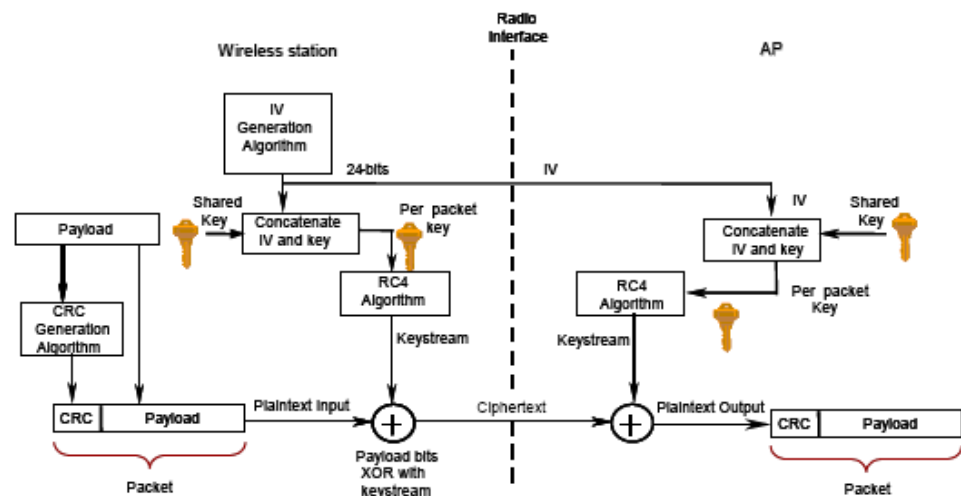


Figure – 12 : WEP Privacy Using RC4 Algorithm

The WEP protocol has weaknesses accepted by IEEE 802.11 working. These weaknesses let malicious users compromise the security of WLANs. These include passive attacks to decrypt traffic based on statistical analysis, active attacks to inject new traffic from unauthorized mobile stations and decrypt traffic.

Security problems with WEP include the following:

1. The authentication in WEP does not provide mutual authentication. That is, the client does not authenticate the AP, and therefore there is no assurance that a client is communicating with a legitimate AP and wireless network.
2. WEP does not address the issue of key management [22]. This may not seem like a problem when using WEP in an environment with three laptops, but it will cause problem when try to deploy WEP across a campus with 5.000 user. Each user must know the key and keep it secret. The new key must be given to every single user and re-entered in her client configuration when client is stolen. Moreover, if every station uses the same key, a large amount of traffic may be rapidly available to an eavesdropper for analytic attacks [23].
3. The IV in WEP, as shown in Figure 12, is a 24-bit field sent in the clear text portion of a message. This 24-bit string, used to initialize the key stream generated by the RC4 algorithm, is a relatively small field when used for cryptographic purposes. Reuse of the same IV produces identical key streams for the protection of data, and the short IV guarantees that they will repeat after a relatively short time in a busy network.
4. The IV is a part of the RC4 encryption key. The fact that an eavesdropper knows 24-bits of every packet key, combined with a weakness in the RC4 key schedule, leads to a successful analytic attack that recovers the key, after intercepting and analyzing only a relatively small amount of traffic. This attack is publicly available as an attack script and open source code.

5. WEP provides no cryptographic integrity protection. However, the 802.11 MAC protocol uses a noncryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledge packets with the correct checksum. The combination of noncryptographic checksums with stream ciphers is dangerous and often introduces vulnerabilities, as is the case for WEP. There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet and CRC sending it to the AP and noting whether the packet is acknowledged. These kinds of attacks are often subtle, and it is now considered risky to design encryption protocols that do not include cryptographic integrity protection, because of the possibility of interactions with other protocol levels that can give away information about cipher text.

4.2.2 WPA and WPA2

Because of weaknesses in WEP, the 802.11i Task Group developed a replacement for WEP in 2003. Originally called WEP2, the name was changed to WPA” which is short for Wi-Fi Protected Access [23]. WPA replaces WEP with a strong new encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC). It also provides a scheme of mutual authentication using either IEEE 802.1X/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology.

