2007

Analysis of Wi-Fi Security Protocols and Authentication Delay

Donation Mkubulo
THE FLORIDA STATE UNIVERSITY

FAMU-FSU COLLEGE OF ENGINEERING

ANALYSIS OF WI-FI SECURITY PROTOCOLS AND AUTHENTICATION DELAY

By

DONATION MKUBULO

A Thesis submitted to the
Department of Electrical and Computer Engineering
in partial fulfillment of the
requirement for the degree of
Master of Science

Degree Awarded
Fall Semester, 2007

Copyright © 2007
Donation Mkubulo
All Rights Reserved
The members of the Committee approved the thesis of Donation Mkubulo defended on November 8, 2007.

___________________________________
Bruce Harvey
Professor Directing Thesis

___________________________________
Simon Foo
Committee Member

___________________________________
Ming Yu
Committee Member

Approved:

___________________________________
Victor E. DeBrunner, Chair, Department of Electrical and Computer Engineering

___________________________________
Ching-Jen Cheng, Dean, FAMU-FSU College of Engineering

The Office of Graduate Studies has verified and approved the above named Committee members.
ACKNOWLEDGEMENT

I would like to express my deep and sincere gratitude to all those who helped me to complete this thesis. First and foremost I want to thank Dr. Ren Moses who made available the financial support that enabled me to complete my graduate studies. Without his unending support and guidance I would never have reached this stage. I am also deeply indebted to my major professor Dr. Bruce Harvey whose help, suggestions and encouragement made it possible for me to complete my thesis.

I gratefully acknowledge the support of my colleagues and friends. I am especially obliged to Mahinga Hekeno, Onyekachi Acholem, Doreen Kobero, Geophrey Mbatu, Dr. Victor Mchuruza and Wolta Shiyo for their constructive criticism and valuable hints during my thesis writing and throughout my time at graduate school.

Last but not least, I would like to thank my family, my mother, sisters and brother who made me the man I am today.
## TABLE OF CONTENTS

LIST OF TABLES .................................................................................................................................................. vi
LIST OF FIGURES ................................................................................................................................................ vii
LIST OF ACRONYMS .......................................................................................................................................... viii
ABSTRACT .......................................................................................................................................................... x
INTRODUCTION .................................................................................................................................................... 1
  1.1 Wireless Networks ......................................................................................................................................... 2
  1.2 IEEE 802.11 Physical Layer ...................................................................................................................... 2
  1.3 802.11 MAC sub layer protocol ............................................................................................................... 4
    1.3.1 WLAN Architecture .......................................................................................................................... 4
  1.4 Wireless Security and Threats ................................................................................................................... 5
    1.4.1 Wireless Security Threats ................................................................................................................ 6
  1.5 Thesis Organization ..................................................................................................................................... 8
THE WEP PROTOCOL ........................................................................................................................................ 9
  2.1 How WEP Works ......................................................................................................................................... 9
    2.1.1 Data Encryption Background ............................................................................................................ 9
    2.1.2 RC4 Algorithm .................................................................................................................................. 11
    2.1.3 WEP Data Encryption ..................................................................................................................... 12
  2.2 WEP Security Features ............................................................................................................................. 13
    2.2.1 Confidentiality .................................................................................................................................... 13
    2.2.2 Data Integrity .................................................................................................................................... 13
    2.2.3 Authentication ................................................................................................................................... 14
    2.2.4 Access Control ................................................................................................................................ 14
  2.3 WEP Vulnerabilities ................................................................................................................................... 15
    2.3.1 Susceptibility to brute force attacks ................................................................................................. 15
    2.3.2 Attacks caused by the reuse of Initialization Vector ....................................................................... 16
    2.3.3 Message Modification Attacks ........................................................................................................ 17
    2.3.4 Station Association Attacks ............................................................................................................. 18
WI-FI PROTECTED ACCESS (WPA)........................................................................................................ 19
3.1  WPA Security Features........................................................................................................ 20
  3.1.1 TKIP and Encryption Key Management......................................................................... 20
  3.1.2 Authentication and MIC............................................................................................... 22
  3.1.3 802.11X...................................................................................................................... 25
3.2  WPA-Personal.................................................................................................................. 28
802.11i SECURITY PROTOCOL.................................................................................................... 30
4.1  Data Confidentiality and Integrity .................................................................................. 30
4.2  Authentication and Key Management ............................................................................ 32
4.3  Analysis of Security Offered by IEEE 802.11i................................................................. 37
  4.3.1 Eavesdropping, Traffic Analysis and Message Injection. ........................................... 37
  4.3.2 Session Hijacking......................................................................................................... 38
  4.3.3 Man-in-the-Middle..................................................................................................... 38
  4.3.4 Security Level Rollback Attack.................................................................................. 38
4.4  Comparison of security features of different protocols ................................................... 39
EFFECT OF AUTHENTICATION PROTOCOLS ON HANDOVER LATENCY .................... 40
5.1  Handover Stages ............................................................................................................. 40
5.2  Authentication Delay and Quality of Service ................................................................. 41
5.3  Delay Analysis Model..................................................................................................... 42
  5.3.1 Authentication Delay for WEP Open System Authentication.................................. 44
  5.3.2 Authentication Delay for WEP Shared Key Authentication..................................... 45
  5.3.3 Delay Introduced by WPA Authentication............................................................... 45
  5.3.4 Delay Introduced by 802.11i Authentication............................................................. 46
5.4  Results Analysis............................................................................................................... 46
CONCLUSION AND FURTHER WORK .................................................................................... 49
BIBLIOGRAPHY ..................................................................................................................... 51
BIOGRAPHICAL SKETCH ......................................................................................................... 55
LIST OF TABLES

Table 1: Summary of the main features of different WLAN standards ratified by IEEE .......... 4
Table 2: Major differences between WEP and WPA security protocols................................. 19
Table 3: Comparison of security protocols............................................................................. 39
LIST OF FIGURES

Figure 1: WLAN architecture ......................................................................................................... 5
Figure 2: Stream cipher encryption ............................................................................................... 10
Figure 3: Block cipher encryption ............................................................................................... 10
Figure 4: WEP key generation and encryption ............................................................................. 12
Figure 5: TKIP key mixing and encryption stages ....................................................................... 21
Figure 6: Components of 802.11X system ................................................................................... 26
Figure 7: Message flow during authentication process ................................................................. 27
Figure 8: Key generation for 4-way handshake operation .............................................................. 32
Figure 9: Key generation for group key hierarchy ........................................................................ 33
Figure 10: RSNA establishment procedure .................................................................................. 34
Figure 11: WEP open system authentication messages ............................................................... 44
Figure 12: WEP shared key authentication message ................................................................. 45
Figure 13: Authentication delay for WEP open system authentication ........................................ 46
Figure 14: Authentication delay for WEP shared key authentication and WPA 802.1X authentication .................................................................................................................................. 47
Figure 15: Authentication delay for 802.11i security protocols .................................................. 48
## LIST OF ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication, Authorization, and Accounting</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>BSS</td>
<td>Basic Service Set</td>
</tr>
<tr>
<td>CBC-MAC</td>
<td>Cipher Block Chaining Message Authentication Code</td>
</tr>
<tr>
<td>CCMP</td>
<td>Counter-mode/CBC-MAC Protocol</td>
</tr>
<tr>
<td>CSMA/CA</td>
<td>Carrier Sense Multiple Access with Collision Avoidance</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EAPOL</td>
<td>Extensible Authentication Protocol Over LAN</td>
</tr>
<tr>
<td>ESS</td>
<td>Extended Service Set</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency Hopping Spread Spectrum</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>GTK</td>
<td>Group Transient Key</td>
</tr>
<tr>
<td>ICV</td>
<td>Integrity Check Value</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IV</td>
<td>Initialization Vector</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MAC</td>
<td>Medium Access Control</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>MIC</td>
<td>Message Integrity Code</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple Input, Multiple Output</td>
</tr>
<tr>
<td>MSK</td>
<td>Master Session Key</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
</tr>
<tr>
<td>PCMCIA</td>
<td>Personal Computer Memory Card International Association</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>PEAP</td>
<td>Protected EAP</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical Layer</td>
</tr>
<tr>
<td>PMK</td>
<td>Pair-wise Master Key</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
</tr>
<tr>
<td>RC4</td>
<td>Rivest Cipher 4</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RSNA</td>
<td>Robust Security Network Association</td>
</tr>
<tr>
<td>RSN IE</td>
<td>Robust Security Network Information Element</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TK</td>
<td>Temporal Key</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WiMAX</td>
<td>Worldwide Interoperability for Microwave Access</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
<tr>
<td>XOR</td>
<td>Exclusive-OR operation</td>
</tr>
</tbody>
</table>
ABSTRACT

This thesis examines security threats facing wireless networks and the effectiveness of security protocols deployed to combat these threats. The thesis will base its study on Wireless Local Area Network (WLAN) as defined by IEEE standards 802.11a/b/g/n. Features of each WLAN Security protocol, from WEP, WPA and IEEE 802.11i will be analyzed and the effectiveness of each protocol in ensuring data integrity, data confidentiality, and network availability will be presented.