TKIP acts as a wrapper for WEP, adding a layer of security around WEP's. One of the first problems TKIP solves is that of key length. WEP uses small keys, and their effective length is shorter due to several design flaws. TKIP uniformly uses a 128-bit encryption key. TKIP also reduces the chance of replay attackers. TKIP expands the initialization vector (IV) to 48 bits from 24 bits, and combines this IV with the fixed key in a more cryptographically secure manner.

Further, TKIP addresses WEP's use of a single key by all clients. To create a base key, TKIP uses either a passphrase or a master key derived from the authentication process, and several other pieces of information,

such as a client's MAC address. This base key in turn is used with the IV to create per-packet keys. So in theory, every packet sent over WPA is encrypted by a separate and unique key.

One fundamental problem continues for networks that have deployed WPA directly, yet do not use authentication. The initial passphrase or secret deployed on clients and access points is often weaker than needed, since it usually must be human-readable and entered by a human. This immediately limits the passphrase or secret to a subset of readable characters that can easily be entered from the keyboard. Furthermore, the length is often limited to 20 characters or less due to the difficulties associated with remembering or entering long strings of seemingly random text.

The other problem is TKIP still makes use of RC4, a relatively weak encryption algorithm that was used due to hardware constraints on most of the devices originally designed to provide WEP.

In 2004, the Wi-Fi Alliance introduced Wi-Fi Protected Access 2 (WPA2), the second generation of WPA security. Like WPA, WPA2 supports IEEE 802.1X/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES).

Both WPA and WPA2 protect the wireless network from a variety of threats, including lost or stolen devices and hacker attacks such as 'man-in-the-middle', authentication forging, replay, key collision, weak keys, and packet forging.

There are 2 modes of WPA and WPA2 certification—Enterprise and Personal (See Table- 4). Both provide an authentication and encryption solution. All Wi-Fi CERTIFIED devices are certified as WPA-Personal by default. Vendors can request additional WPA2-Personal, WPA-Enterprise or WPA2-Enterprise certification.

Table 4 - WPA and WPA2 Mode Types

	WPA	WPA2
Enterprise Mode (Business and Government)	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES- CCMP
Personal Mode (SOHO/Personal)	Authentication : PSK Encryption: TKIP/MIC	Authentication : PSK Encryption: AES- CCMP

4.2.2.1 Enterprise Mode Components for Authentication

Enterprise authentication authorizes users' access to the network on a per-user basis. An authentication deployment confirms user identity and determines the rights for each user.

There are 6 components to authentication in an enterprise deployment for either WPA or WPA2. (Figure 13.) They include:

- Client Adapter (NIC) to install Wi-Fi CERTIFIED devices.
- Client Supplicant, An IEEE 802.1X supplicant is a software that is installed on the client to implement the IEEE 802.1X protocol framework and one or more EAP methods.
- Extensible Authentication Protocol (EAP) types offer a range of options that can be used with different authentication mechanisms, operating systems, and back-end databases.
- New APs to be deployed in an enterprise network using EAP authentication should be WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED
- Authentication Server stores the list of the names and credentials of authorized users against which the server verifies user authenticity. Typically, a Remote Authentication Dial-In User Service (RADIUS) server is used.

- Authentication Database: User credentials may also be stored in an external database, such as SQL, LDAP or Active Directory, that can be accessed by the authentication server.

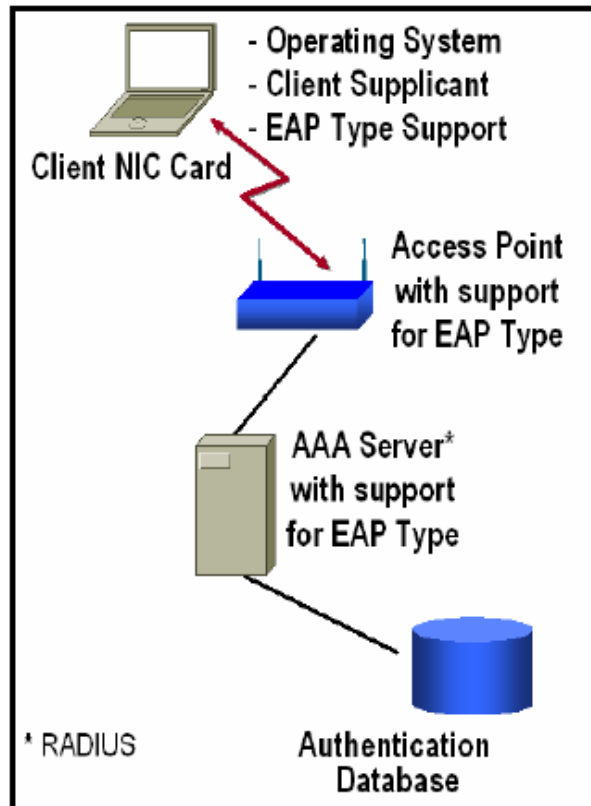


Figure – 13 : WPA and WPA2 Components

4.2.2.2. How WPA and WPA2 Authentication Works

WPA-Enterprise and WPA2-Enterprise mutual authentication is initiated when a user associates with an access point. The AP blocks access to the network until the user can be authenticated. The authentication process is enabled by the IEEE 802.1X/EAP framework which are treated as authentication message carriers. When the client starts establishing wireless connection, it sends the authentication message inside the IEEE 802.1x frame to the AP. The AP then forwards that frame to the centrally located authentication server (like RADIUS server). The authentication server is configured with the required information to authenticate the client. It accepts or rejects the packets and thus replies to the AP whether the client is an authorized use or not.

The AP accepts messages from the client only after the authentication server authenticates the client.

Mutual authentication helps to ensure that only authorized users access to the network and confirms that the client is authenticating to an authorized server. It helps to protect users from accidentally connecting to unauthorized 'rogue' APs.

If the authentication server accepts the user's credentials, the client joins the WLAN. If not, the client remains blocked. Once the user has been authenticated, the authentication server and the client simultaneously generate a Pair wise Master Key (PMK).

A 4-way handshake then takes place between the client and the AP, to complete the process of authenticating the AP with the client, establishing and installing the TKIP (WPA) or AES (WPA2) encryption keys. As the client begins communicating on the LAN, encryption protects the data exchanged between the client and the AP.

4.2.2.3. How WPA Encryption with TKIP Works

In this process, after accepting a user's credentials, the authentication server uses 802.1X to produce a unique master, or 'pair-wise', key for that user session. TKIP distributes the key to the client and AP, setting up a key hierarchy and management system. TKIP dynamically generates unique keys to encrypt every data packet that is wirelessly communicated during a session. This hierarchy replaces WEP's single static key with some 280 trillion possible keys that can be generated for a given data packet.

The MIC is employed to prevent an attacker from capturing, altering and resending data packets. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If it does not match, the data is assumed to have been tampered with and the packet is dropped—unless the optional MIC countermeasure is implemented in which case all clients are deauthenticated and new associations are prevented for one minute.

4.2.2.4. How WPA2 Encryption with AES Works

With AES, bits are encrypted in blocks of plaintext that are calculated independently, rather than a key stream acting across a plaintext data input stream. AES has a block size of 128 bits with 3 possible key lengths 128, 192 and 256 bits as specified in the AES standard. For the WPA2/802.11i implementation of AES, a symmetric 128-bit block cipher is used, replacing the DES encryption.

AES uses the Counter-Mode/CBC-Mac Protocol (CCMP). CCM is a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The 2 underlying modes employed in CCM include Counter mode (CTR) that achieves data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity.