To allow mobility of users while ensuring network services are received at an acceptable quality level, fast handovers of client device from one Access Point (AP) to another are necessary. Mainly probing process, in which a client device looks for a proper AP to associate with, and the authentication process cause Handover delays. This thesis provides an analysis of authentication delay resulting from the use of different security protocols. A mathematical model was developed and used to calculate the authentication delay. The results obtained show that the largest delay is experienced with the 802.11i security protocol. In a network where frequent handovers of a client device are required from one Access point to another; the large latencies may lead to poor Quality of Service (QoS) or even interruption of real-time and interactive network services such as Voice Over Internet Protocol (VOIP).
CHAPTER 1
INTRODUCTION

Wireless networks have experienced an explosive growth in recent years. This rapid growth is due to proliferation of laptop computers, Personal Digital Assistants (PDAs) and other handheld devices and also due to many advantages offered by wireless networks to both the user and the network operator. To the user wireless networks offers mobility and the flexibility of being able to access the network from any place. Today it is commonplace to find people reading their emails, downloading files, music and pictures from the Internet through wireless networks. To network operator, wireless networks allows rapid deployment and scalability of networks without the need of laying out cables.

The ubiquitous use of wireless networks have also brought into focus security problems associated with these networks. Apart from inheriting all the security problems experienced by wired networks, wireless networks have got additional problems caused by the nature of the transmission media. As messages are broadcast openly over radio waves and are not protected by physical barriers as in wired networks, interception and masquerading by an intruder becomes easy for anyone with only basic equipments. This highlights the need of ensuring that wireless networks are properly secured.

The purpose of this thesis is to study the problem of security in wireless networks with emphasis on IEEE 802.11 networks. The paper will start by discussing the security threats faced by wireless networks. The paper will then look at the security protocols suggested to mitigate the threats. Effectiveness and shortcomings of each security protocol will be analyzed. The thesis will then study the latency introduced by authentication procedure when a client device needs to associate with an access point. A delay analysis model will be developed and used to calculate delays introduced by different security protocols.
1.1 Wireless Networks

The term ‘Wireless networks’ in this thesis will refer to the telecommunication networks in which the connections between different nodes are implemented without the use of wires. The most common wireless technologies can be divided into different categories according to the coverage area of the networks. The largest wireless networks are the cellular networks and can cover the whole country or when taken all together they can cover the whole world. The next category of wireless networks is the Metropolitan Area Networks (MAN) that has a coverage area of the whole city. WiMAX (IEEE 802.16) is the standard that can provide ubiquitous coverage to the whole metropolitan area. On the local area level, Wi-Fi (IEEE 802.11) is the standard that provides Wireless Network Area Network (WLAN). Finally on the personal area level, Bluetooth (IEEE 802.15 standard) provides connectivity for wireless networks within the coverage distance of up about 10 meters.

Wi-Fi has experienced an explosive growth in recent years due to many advantages offered by these networks. Apart from user mobility, which is the main benefit offered by WLAN, another major advantage is flexibility. Users have the flexibility to set-up and dismantle WLAN very easily to cater for temporary uses such as conferences, trade fairs or meeting. Another advantage is the ease with which topologies can be configured to meet different uses from a small home use to large university campus that allows roaming over large area. WLAN also allows for rapid installation, as no wires need to be laid out.

1.2 IEEE 802.11 Physical Layer

802.11 standard employs the use of 2.4GHz and 5GHz the unlicensed frequency bands in communication. The Institute of Electrical and Electronic Engineers released the first Wireless local area network standard, IEEE 802.11 in 1997. The standard gave specifications for Wireless LAN that used the 2.4 GHz band. The data rates achieved by the initial networks were 1 Mbps and 2 Mbps. An improved standard IEEE 802.11b operating in a 2.4 GHz frequency band and offering data rates of up to 11Mbps was released in 1999. The improved data rate was
comparable to that offered by wired LANs and therefore opened up the commercial viability of WLAN. Standard IEEE 802.11a was later released offering data rates of 54 Mbps and operating at 5 GHz. Despite the higher data rates offered by 802.11a standard, it was not considered as an alternative to 802.11b as it used a different frequency band from that used by 802.11b.

In June 2003, IEEE ratified standard 802.11g that used Orthogonal Frequency Division Multiplexing (OFDM) technology to offer data rates of up to 54 Mbps in a 2.4 GHz band. This standard was widely implemented by WLAN device vendors due to a higher throughput and frequency band compatibility with 802.11b standard. To further improve the throughput, IEEE is working on a new standard, IEEE 802.11n, whose draft was published in 2007. The new standard provides for a number of options and different configurations, which offer different data rates. When all optimum options are used, 802.11n standard can support data rates of up to 600 Mbps.

To improve performance, 802.11n standard employs Multiple Input, Multiple Output (MIMO) technique. With MIMO technology, multiple antennas are used on WLAN device. During transmission, the transmitting WLAN device splits data into multiple parts called spatial streams and transmits each spatial stream through separate antenna to a corresponding antenna on the receiving end. Increasing the number of spatial streams proportionately increases the transmission throughput, the tradeoff being the increased power consumption. 802.11n standard also employs other techniques such as beam-forming, spatial diversity, and MIMO power-save to further improve performance. With beam forming, the radio signals are directed straight to the receiving antenna thereby reducing signal power loss and interference. Diversity technique puts in use extra antennas that may be found on a WLAN device to combine output signals from those antennas and therefore obtaining a stronger signal. This enables a WLAN device to operate at a longer range. An example of this is when a laptop with two antennas connects to an Access Point (AP) with four antennas. Only two spatial streams can be sent from the laptop but these will be received on the four AP antennas, therefore, output from two AP antennas may be combined to obtain one spatial stream.

Table 1 provides a summary of the main IEEE standards that specify wireless LAN Media Access Control (MAC) and Physical Layer (PHY) requirements.
Table 1: Summary of the main features of different WLAN standards ratified by IEEE

<table>
<thead>
<tr>
<th>WLAN Standard</th>
<th>Year Ratified</th>
<th>Operating Frequency</th>
<th>Maximum Data Rate</th>
<th>Physical Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy 802.11</td>
<td>1997</td>
<td>2.4 GHz</td>
<td>2 Mbps</td>
<td>FHSS/DSSS</td>
</tr>
<tr>
<td>802.11b</td>
<td>1999</td>
<td>2.4 GHz</td>
<td>11 Mbps</td>
<td>DSSS</td>
</tr>
<tr>
<td>802.11a</td>
<td>1999</td>
<td>5 GHz</td>
<td>54 Mbps</td>
<td>OFDM</td>
</tr>
<tr>
<td>802.11g</td>
<td>2003</td>
<td>2.4 GHz</td>
<td>54 Mbps</td>
<td>OFDM</td>
</tr>
<tr>
<td>802.11n (Draft)</td>
<td>Published 2007</td>
<td>2.4/5 GHz</td>
<td>600 Mbps</td>
<td>MIMO</td>
</tr>
</tbody>
</table>

### 1.3 802.11 MAC sub layer protocol

The basic access method for 802.11 networks is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). In this network access protocol when a station wants to transmit, it first sends a management frame called Request to Send (RTS). This frame will indicate the duration of the following transmission and the source and destination of the data. Upon the receipt of the RTS frame, if the destination is free to receive data, it will send back the Clear to Send (CTS) frame. This frame will copy the transmission time as indicated in the RTS frame. Upon receipt of the CTS frame, the requesting station will start transmitting data. All stations hearing the RTS and/or CTS frames will refrain from sending data for the duration indicated in the frames. This mechanism reduces the possibility of packets collision at the destination, as all stations that are not in the requesting station’s radio range, and therefore could not hear the RTS, will hear the CTS from the destination, and will refrain from transmitting.

#### 1.3.1 WLAN Architecture

The basic 802.11 WLAN structure is made up of a Basic Service Set (BSS). A BSS is made up of wireless stations (laptops, PDAs, etc) communicating with each other through an Access Point (AP). The AP acts as a base station for a WLAN, bridging the network to the wired network. The reliable coverage area of a BSS depends on many factors such as sources of RF interference, physical objects in the area and their characteristics, WLAN device power and antenna usage. The whole WLAN can be made up of one or several BSSs. A combination of communicating
BSSs and a distribution system is known as an Extended Service Set (ESS). Figure 1 depicts the WLAN architecture.

![WLAN architecture diagram](image)

**Figure 1: WLAN architecture**

**1.4 Wireless Security and Threats**

For the wireless network to be secure, the services of confidentiality, authentication, integrity and availability must be fully provided by the security protocols.

**Confidentiality (Privacy):** The purpose of this security service is to ensure that only authorized persons have the ability to view the data transmitted between the sender and the receiver. The security protocol must be capable of preventing eavesdropping of the data.

**Authentication:** This security service make sure that only the authorized persons take part in the communication process; that is only authorized parties can access the network and send or receive data from the network. The security protocol must be capable of establishing the identities of parties before those parties are involved in communication.
**Data Integrity:** The purpose of this security service is to ensure trustworthy of data in the network. Security protocol must be capable of preventing addition, removal or modification of data between the sender and receiver.

**Network Availability:** This service ensures that network resources are accessible and usable whenever needed by the authorized entities.

### 1.4.1 Wireless Security Threats

Attacks on a wireless networks can be divided into two broad categories of passive and active attacks. Passive attacks refer to the security breach in which an unauthorized person gains access to the network and data being transmitted in the network but does not modify the data. On the other hand, active attacks refer to security breaches whereby an intruder gains access to network assets and modifies the contents of data being transmitted from the sender to the receiver. Below is a list of attacks that can be launched on a wireless networks:

**Eavesdropping:** This is a passive attack in which an authorized person monitors the traffic in a wireless network for message content.

**Traffic Analysis:** In this type of attack, an authorized person stores all the traffic in a wireless network and tries to learn partial or complete information from the collected information. This is also a passive attack as there are no attempts done to try to modify the original information.

**Masquerading:** In this type of attack the attacker impersonates a legitimate user and gains unauthorized access to the network.

**Message Deletion:** In this form of active attack, the attacker can remove data from the network before it reaches the intended destination. This is usually done by interfering with the data at the receiver antenna or causing data to seem as it contains errors leading the receiver to discard the data. The adversary can do this attack to deny a legitimate device access to the network by
deleting all or part of the messages required to authenticate a device before granting it access to the network.

**Denial of Service (DoS):** In DoS attacks, the attacker prevents legitimate users from the use or management of a network asset. DoS attack usually consists of frequency jamming whereby the attacker interferes with the whole of frequency band used in transmission of data by sending signals with more power at the same frequency. Also DoS attacks can be launched exploiting the manner in which channels are allocated to WLAN nodes wishing to transmit data. The attacker can cause the client device to think the channel is busy and defer sending data waiting for the channel to be idle. Furthermore, DoS attacks against a network can be launched by saturating a network device with requests such that it cannot respond to legitimate traffic and therefore making that particular device unavailable to legitimate users.

**Session Hijacking:** The attacker can wait for the legitimate network devices to complete authenticating themselves and then it can hijack the session between the devices by disconnecting one device and masquerading as the disconnected device. In this type of attack the attacker will be able to receive all data destined to the disconnected device and sending data as the legitimate device. This attack is usually launched after a legitimate device is authenticated to the network therefore a rogue device does not have to go through authentication.

**Message Replay:** This is an active attack whereby the attacker gains access to the network, captures and retransmits messages to one or more destinations as the legitimate user. By re-sending the messages, the adversary can cause the intended target to re-perform the same task a number of times and fail to perform other legitimate tasks. In another form, the adversary can use this attack to gain access to unauthorized network services by capturing the password supplied by the user device, and replaying that password to the AP, thereby gaining access to services offered by the AP.

**Man-in-the-middle:** In this attack an adversary breaks a direct connection between the wireless station and the access point and acts as a middle device between the two devices. To a legitimate user device the rogue device will appear as an AP while to the legitimate AP the rogue device
will appear as the user device. This attack enables the adversary to control the data relayed between the legitimate user device and the AP. For example when the user wants to access a certain web page, the attacker can change the address of the requested web page before sending the request to the AP. As a result a legitimate user will receive a different web page. Furthermore, the delivered web page may require the user to enter sensitive information such as credit card number, user name and password, which the attacker can use for unauthorized purposes.

1.5 Thesis Organization

The remainder of the thesis is organized as follows: Chapter 2, 3 and 4 will give analysis of WEP, WPA and 802.11i security protocols respectively. These chapters will provide a detailed analysis of effectiveness and shortcomings if these protocols at combating different security threats facing wireless networks.

Chapter 5 will look in detail the problem of authentication latency in relation to handovers of client devices in a wireless network. Seamless handovers are required for effective real-time and interactive services like Voice over Internet Protocol (VoIP) and to achieve this, the handover latency should be kept to the minimum. A mathematical model will be developed in this chapter and it will be used to calculate authentication latencies introduced by different authentication schemes.
CHAPTER 2
THE WEP PROTOCOL

The Wired Equivalent Privacy (WEP) protocol was the original security protocol for 802.11 networks. As the name indicates, WEP protocol was intended to provide to wireless networks, similar data confidentiality as that provided by wired networks.

2.1 How WEP Works

2.1.1 Data Encryption Background

Encryption is a process of converting plaintext data into the form that is unintelligible to unintended recipient called the ciphertext. Encryption can be performed using either a private key or public key.

In private key encryption, also known as symmetric key encryption, the same key is used to encrypt and decrypt the data at the sender and receiver respectively. Both the sender and receiver must have the knowledge of a secret key for proper communication to take place. Some of the most popular private key encryption algorithms include Advanced Encryption Standard (AES), Triple Data Encryption Standard (Triple DES), and Rivest Cipher (RC4) algorithms. Public key encryption on the other hand uses different keys for encryption and decryption. The public key that is known to the both communicating parties is used to encrypt the message that is sent to the receiver where it will be decrypted using receiver’s private key. The most popular public key encryption algorithm is RSA algorithm.

Stream and Block Cipher: Ciphertexts can be generated by using two methods: Stream cipher encryption and Block cipher encryption. In stream cipher encryption each bit of data is
sequentially encrypted using one bit of cipherkey. Stream cipher encryption is depicted in Figure 2.

![Figure 2: Stream cipher encryption](image)

In Block cipher encryption, depicted in Figure 3, plaintext data is divided into blocks before encryption is performed on the blocks of data. The block cipher specification will give the block sizes applicable and the size of encryption key to be applied on the blocks. AES algorithm is a block cipher that specifies blocks of 128 bits and keys of sizes 128, 192 and 256 bits. Another block cipher is Data Encryption Standard (DES), which has plain text block sizes of 64 bits and 56-bit encryption key.

![Figure 3: Block cipher encryption](image)
2.1.2 RC4 Algorithm

RC4 is a stream cipher, symmetric key encryption algorithm that was designed in 1987 and trademarked to RSA Data Security Inc. RC4 key has a variable length of 1 to 256 bits. For standard WEP application, a 40-bit key is used, although different vendors have implemented different key lengths to up to 104 bits. The encryption key is used to generate a 256-bit state table that is later used to develop a pseudo-random bit stream, which is XORed with the plain text to generate ciphertext.