CBC-MAC is used to generate an authentication component as a result of the encryption process. This is different from prior MIC implementations, in which a separate algorithm for integrity check is required. To further enhance its advanced encryption capabilities, AES uses a 48-bit Initialization Vector (IV). AES has no known attacks and the current analysis indicates that it takes 2^{120} operations to break an AES key—making it an extremely secure cryptographic algorithm.

4.2.2.5 Problem with 802.1x/EAP

Like in all new protocol proposals, Mishra and Arbaugh [25] believe that they have identified weaknesses that allow for both a Man-In-Middle attack and to allow a Session Hijacking to occur. The first attack focuses on the relationship between the Authenticator and the Authenticating Server. No explicit mutual authentication is specified in the standard and thus someone sitting between these two entities could gain access and assume either role. The second attack relies on the wireless operational environment and the ability for an attacker to use certain management frames to change the Supplicants and

Authenticators connection to a different Supplicant while remaining in an Authenticated state.

4.2.2.6 Problem with WPA-PSK

A dictionary attack can perform against WPA-PSK networks. This weakness is based on the fact that the pair wise master key (PMK) is derived from the combination of the passphrase, SSID, length of the SSID and nonces. The concatenated string of this information is hashed 4,096 times to generate a 256-bit value and combine with nonce values. The information required to create and verify the session key is broadcast with normal traffic and is readily obtainable; the challenge then becomes the reconstruction of the original values. Moskowitz [26] explains that the pair wise transient key (PTK) is a keyed-HMAC function based on the PMK; by capturing the four-way authentication handshake, the attacker has the data required to subject the passphrase to a dictionary attack. According to Moskowitz, "a key generated from a passphrase of less than about 20 characters is unlikely to deter attacks."

4.3. Security Method Used in Network Layer

The network layer is responsible for routing packets, establishing the network service type (connectionless versus connection-oriented), and transferring packets between the transport and link layers. In a mobile environment this layer has the added responsibility of rerouting packets and mobility management. Users of PCs and PDAs want to roam and communicate with their home environment, such as servers, from remote IP connecting points. In order to realize such mobile communication, IP layer security and mobility support is needed. IP security (IPsec) [27] and Mobile IP [28] are proposed by the Internet Engineering Task Force (IETF) as the standard IP technologies [29].

4.3.1. IP Security (IPsec)

IPSec is the standard network layer security protocol, and provides a standard and extensible method to provide security to network layer (IP) and upper layer protocols such as TCP and UDP. It is used extensively to secure network connections that extend from network hosts to both IPSec gateways and to other hosts. IPsec is the enabling technology behind most virtual private networks (VPN) used on the internet today.

IPSec utilizes two protocols one of which can be used at a time or a combination can be used. These protocols are known as authentication header (AH) protocol [30] and encapsulated security payload (ESP) protocol [31]. AH provides authentication to the whole packet while ESP can either provide authentication or not. ESP uses encryption unlike AH.

IPsec has many different cryptographic algorithms that can be used for AH and ESP. the most commonly used encryption algorithms for ESP are Data Encryption Standard (DES), Triple DES (TDES) and AES. The most commonly used authentication algorithms used for AH are Message Digest 5 (MD5) and Secure Hash Algorithm (SHA).

Two modes can be used by IPsec for encapsulating data. Transport mode is normally used when using IPsec to communicate between two hosts. Transport mode only encrypts the data of the IP packet and all the header information remains unencrypted. Tunnel mode encrypts the entire IP packet including the headers, see Figure- 14.

The standard does not provide solution for key exchange. Key exchange can be achieved by using Internet security association key management protocol (ISAKMP) and Internet key exchange (IKE).

There are security weaknesses related to IPSec like session stealing, encryption weakness and lack of access control and non-repudiation [32, 33].

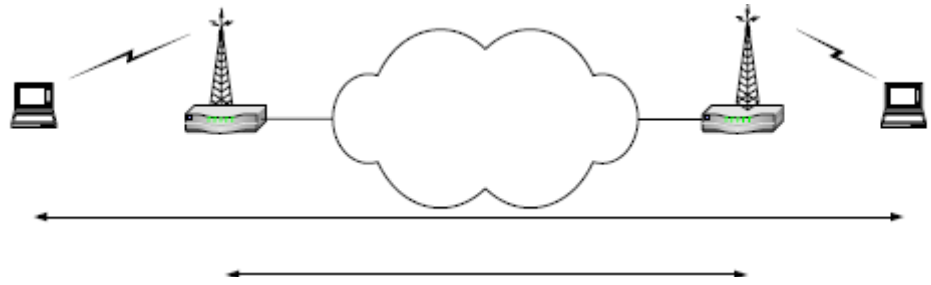


Figure – 14 : Ipsec Transport and Tunnel Mode

4.3.2. Mobile IP

Mobile IP allows mobility of devices in Internet by transparent routing of IP packets as shown in figure 15 [34, 35]. A location independent address is used to keep TCP/IP connectivity alive, while a temporary location-dependent address is used to provide connectivity to the local network resources.

Each mobile node (MN) is always identified by its home address (HA) which is placed on home network, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of-address (CoA), which is provided by foreign agent (FA) on the visiting network. The protocol provides for registering the care-of address with a home agent. The home agent sends datagram destined for the mobile node through a tunnel to the care-of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node.

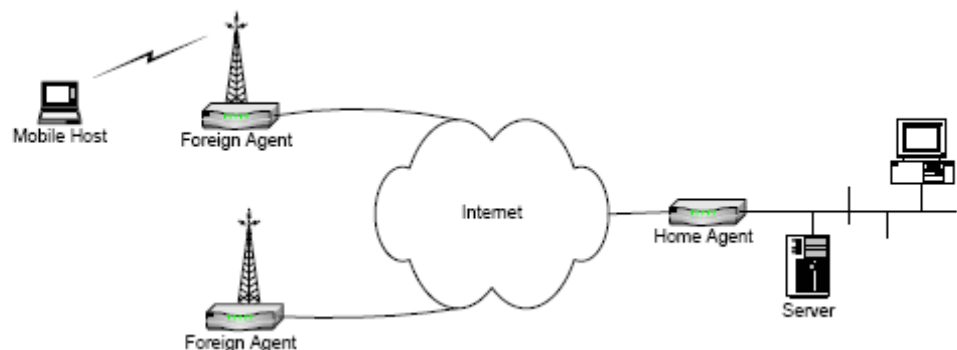


Figure - 15 : Mobile IP Elements

Mobile IP provides transparent IP mobility support for mobile terminals. However, when we try to use Mobile IP for accessing a corporate network from a remote site, there are several security vulnerabilities like a) Packets going into the corporate network, b) Packets going out from the visiting network, c) Confidentiality of communication. Most of these problems can be solved by introducing Ipsec security.

In IPsec, AH confirm that the received packets are actually sent by mobile node or guarantees that the packet received by the firewalls comes from a mobile node. Also ESP employ for protecting the IP datagram. When the packet goes toward the outside mobile node, ESP will use between the firewall and the mobile node to avoid eavesdropping.

Some network administrators may feel justified in relying on IPSec for WLAN security. But given the underlying shared medium (the radio frequency spectrum), IPSec is not an optimum solution. Older, widely deployed network layer security methods face new threats today that they were not designed to address. While it is possible to supplement network layer security to appear to provide wireless security, these complex solutions will always need to be reviewed in light of new risks. IPSec security protects data beginning with the network layer. It provides protection for only selected network connections, and leaves the network open to attacks that work outside of this limited security method. In addition, network layer protocols often use authentication mechanisms that require that the network be completely open to all wireless devices, ultimately leaving the network vulnerable.

Although IPSec is often used to provide wireless LAN security, there are some serious drawbacks to using network layer security alone for securing the wireless LAN. Since it protects only the network layer and upper layer protocols, it leaves the link layer vulnerable. It provides protection for only selected network connections, and leaves the network open to attacks that work outside of this limited security method.