The RC4 algorithm works in two phases: Key-scheduling stage and ciphering stage. In a key scheduling stage, the 256-bit state table, S, is populated using the key, k. Each element in the state table is then swapped at least once to ensure random values of state table. The key-scheduling algorithm can be summarized using the pseudo code below:

\[
\begin{align*}
\text{j} &= 0; \\
\text{for } i = 0 \text{ to } 255 & \quad S[i] = i; \\
\text{for } i = 0 \text{ to } 255 & \quad j = (j + S[i] + k[i \bmod \text{keylength}]) \bmod 256 \\
& \quad \text{swap } S[i] \text{ and } S[j] \\
\end{align*}
\]

Once the key-scheduling stage is completed, ciphering will follow, which includes more randomization of state table values to obtain the ciphering key, which will be XORed with the plain text to obtain the ciphertext. This stage can be summarized by the pseudo code below:

\[
\begin{align*}
\text{j} &= \text{i} = 0; \\
\text{for } k = 0 \text{ to } N-1 & \quad i = (i +1) \bmod 256 \\
& \quad j = (j +S[i]) \bmod 256 \\
& \quad \text{swap } S[i] \text{ and } S[j] \\
& \quad \text{ck} = S[(S[i] +S[j]) \bmod 256] \\
& \quad \text{output } M[k] \text{ XOR ck} \\
\end{align*}
\]

Where \(M[0…N-1]\) is the input message consisting of \(N\) bits and \(ck\) is the cipher key.
Due to its speed of execution and simplicity in software and hardware implementation, RC4 is one of the most widely used stream cipher. It is used in security protocols such as WEP, Microsoft Point-to-Point Encryption (MPPE), WPA, Secure Socket Layer (SSL) and Ciphersaber.

### 2.1.3 WEP Data Encryption

WEP relies on the secret key (k) shared by all authorized stations in the network to protect data. Data encryption is done as follows:

**Step 1:** The Integrity Checksum Value (ICV) is calculated on the message frame (M), then the ICV and M are concatenated to form a plaintext $P = [M, c(M)]$ which will be encrypted.

**Step 2:** The RC4 algorithm uses a common secret key and the initialization vector (IV) to generate a key stream denoted by $RC4(IV, k)$. The Initialization Vector is changed for each frame whereas the secret key is kept constant. An Exclusive OR operation is then performed on the plaintext, $P$ and the RC4 keystrem to produce a ciphertext $C = P \oplus RC4(IV, k)$

**Step 3:** The Initialization Vector (IV) together with the Ciphertext (C) are transmitted over the radio link. The IV is not encrypted and is transmitted as plaintext.

![Figure 4: WEP key generation and encryption](image-url)
At the receiving end the following processes are undertaken to recover the original message and check the integrity of the received data:

**Step 4:** The receiving station obtains the Initialization Vector (IV) from the transmitted message and uses it together with the secret key (k) and RC4 algorithm to obtain the RC4 keystream. The keystream is then applied on the received ciphertext to recover the plaintext as shown below:

\[
P' = C \oplus RC4(IV, k)
\]

\[
P' = [P \oplus RC4(IV, k)] \oplus RC4(IV, k)
\]

\[
P' = P
\]

**Step 5:** The recipient station then splits the plaintext into the message and the Integrity Check Value (ICV). The Checksum is then computed on the message and compared with the one received in the plaintext. If the two checksums are equal the message is accepted and the communication is completed.

### 2.2 WEP Security Features

#### 2.2.1 Confidentiality

WEP was supposed to prevent eavesdropping by employing a stream cipher known as Rivest Cipher (RC4). The original WEP uses a 40-bit key together with a 24-bit Initialization Vector (IV) in forming a RC4 traffic key used in encrypting messages. All devices in a network, access points and stations, used the same key, which was meant to be a secret for a given network. The key was manually entered on all devices in the network. Changing the secret key required manually changing the key setting for all devices, a difficult task for a large network.

#### 2.2.2 Data Integrity

WEP was meant to prevent modification and editing of the transmitted messages by calculating and Integrity Check Value over a Cyclic Redundancy Checksum (CRC) on the message frame. The ICV together with the message frame are all encrypted and transmitted to the destination where the encrypted frame is decrypted and the original ICV is recovered. The new ICV is then
calculated on the decrypted message and compared to the received ICV. If the two are equal a message is accepted as authentic otherwise the received message is discarded.

2.2.3 Authentication

Before mobile stations (Laptop computers, PDAs, etc) are allowed to access the network, they need to be authenticated into the network. To do this, WEP relies on the knowledge of a secret shared key among the mobile stations. Only stations with the knowledge of the secret key will be allowed to associate with the network.

A challenge and response process is used before associating a station. When a station requests association, the serving Access point will send a challenge to the station consisting of 128 bits of cleartext. On receiving the challenge, the mobile station will encrypt it using the secret key and send the encrypted signal back to the Access Point. The Access Point will then decrypt the signal and compare the decrypted text with the original plaintext. If the two are equal the station will be considered to possess the correct key and will be allowed to associate with the network.

The IEEE 802.11 Standard also includes an optional feature that allows stations to discard all packets that are not properly encrypted using WEP.

2.2.4 Access Control

The original 802.11 supports open access control configuration. With this configuration, any user is capable of accessing the network, which is equivalent to having no access control at all. However, different wireless equipment vendors implemented two major ways of controlling the users’ access to the network.

2.2.4.1 Closed Network: With this configuration, only access points with the knowledge of the network secret name called Service Set Identifier (SSID) can access the network. The SSID is a 32-character identifier that is appended to the header of packets sent over the 802.11 networks and is used to differentiate one network from another. An example of a vendor that implemented this type of configuration is Lucent Technologies in their ORiNOCO equipments [11]. The shortfall of this method is that the SSID of the network can be sniffed in plaintext during the
transmission and an attacker can then use the SSID to access the network masquerading as an authorized user. This configuration therefore does not offer any security to the network from a dedicated intruder.

2.2.4.2 Access Control List: This is another mechanism used by vendors. With this mechanism, an access point maintains a list of users allowed to access the network. The list is based on users’ MAC addresses and only users whose MAC addresses are on the list will be capable of accessing the network. If the MAC address of the user is not listed on the Access point the user is not granted access to the network. This method of access control has its own shortcomings. Since 802.11 network interface cards allow their MAC addresses to be changed, an attacker can easily bypass this feature by passively monitoring the transmissions in the network and making up a list of MAC addresses allowed to access the network. The attacker may then change his MAC address to one of the authorized addresses and thereby gaining access to the network.

2.3 WEP Vulnerabilities

WEP as described in the original IEEE 802.11 standard has been known to fail in all the three security goals it was intended to provide. Below is a discussion of the vulnerabilities encountered when using WEP.

2.3.1 Susceptibility to brute force attacks

The WEP protocol defined in IEEE 802.11 standard uses a 40-bit key together with the 24-bit initialization Vector in generating the RC4 keystream. Since the Initialization Vector is transmitted openly and is therefore accessible to the potential attackers, the only part of the key that is secret is the 40-bit key. It has been shown [9] that an intruder with a powerful computer may decrypt the message by generating every possible permutation of the key.

However Extended versions of WEP have been developed that provide key lengths of up to 104 bits together with a 24-bit initialization vector. This makes a brute attack practically impossible to carry out even with the most advanced computers currently in market.
2.3.2 Attacks caused by the reuse of Initialization Vector

WEP operates by using a common secret key to all stations in the network and a public initialization Vector. RC4 algorithm will then use the secret key and the IV into generating a keystream used in encrypting messages. The pitfall in this method is that whenever the Initialization vector is re-used, the RC4 algorithm will generate the same keystream and the two encrypted messages may be used to obtain information about the original messages as shown below:

\[
C_1 = P_1 \oplus RC4(IV, k) \\
C_2 = P_2 \oplus RC4(IV, k) \\
C_1 \oplus C_2 = [P_1 \oplus RC4(IV, k)] \oplus [P_2 \oplus RC4(IV, k)] \\
C_1 \oplus C_2 = P_1 \oplus P_2
\]

Therefore performing an Exclusive OR operation on two ciphertexts generated using the same Initialization Vector (IV) will generate an output of Exclusive OR operation to the original plaintexts from which the original messages can be obtained if partial knowledge of one of the plaintexts is known.

To prevent this type of attacks the WEP standard recommends that the Initialization Vector be changed for every packet. However, most Network Interface Cards (NICs) implement the recommendation by resetting the IV every time the card is inserted into the computer and incrementing the IV by one for each successive message frame. In the normal operation of a wireless station, PCMCIA card is likely to be inserted and removed a number of times in a day leading to low values of IV vectors to be reused during the day whenever the card is inserted in the computer. Furthermore, even when the IV is not initialized during the day it easy to find instances of vector reuse as the vector has only 24 bits, and for a busy station all possible permutations (2^{24}-1 different vectors) will be used pretty quickly and the vectors will start to be reused after that point.
The chances of IV and hence keystream reuse are further increased by the fact that all stations in a network under WEP share the same secret key. Therefore whenever stations in one network pick the same IV, similar keystreams will be generated and these may be used to gain knowledge of the secret key. The reuse of IV makes WEP protocol susceptible to attacks regardless of the secret key size. [9]

2.3.3 Message Modification Attacks

The Cyclic Redundancy Checksum (CRC-32) employed by WEP to ensure message authenticity is not sufficient as messages can be modified in-transit without altering the checksum value.

The vulnerability of the checksum value lies in its property that it is a linear function of the message. That is for all choices of messages ‘a’ and ‘b’ we have:

\[ c(a \oplus b) = c(a) \oplus c(b) \]

Where \( c(a) \) indicates a cyclic redundancy checksum for message ‘a’.

The result of the above linearity property is that it allows the ciphertext to be modified without modifying the checksum value and therefore defeating the function of Cyclic Redundancy Checksum.

All the attacker needs to know in defeating the checksum value is the actual ciphertext (C) and the desired plaintext (E), which is chosen arbitrarily by the attacker. The desired plaintext is then used to calculate the new ciphertext (C’) that will lead to a new message M’ being delivered to the recipient. The new ciphertext and message are given by:

\[ C’ = C \oplus [E, c(E)] \quad \text{and} \]

\[ M’ = M \oplus E \]

The new ciphertext (C’) will be transmitted in place of the original plaintext (C). On decryption the plaintext P’ will be a concatenation of a new message M’ and a new checksum value c(M’) which will be a correct checksum for the message M’. This is shown below:
This demonstrates that modifications can be made on an encrypted signal and the checksum value will not be able to detect the modification.

### 2.3.4 Station Association Attacks

The attacker wishing to associate with a wireless network can do so without the advance knowledge of the shared secret key. This can be accomplished with the knowledge one plaintext and its corresponding ciphertext. With the knowledge of plaintext-ciphertext pair, the attacker can easily derive the key used in obtaining the encrypting the plaintext. The attacker may then use the key to associate the device with the network by correctly encrypting the challenge from the Access Point.

With the knowledge of a plaintext, $P$ and the ciphertext $C$, the attacker may obtain the secret key as below:

$$P \oplus C = P \oplus [P \oplus RC4(IV, k)]$$

$$= RC4(IV, k)$$

Therefore performing an Exclusive OR operation on the plaintext and the ciphertext will enable the attacker to obtain the key that may be used in associating the station.
CHAPTER 3
WI-FI PROTECTED ACCESS (WPA)

To solve security flaws experienced on WEP protocol, Wi-Fi Alliance developed WPA security protocol. WPA was released as an interim solution to WEP security flaws while a more robust solution (IEEE 802.11i) was being developed. To offer backward compatibility to systems supporting WEP, WPA supported the same encryption algorithm as WEP, and it required only the software change to upgrade a system from WEP to WPA.

WPA addresses security flaws encountered in WEP by introducing several new security features. These include an enhanced data confidentiality protocol called Temporal Key Integrity Protocol (TKIP), the use of a 48-bit Initialization Vector and a 128-bit key in forming an encryption key. WPA also uses 802.11X/EAP authentication scheme. Furthermore, WPA adds Message Integrity Check (MIC) to protect the transmission against packet forgeries.

Table 2 highlights the major differences between WEP and WPA Security protocols. [12]

<table>
<thead>
<tr>
<th></th>
<th>WEP</th>
<th>WPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>40-bit keys</td>
<td>128-bit keys</td>
</tr>
<tr>
<td></td>
<td>Static key – Same key used by everyone in the network</td>
<td>Dynamic key assignment – Keys change per user, per session, per packet</td>
</tr>
<tr>
<td></td>
<td>Manual distribution of keys</td>
<td>Automatic distribution of keys</td>
</tr>
<tr>
<td>Authentication</td>
<td>Flawed, used WEP key itself for authentication</td>
<td>Strong user authentication utilizing 802.11X and EAP</td>
</tr>
</tbody>
</table>
3.1 WPA Security Features

3.1.1 TKIP and Encryption Key Management
In addition to using an extended Initialization Vector and a longer key, TKIP replaces a static shared key employed by WEP with a dynamically distributed key. After the authentication server associates a station, a session between a station and the serving Access Point is established. 802.11X protocol is then used to produce a unique master key also known as a pair-wise key for this particular session and is distributed to the station and the Access Point. The master key is made up from the AP and client device MAC addresses and special secret number for the session. A hash function is then applied to the master key and a random number to produce a Temporal Key (TK) for the session. The TK for the session will then be used to dynamically generate unique data encryption keys for each packet transmitted during the session as depicted in Figure 5. When the session ends, the Master key is discarded and a new Master key will be distributed for the next session. In this way unique keys are used for each session, for each user and for each packet transmitted.

**Encryption:** As with WEP, TKIP also employs the EXCLUSIVE-OR operation to generate the ciphertext from plain text and a random keystream. TKIP uses a 128 temporal key (TK) together with a 48-bit IV and the client device MAC address in deriving the random key stream. At the start of each transmission, the IV is reset to 0 and incremented by one for each packet transmitted. The length of IV (48 bits) ensures any IV will not be reused with the same TK, as it will take the transmission of $2^{48}-1$ packets in one session for IVs to be reused. This will take approximately 600 years at a data transfer rate of 54Mbps [10]. The use of a longer IV and a temporal key eliminates one of the major flaws of WEP security protocol.

TKIP generates the random keystream by mixing keys in two stages. Mixing is done using substitution boxes (Sboxes) where an m-bit input stream is changed into n-bit output stream using look-up tables. In the first phase, the TK is mixed with the user’s MAC address and the first 4 bytes of the IV to obtain an Intermediate Temporal Key (ITK). The purpose of this first stage is to prevent key stream reuse due to cross-station IV collision. The second stage of key mixing operation takes the TK again and mixes it with the ITK and the last 2 bytes of the IV to
generate a 128-bit stream that will be fed into the RC4 algorithm to generate the random keystream. The purpose of the second stage of key mixing is to remove any association between the IV and the key fed into the RC4 algorithm and thereby preventing the use of weak keys to recover TK. After the keystream is generated using RC4 algorithm, the plaintext is obtained by XORing the keystream with the plaintext. Figure 5 gives a grammatical presentation of key mixing and encryption processes performed by TKIP. [10]

The use of dynamically distributed keys also removes the needs to manually change the keys for all access points and mobile station, a process that is necessary when a change of WEP static keys is required.

Figure 5: TKIP key mixing and encryption stages
3.1.2 Authentication and MIC

WPA employs IEEE 802.11X authentication with one of the Extensible Authentication Protocols (EAP) available. 802.11X is a port-based network control access protocol that can be used both in wired and wireless LANs. IEEE adopted 802.11X as a standard in 2001. With 802.11X, user’s credentials are presented as digital certificates and they can be based on usernames, user passwords, smart cards or any other digital identity that the network administrator will like to use.

Together with EAP, 802.11X enables mutual authentication of stations with the authentication server. This prevents the possibility of a client station associating with a rogue access point. This scenario is a possibility under WEP where there is no mutual authentication and only client stations are authenticated before making association with any access point in the network. When users requests association, the user’s credentials will be sent to the Authentication server through the access point. If the Authentication server authorizes the user, TKIP will generate a master key that will be sent to the user and the access point. To complete the authentication process, a four-way handshake will take place between the user and the AP.