In addition, managing an IPSec installation can be much more difficult than deploying a WPA solution. There are also some integration and usability concerns that stem from using IPSec differently from how it was intended. Finally, it must be noted that the Total Cost of Ownership (TCO) is likely much greater for an IPSec solution.

Network layer security will remain important to the wireless user in an untrusted (e.g., hot spot) wireless network, but is most effective when used in combination with link layer security.

4.4. Security Method Used in Transport Layer

The SSL (Secure Sockets Layer) Handshake Protocol was developed by Netscape Communications Corporation. It has been universally accepted on the World Wide Web for authenticated and encrypted communication between clients and servers. SSL works by using a public key to encrypt data that's transferred over the SSL connection. The Transmission Control Protocol/Internet Protocol (TCP/IP) controls and is responsible for the routing and transmission of data all over the Internet. The SSL protocol runs in a "layer" above TCP/IP and below higher-level protocols such as HTTP or IMAP. SSL makes use of a public key infrastructure (PKI) to operate. The server operating securely generally obtains an SSL key and certificate pair from an issuing authority. It then makes these available on the server itself and announces the availability within the protocol exchanges between the server and client.

An SSL exchange is initiated with an SSL handshake where the client and the server exchange information with each other regarding the encryption information indicated by the SSL certificate.

Once this handshake is completed both the client and the server know exactly how to encrypt the information in a way that the other end will understand and be able to decrypt.

From that point on, anyone listening to (or snooping on) the data transfer between the client and the server will only see this encrypted

information. They would then have to spend a long time decrypting it before they could make any sense out of it.

The greater the number of bits used when generating a certificate the stronger the encryption used with 1024 bit keys now being commonplace. It can take weeks of work using fast computers to successfully decrypt such a key.

4.4.1 How Does Secure Socket Layer (SSL) Work?

Client wants to communicate with Company to send important information back and forth. Client wants to be 100% sure that s/he is communicating with Company and that no one can eavesdrop on the communications. How can s/he do this?

- Client sends a courier to the Company's address.
- The company has envelopes that, when closed, can only be opened by the company. The company and the courier go together to a trusted third party -- a notary -- who makes the company provide documentation to prove its identity. The notary certifies the company's secure envelopes and the courier takes these back to the client.
- The Client makes a connection to *company.com* with its computer. This connection is made to a special "port" (address) on *company.com* that is set up for SSL communications only.
- When Client connects to *company.com* on its SSL-secured port, Company sends back its public key.
- Client with its public key stored in its computer by any third party companies, can decrypt the validation information, prove the validation is from Third Party Company and verify that the public key is certified by this company.
- If Client trusts certification, then Client can trust that he/she is really communicating with Company. If Client doesn't trust certification then the identity of who is running the computers to which Client is connecting is suspect.

- If client decides to trust the public key, then Client will send to Company the Client's public key.
- Company will then generate a "password" and encrypt it using both Client's public key and Company's private key, in succession, and send it back to the client.
- Client will decrypt the password. This process proves that Company sent the password and that only Client was able to read it.
- Client will start communicating with Company by encrypting data using this password. Normal "symmetric" (password-based) encryption takes place from this point forward because it use much faster than using the public and private keys for everything. These keys were needed to enable Company to prove its identity and right to domain.com and to give client the password in a safe way.

4.4.2 Limitation for SSL

Key Length: The statement that "only someone with the private key can decrypt something encrypted with the public key" is true so long as the private key cannot be "guessed". Hackers may try to do this by trying all possible private key combinations. Older "40bit" keys can be broken by trial and error if one has access to vast computer resources and a good amount of time. These days, keys used in SSL are 128bit or better. There are so many possible keys with 128bit that it would take significantly longer than the age of the universe to "guess" one.