**Message Integrity check (MIC):** WPA introduced as a means of ensuring that packets are not altered or forged during transmission. In case the message integrity is compromised, the discrepancy is supposed to be detected and the edited frames are to be discarded. MIC was designed to combat the flaws experienced in the use of CRC checksum employed in WEP security protocol.

MIC is computed using a cryptographic algorithm known as Michael. Michael uses a 64-bit key and a message of arbitrary length to produce a 64-bit MIC value, which is padded at the end of the 802.11 frames. The message bodies together with the computed 64-bit MIC value are encrypted using RC4 stream cipher and transmitted to the receiver. The receiver will recompute the MIC value from the message body and compare the result with the value that came with the message. The receiver will accept the message if the two values match, otherwise the massage will be rejected.
Given a message, the Michael algorithm pads the end of a message with one byte of hexadecimal value 5a and a number of zeros to make the overall length of the padded message divisible into groups of 4 bytes. Finally, a mixing function implementing rotations, bit swaps and XOR operations is applied to each group of 4 bytes and a key to produce a 64 bit sequence that serves as a checksum of the packet.

MIC computations can be depicted using the simplified pseudo-code shown below. $K_0$ and $K_1$ represent two groups of 32 bits each obtained by dividing the secret MIC key. $M_0, M_1, \ldots, M_{N-1}$ are $N$ groups of 32 bits obtained from the padded message. $V_0$ and $V_1$ are the two groups if 32 bits that make up the final MIC value. Function ‘b’ is an un-keyed 4-round Feistel structure used to swap, rotate and XOR groups of 32 bits. [40]

Procedure Michael($K_0, K_1, M_0, M_1, \ldots, M_{N-1}$)
Input: MIC Key ($K_0, K_1$); Padded Message ($M_0, M_1, \ldots, M_{N-1}$)
Output: MIC Value ($V_0, V_1$)

$(l, r) \leftarrow (K_0, K_1)$
for $i = 0$ to $N-1$ do
    $l \leftarrow l \oplus M_i$
    $(l, r) \leftarrow b(l, r)$
return $(l, r)$

Procedure $b(l, r)$
$r \leftarrow r \oplus (l \leftarrow 17)$
$l \leftarrow (l+r) \mod 2^{32}$
$r \leftarrow r \oplus \text{XSWAP}(l)$
$l \leftarrow (l + r) \mod 2^{32}$
$r \leftarrow r \oplus (l \leftarrow 3)$
$l \leftarrow (l+r) \mod 2^{32}$
$r \leftarrow r \oplus (l \leftarrow 2)$
$l \leftarrow (l+r) \mod 2^{32}$
return $(l, r)$

Note: Michael operation $\leftarrow$ indicates left rotation of bits and operation $\leftarrow$ indicates right rotation. XSWAP is an operation that swaps the positions of two most significant bytes and the positions of two least significant bytes of the word. [21]

Weaknesses: 802.11 Network Interface Cards (NIC) and Access Points carry out Michael computations. These devices have low computational power, which led to the design of an algorithm with low computation overhead to reduce the system delay. The shortcoming of this
approach was that the defense offered by Michael against message forgery was weakened. Although the checksum value is made up of 64 bits, it can provide only $2^{20}$ unique checksum values. However it has been shown that integrity check values of up to $2^{29}$ unique values are susceptible to cryptographic attacks.

Another weakness of Michael algorithm is that the mixing function is an un-keyed Feistel structure. A Feistel structure is a cryptographic structure employed in a number of block ciphers such as Feistel cipher and DES. With this structure a block of data to be is divided into two halves (indicated by ‘l’ and ‘r’ in the pseudo-code below). A number of repeated operations such as bit rotations and byte swaps are then applied to one half and the result is XORed with the other half. In Michael algorithm the Feistel structure has four XOR operations and is therefore called a four-round Feistel structure.

Because the Feistel structure employed in Michael algorithm does not depend on any key, it can therefore be inverted [21]. Using the MIC value, the mixing function can be applied in reverse order to arrive at the MIC key as shown in the pseudo-code below. [21]

```
Procedure InvMichael((K₀,K₁),(M₀,M₁,...,Mₙ₋₁))
Input: MIC Key (V₀,V₁); Padded Message (M₀,...,Mₙ₋₁)
Output: MIC Value (K₀,K₁)

(l,r) ← (V₀,V₁)
for i =N-1 down to 0 do
    (l,r) ← b⁻¹⁽¹⁾(l,r)
    l ← l ⊕ Mᵢ
return (l,r)

Procedure b⁻¹⁽¹⁾(l,r)

l ← (l-r) mod 2³²
r ← r ⊕ (l − 2)
l ← (l-r) mod 2³²
r ← r ⊕ (l − 3)
l ← (l-r) mod 2³²
r ← r ⊕ XSWAP(l)
l ← (l-r) mod 2³²
r ← r ⊕ (l − 17)
return (l,r)
```
Note: Michael operation $\neg$ indicates left rotation of bits and operation $\sigma$ indicates right rotation. XSWAP is an operation that swaps the positions of two most significant bytes and the positions of two least significant bytes of the word. [21]

3.1.3 802.11X

IEEE 802.11X is a standard that defines the mechanism for port-based network access control. It provides a framework to authenticate and authorize devices needing to access the WLAN. 802.11X relies on EAP to provide access control, easy key management and authentication. 802.11X standard defines the manner in which authentication messages will be routed through different system components whereas the actual authentication messages routed will depend on a specific EAP authentication mechanism employed. In other words, 802.11X is merely the transport vehicle for authentication messages. This arrangement allows changing of authentication implementations without the AP being cognizant of the change. Different implementations of EAP protocols can be used; these include EAP – Transport Layer Security (EAP-TLS), EAP Message Digest 5 (EAP-MD5), EAP – Tunneled Transport Layer Security (EAP-TTLS) and Protected Extensible Authentication Protocol (PEAP).

802.11X authentication system is made up of largely three major components: the supplicant, the authenticator and the authentication server. The supplicant is usually the mobile station like a laptop or PDA that requires access to the network. The authenticator is usually the network AP whose purpose at the authentication stage is to receive authentication messages from the supplicant and pass them to the authentication server in the required format. The final component is the authentication server, also called the authentication, authorization and accounting (AAA) server. This is usually a RADIUS server, although other types of servers like Diameter server can be used. The term port in 802.11X represents the association between the supplicant and the authenticator [17].

Figure 6 shows the components of 802.11X system and the interconnection between the components. Both the supplicant and the authenticator have a Port Access Entity (PAE) that is responsible for operation of the algorithms and protocols associated with authentication mechanism. Before the supplicant is authenticated, the controlled port will be open and the
supplicant will not be able to access any of the network’s services. All the authentication messages between the supplicant and the authentication server will pass through the uncontrolled port. Once the authentication server accepts the identity of the supplicant, it will inform the authenticator of the success of the operation and key information will be passed to the supplicant. The controlled port will then be closed and the network services will be available to the supplicant. 802.11X also defines the encapsulation of EAP messages over LAN (EAPOL) to be used in message interchanges between the supplicant and the authenticator [17].

Figure 6: Components of 802.11X system

**Message-flow during authentication process:** The authentication process start when the supplicant sends the authentication request (EAPOL start) to the authenticator. The authenticator
will respond (EAP - request) by asking the supplicant to provide its identification. At this stage all other messages from the supplicant are blocked and the user device cannot access any service in the network. In the third stage of the process, the supplicant sends the EAP – response message, which contains its identification to the authentication server. The authentication server then uses the implemented authentication algorithm like password, smart card, username, etc to verify the identity of the supplicant. The server will then send an EAP-success or EAP-failure message to the supplicant depending on the outcome of the authentication. If the authentication was a success, the controlled port will be closed and the supplicant will then be able to access the network services. Figure 7 depicts the message flow between the supplicant, authenticator and the authentication server during authentication process. [8]

![Message flow during authentication process]

**3.1.5.2 Weaknesses:** A number of successful attacks can be launched at 802.11X authentication and access control protocol. Denial of service, session hijacking and man-in-the-middle attacks can all be launched on an 802.11 network implementing 802.11X authentication protocol.

When the supplicant has failed to authenticate and has received an EAP-failure message, it is supposed to wait for 60 seconds before sending another authentication message. An intruder wishing to launch a DoS attack can exploit this process by spoofing the EAP-failure message and sending it to the supplicant every 60 seconds. On receiving this message, the supplicant will assume that it comes from a legitimate AP and it will wait for 60 seconds before sending another
authentication request to which another authentication failure message will be sent from a rogue device.

Another DoS attack can be launched by continuously sending EAP-start messages to the authenticator. The authenticator will be overloaded with authentication dialogue from a rogue device and it will fail to handle legitimate traffic. DoS attack can also be launched by spoofing the legitimate supplicant’s MAC address and sending the logoff request to the serving AP (EAP-Logoff). The AP will assume the request comes from the legitimate device and it will disassociate the device.

802.11X authentication protocol offers only one-way authentication; only the supplicant is associated with the assumption that the authenticator is a trusted entity in the network. An adversary wishing to launch a man-in-the-middle attack can exploit this assumption by acting as an AP and receiving all data traffic from the authenticator. To prevent this type of attack, mutual authentication between the supplicant and the authenticator is necessary.

3.2 WPA-Personal

Wi-Fi Protected Access protocol can be implemented in two modes: the first mode and the one that has been discussed so far in this chapter is known as WPA-Enterprise. This mode employs the use of 802.1X authentication protocol and authentication servers. Due to high cost and complicated configuration of authentication servers, WPA-Enterprise implementation of WPA protocol is not appropriate for small office and home uses. This led to the second mode of WPA implementation known as WPA-personal.

WPA-Personal uses a Pre-Shared Key (PSK), which is made up of a pass-phrase whose length range from 8 to 63 ASCII characters or 64 hexadecimal digits (256 bits). If ASCII characters are chose, a hash function is used to reduce the number of bits from 504 bits obtained from 63 characters to 256 bits. The PSK is entered in all WLAN devices in the network and after the device is authenticated, TKIP will use the PSK, the Service Set Identity and nonces to generate
the Pair-wise Master Key (PMK) that will be used to generate data encryption keys as discussed in section 3.1.1. Thus the main difference between the two modes of operation is that with WPA-Enterprise the authentication server generates the PMK whereas with the WPA-Personal, the PMK is generated from the pass-phrase.

Although TKIP ensures that encryption keys for WPA-Personal are often changed, it has been shown [34] that security offered by this implementation of WPA largely relies on the length of the pass-phrase used as the Pre-Shared Key. Any pass-phrase that is less than 20 characters long is susceptible to dictionary attacks. The use of one pass-phrase for all devices in the Extended Service Set (ESS) increases the damage the attacker can do to the network, since after getting hold of the PSK, the attacker can read and modify any traffic in the ESS. Therefore to ensure proper level of security for WPA-Personal implementation, long pass-phrases should be used.
CHAPTER 4
802.11i SECURITY PROTOCOL

This is latest WLAN security standard ratified by IEEE in June 2004. 802.11i is also known as WPA 2 since WPA was based on the initial draft of 802.11i. Therefore many security features found in WPA are also available in 802.11i including TKIP and Michael algorithm. However 802.11i uses enhanced encryption, authentication and key management protocols that provide enhanced security to WLAN.

802.11i specifications defines two classes of security algorithms:

1. Robust Security Network Association (RSNA): This provides TKIP and Counter-mode/CBC-MAC protocol (CCMP) as data confidentiality protocols. It also provides 4-way handshake authentication procedure, 802.11X authentication and key management protocols.

2. Pre- Robust Security Network Association (Pre-RSNA): Data confidentiality here is provided by WEP and there is no 4-way handshake. The implementation of Pre-RSNA is necessary to make 802.11i backward compatible. The operation of WEP and other Pre-RSNA primitives were discussed in previous chapters and will not be covered in this chapter.

4.1 Data Confidentiality and Integrity

802.11i standard defines two data confidentiality protocols under RSNA security algorithm: TKIP and CCMP. Since TKIP has been discussed in the previous chapters, this section will confine its discussion on CCMP.
CCMP protocol handles encryption of wireless data and packet authentication. For encryption, CCMP employs Advanced Encryption Standard (AES) in the counter mode instead of RC4 used in WEP and TKIP protocols. AES is a more secure standard and is approved by Federal Information Processing Standard (FIPS) [19]. The Cipher Chain Blocking Message Authentication Code (CBC-MAC) provides packet authentication instead of Michael used in WPA protocol.

AES algorithm is a symmetric block cipher capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits [19]. The counter mode with CBS-MAC operation of AES algorithm uses 128 bits cipher keys making it secure against brute force attacks. AES allows the use of one encryption key in encrypting all packets, which eliminates the problems associated with key scheduling and key distribution as in WEP and TKIP protocols. The Message Integrity Check is provided to the frame body as well as the unencrypted MAC header, which prevents attackers from spoofing the source and destination MAC addresses and using them in launching attacks. Furthermore CCMP employs a 48-bit packet number (also called ‘nonce’), which is incremented every time a packet is transmitted. This prevents packet replay attacks as any repetition of a packet number (PN) will be noted and the packet will be discarded. The length of PN field (48 bits) ensures that a particular packet number will not be reused in any one association. The CBS-MAC (8 bytes), the nonce and 2 bytes of 802.11 overheads make the size of CCMP packet to be 16 bytes larger than the unencrypted 802.11 packet.

CCMP largely eliminates the threat of passive eavesdropping and traffic analysis since although the attacker can eavesdrop on traffic but it will be difficult to decrypt the packets as there is no way to discover the Temporal Key (TK) used for encryption. However since the MAC header is not encrypted, the intruder can gain knowledge of the packet size and frequency of transmission. Fortunately, the knowledge of this information cannot lead to any attack that can compromise the confidentiality of data.
4.2 Authentication and Key Management

802.11i EAPOL-key exchange uses a number of keys and has two key hierarchies that divide up initial keys into useful keys. The two key hierarchies are: 4-way handshake and group key handshake.

**4-way handshake:** For 4-way handshake the starting point is a Pair-wise Master Key (PMK). If 802.11i implements 802.11X, the PMK will come from the authentication server and when Pre-Shared key (PSK) is used, 802.11i will map the password into the PMK. The PMK will then be an input into a pseudorandom function, together with a nonces and MAC addresses from both the AP and the client device to obtain the Pair-wise Transient Key (PTK). The PTK will then be divided into 3 keys. The first key is the EAPOL-Key Confirmation Key (KCK), which is used in EAPOL key exchanges to provide data origin authenticity. The second key is EAPOL Key Encryption Key (KEK), which is used in EAPOL key exchanges to provide confidentiality. The final key derived from PTK is Temporal Key, which is used for data confidentiality.

![Figure 8: Key generation for 4-way handshake operation](image)

**Group Key Hierarchy:** The starting point for group key hierarchy is a random number called the Group Master Key (GMK). Then the authenticator MAC address, the authenticator nonce and GMK are input into a random function to produce the Group Temporal Key (GTK).
As discussed above, IEEE 802.11i defines RSNA procedure that provide for mutual authentication and key management protocol that ensures fresh Temporal Keys are generated to ensure data confidentiality. Figure 10 depicts the messages exchanged between, and the state of the supplicant, authenticator and the authentication server during RSNA establishment Procedure.
Figure 10: RSNA establishment procedure
**Stage 1: Network and Security Capability Discovery**

This stage is also known as the negotiation stage as the client device (supplicant) and the AP (authenticator) use this stage to agree on the security protocol to be used in their communication. This stage consists of messages numbered (1) to (3). Because 802.11i provides for 3 data confidentiality protocols: WEP, TKIP and CCMP, there must be a way for a client device and the AP to agree on which protocol to use. Client devices also use this protocol negotiation stage to discover other security features enforced by the AP. The AP broadcasts its security features, indicated by RSN IE (Robust Security Network Information Element) on the beacons it sends regularly. It can also provide its security features as a response to a probe request from a supplicant through a Probe Response frame. Some of the security parameters that an AP broadcasts are the list of all data confidentiality protocols that it supports in unicast communication, the data confidentiality protocol used in broadcast communication (this cannot be negotiated) and whether the Pre-Shared key (PSK) or 802.11X is being used.