Trust: While use of SSL ensures that your communications cannot be spied on, it comes down to trust to ensure that you are actually communicating with your intended company. This is reflected in the validation of *company.com* and your trust of the third party organization. Some "secure sites" do not bother to get a third party's approval and have their keys approved by "themselves". Others use third parties that are almost free and which spend very little effort in validating the company. In these cases, SSL provides you with no real assurance that you are really talking to your intended company and not

some hacker trying to forge their identity to communicate with you in a manner in which you think you are safe.

For defensive use of the web, you should pay attention to warnings generated by SSL when you connect to secure sites. Such warnings include "expired certificates", "domain name mismatches" where the domain name presented by the company is different than the one to which you are connecting, and "non trusted certificates" where the public key (certificate) presented by the company was not validated by a third party that your computer trusts. In all of these cases, you should be wary.

CHAPTER 5

CONCLUSION

The wireless revolution began in the 1980s with the advent of cellular telephony. Personal digital assistants joined the fray, and eventually computer connectivity transitioned to wireless local area networks. Today, users can link their laptops to the Internet in many public places that are wired for wireless. And the future will have an even greater wireless characteristic. New wireless standards about to be adopted will open up almost every known information technology application to the wireless realm. These drastic changes is important in the near term. For the long term, the use of fiber or wire media may be the exception rather than the rule. But with liberty comes license, and wireless technologies are no exception. The freedom unleashed by wireless connectivity brings with it new responsibilities. Those, of course, revolve around information security.

The coming wave of wireless innovation may actually constitute a new information revolution. The future of wireless is bright, and the future that it will bring to the public is even brighter. But, as with any leap ahead, there exists a possible dark cloud that could dim that bright future. Secure wireless connectivity will face greater requirements than ever before, and both customers and providers must work closely together to avoid losing the benefits of this innovative technology.

Wireless technologies provide ease of accessibility to the Internet virtually from anywhere and enable freedom of mobility for users by releasing the constraint of physical connections to networks. Besides these advantages, inherent broadcast nature of wireless networks has raised security concerns because when data is exchanged over air medium, interception and eavesdropping become easier to anyone with radio access equipment. Consequently it necessitates the need to deploy security services provided by security protocols. Existing security protocols provide security features at different network layers. For example, Wired Equivalent Privacy (WEP) is the very first protocol to be considered for a wireless network, which works at link layer but has been identified with major security drawbacks.

To overcome WEP weaknesses, a new standard WPA designed which also works at link layer, and provides port based access control for wireless nodes. Also, EAP exploits the use of Extensible Authentication Protocol (EAP), which is used as a transport mechanism. At network layer, we consider IP Security (IPsec) protocol suit, which is originally designed for wired network, but it is now being considered for wireless network due to its strong authentication and encryption methods. Secure Sockets Layer(SSL) is a transport layer protocol, and it is the most widely deployed security protocol on the Internet today.

Although security protocols exist at every network layer and have a security level that protect wireless LANs from different attacks; however each security protocol has its own limitation or weaknesses. Main weaknesses and limitation in these protocols were discussed in chapter four. For example the security protocol for physical and data link layers are not sufficient because the transmission medium is air and data is spread everywhere. Attacker can perform attacks like MITM and DoS to make hole in security protocols and access to network. Also the protocols in network layer provide end to end security across a routed network and can provide authentication, data integrity, and encryption services. But it is not sufficient when it is used alone. It will be most

effective when used in combination with link layer and other layer protocols.

Deployment of robust security for wireless network need big effort and is a costly method. Most of time needed there is for new hardware, installing security protocols and administration to put into practice. For this reason user do not pay attention to select appropriate security protocol and leave their network under risks.

REFERENCES

- [1] <http://ftp.vub.ac.be/~sijansse/2e%20lic/BT/Voorstudie/PreliminaryStudy.pdf>
- [2] Gartner's public web site can be viewed at www.gartner.com,
- [3] **Van Nee R., Prasad R.** (2000) *OFDM for Wireless Multimedia Communication*, Artech House, Inc. Norwood, USA.
- [4] <http://portal.etsi.org/bran/Summary.asp>
- [5] <http://portal.etsi.org/bran/kta/Hiperlan/hiperlan2.asp>
- [6] **Pahlavan K., Krishnamurthy P.**, (2001) *Principles of Wireless Networks*, Prentice Hall PTR, USA.
- [7] **Stallings W.** [2000], *Data & Computer Communication*, 6th Ed. Prentice Hall, USA.
- [8] **Rozenblit M.** (2000) *Security for Telecommunications Network Management*, Wiley – IEEE Press, NY, USA.
- [9] <http://www.cwt.vt.edu/faq/default.htm#ism>

- [10] ITU, International Telecommunication Union, (2001), *Radio Regulations*, Chapter II – Frequencies, Artical 5, Frequency Allocations.
- [11] <http://www.cs.umd.edu/~waa/wireless.pdf>
- [12] **Dr. Peikari C., Fogie S.** (2003) *Maximum Wireless Security*. An Insider's Guide to Protecting Your Wireless Network, Macmillan Computer Publication.
- [13] <http://www.bit.tekotago.ac.nz/staticdata/papers04/linsecurity.pdf>.
- [14] http://www.commsdesign.com/design_library/cd/hn/OEG20021126S0003
- [15] NIST-FIPS (2001), *Announcing the Advanced Encryption Standard(AES)*, Publication no: 197.
- [16] **Daemen J., Rijmen V.**, *The Block Cipher Rijndael*, Lecture Notes in Computer Science, Volume 1820, Springer-Verlag.
- [17] <http://www.ietf.org/rfc/rfc2865.txt>
- [18] **Maxim M., Pollino D.** (2002), *Wireless Security*, Osborne McGraw – Hill CA. USA.
- [19] **Chan H. , Perrig A.** (2003), *Security and Privacy in Sensor Networks*. IEEE Computer Magazine.
- [20] <http://www.csse.uwa.edu.au/adhocnets/802.11-1999.pdf>
- [21] <http://www.dis.org/wl/pdf/unsafe.pdf>,

- [22] **J. Walker** (2000), "*Unsafe At Any Key Size: An Analysis Of The WEP Encapsulation,*" Tech. Rep. 03628E, IEEE 802.11 Committee.
- [23] **Barken L.** (2003) *How Secure Is Your Wireless Network?* Prentice Hall.
- [24] **Carter B. , Shumway R.** (2002), *Wireless Security End To End.* John Wiley & Sons, Inc.
- [25] **William A.** (2001) "*An Initial Security Analysis of the IEEE 802.1X Standard*", University of Maryland, Department of Computer Science, Report no: CS-TR-4328, UMIACS-TR- 2002-10.
- [26] **Fleishman G., Moskowitz R.** (2003), *Weakness in Passphrase Choice in WPA Interface*, Part of the ECT News Network.
<http://wifinetnews.com/archives/002452.html>
- [27] <http://rfc.net/rfc1825.html>
- [28] <http://www.faqs.org/rfcs/rfc2002.html>
- [29] **Frankel S.** (2001), *Demystifying the IPsec Puzzle*, Artech House, Norwood, USA.
- [30] <http://www.rfc-editor.org/rfc/rfc2402.txt>.
- [31] <http://www.ietf.org/rfc/rfc2406.txt>.

- [32] **Elkeelany O. , et al**, (2002), "*Performance Analysis of IPSec Protocol: Encryption And Authentication,*" Proc. Of IEEE Int. Conf on Communication (ICC 2002), vol.2
- [33] **Bellovin S.** (1996) "*Problem Areas for the IP Security Protocols,*" in Proceedings of the Sixth Usenix Unix Security Symposium, San Jose, CA.
- [34] <http://www.ietf.org/html.charters/mobileip-charter.html>.
- [35] <http://RFC.net/rfc2002.txt>