**Stage 2: 802.11 Authentication and Association**

This stage consists of messages numbered (4) to (7). After the client device knows the parameters supported by the AP it then sends the associate request identifying the security feature it wants to use. This is message 6 (Association Request + SPA RSN IE). The security feature chosen by the client device must be included in the list of supported features otherwise the association will fail. After the supplicant receives the Association Response (message 7) the two devices (authenticator and supplicant) will be in association and authentication state but the 802.11X port will remain blocked and no data packets can be exchanged. Messages 4 and 5 are used in 802.11 Open System Authentication and are included to allow backward compatibility.

**Stage 3: EAP/802.11X/RADIUS Authentication**

This stage includes messages number 8 to 14. At this stage the supplicant and the authentication server execute mutual authentication. The authenticator acts as the relay point for messages from the server to the supplicant. The authenticator also encapsulates the messages in the required format before delivering them to the intended target. After the supplicant and the authentication server have authenticated each other a common secret key called the Master Session Key (MSK) will be shared between the devices. The supplicant will then use the MSK to generate the Pair-
wise Master Key (PMK). Authentication features will also be passed to the authenticator through message 15 to enable it to generate the PMK.

**Stage 4: 4-Way handshake**

A 4-way handshake as defined by IEEE 802.11i performs several functions including confirming the PMK between the supplicant and the authenticator, establishing the temporal keys to be used by the data confidentiality protocols and authenticating security parameters agreed to between the supplicant and the authenticator. During the 4-way handshake process four messages (message 16 through 19) are exchanged between the supplicant and the authenticator:

1. **Message 16:** In this message, the authenticator sends a nonce to the supplicant. This nonce is called ANonce. At this stage the supplicant creates its own nonce known as SNonce and calculates the PTK.

2. **Message 17:** In the second 4-way handshake message the supplicant sends the SNonce to the authenticator. The supplicant also sends security parameters used during association (SPA RSN IE). An authentication check will be applied on the received message using KCK. At this point the authenticator can verify the validity of security parameters used during association and derive a fresh Pair-wise Transient Key (PTK) to be used in the following data session. In case of group communication, the Group Transient Key is generated after the authenticator receives this message.

3. **Message 18:** In the third 4-way handshake message, the authenticator sends to the supplicant the security feature it broadcasts in its beacons (AA RSN IE). The authenticator also sends the GTK encrypted using KEK (In case of multicast application). The whole message will receive authentication check at the supplicant to verify that the authenticator’s security parameters are valid and similar to those used at association.

4. **Message 19:** The fourth message indicates that the temporal keys, PTK and GTK (for group communication) are now shared between the supplicant and the authenticator and are in place to be used for data confidentiality purposes. 802.11X ports will be unblocked and the supplicant can access services offered by the authenticator.
Stage 5: Group Key Handshake
This stage is only applicable during multicast applications. Group Transient key (GTK) is distributed to supplicants in this stage.

Stage 6: Secure Data Communication
Using the PTK (or GTK) and the negotiated security protocol, the supplicant and the authenticator will construct a secure communication channel to transmit data packets.

4.3 Analysis of Security Offered by IEEE 802.11i
IEEE 802.11i was designed to combat all the security flaws experienced in WEP and WPA protocols. This was accomplished in large part and 802.11i offers better security than all the previous protocols. Below is an analysis of the robustness of security offered by 802.11i to the common wireless threats.

4.3.1 Eavesdropping, Traffic Analysis and Message Injection.
It is still possible for an adversary to sniff and store all the data traffic in an 802.11i-protected WLAN. However due to the use of Temporal Keys (TK), the adversary will not be able to decrypt the data. Therefore the mere eavesdropping of data will not compromise data confidentiality and traffic analysis cannot be carried out. Management frames however poses another problem, as they are not protected by TK encryption. The attacker therefore can sniff messages communicated between the client device and the AP during security capability discovery stage and association stage of RSNA establishment procedure (stages 1 and 2). An attacker can then use the sniffed security capabilities and send them to the client device leading the device to associate with a rogue AP or use inappropriate security parameters in associating with legitimate AP. However, mutual authentication and 4-way handshake as implemented in stages 3 and 4 of RSNA establishment procedure will remove the risks posed by an attacker sniffing management frames.
4.3.2 Session Hijacking

This attack is launched after a client device has completed authenticating itself and therefore cannot be protected against by strong authentication mechanism. To launch this attack, an adversary can forge disassociate message and send it to the client device. After the legitimate device is disassociated, the rogue device will take over the session and continue communication with the serving AP. If the rogue device will only receive data from the AP, the TK implemented by 802.11i will prevent the rogue device from decrypting the data and no harm will be caused on data confidentiality. The rogue device cannot also send traffic to the AP, as it will not have the knowledge of Pair-wise Transient Key required for creation of acceptable traffic.

4.3.3 Man-in-the-Middle

To launch a successful Man-in-the-middle attack, the intruder need first to break the association between the client device and AP. To do this, an intruder can send de-authentication message to the legitimate device and authenticate the rogue device with the AP. The legitimate device will start sending probes looking for another and the attacker will associate the rogue device with the legitimate device. Therefore the attacker’s device will act as an AP to the client device and a supplicant to the legitimate device. However when a strong mutual authentication mechanism (like EAP-TLS) is implemented with 802.11i the rogue device will not be able to authenticate itself with the legitimate AP. Weak mutual authentication protocols can lead to a successful man-in-the-middle attack.

4.3.4 Security Level Rollback Attack

802.11i provides for two classes of security mechanisms: RSNA and Pre-RSNA. Pre-RSNA is implemented to provide backward compatibility when 802.11i is deployed in situations in which there are legacy devices that only support WEP security protocol. Also to cater for implementations of 802.11i where there are many supplicants, some with legacy devices, the standard defines a Transient Security Network (TSN) that supports both Pre-RSNA and RSNA algorithms. A supplicant might be configured to support both algorithms to allow association with any AP within the serving range regardless of the algorithm. An AP can also be configured as TSN to provide services to as many supplicants as possible in the network.
The TSN allows a security rollback attack to be launched against the network. To launch this attack, the adversary can impersonate the supplicant and send Associate Request messages to the legitimate APindicating that only Pre-RSNA algorithm is supported. Alternatively, the attacker can impersonate the AP and send beacons to the supplicant indicating that only Pre-RSNA security features are supported. This will enable the attacker to establish a Pre-RSNA association with a legitimate device. The attacker can then exploit the weaknesses of WEP protocol to completely undermine the security of the network. [22]

The solution to this security threat depends on the level of security the network administrator and users need to have. When network security is of utmost importance, the solution is to configure the authenticator and the supplicants so that only RSNA algorithm is allowed in the network. The downside of this solution is that network access will be available only to those devices that support RSNA algorithm.

4.4 Comparison of security features of different protocols

Table 3 gives a comparison of security features offered by different security protocols discussed in chapter 2 through 4.

<table>
<thead>
<tr>
<th>Security Protocol</th>
<th>WEP</th>
<th>WPA -TKIP</th>
<th>802.11i -CCMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption algorithm</td>
<td>RC4</td>
<td>RC4</td>
<td>AES</td>
</tr>
<tr>
<td>Encryption key size</td>
<td>40 bits</td>
<td>128 bits for encryption</td>
<td>128 bits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>68 bits for authentication</td>
<td></td>
</tr>
<tr>
<td>IV size</td>
<td>24 bits</td>
<td>48 bits</td>
<td>48 bits</td>
</tr>
<tr>
<td>Key management</td>
<td>Not available</td>
<td>802.1X/EAP</td>
<td>802.1X/EAP</td>
</tr>
<tr>
<td>Per packet key</td>
<td>IV concatenation</td>
<td>Mixing function</td>
<td>Not required</td>
</tr>
<tr>
<td>Massage Integrity</td>
<td>CRC-32</td>
<td>Michael</td>
<td>CCM</td>
</tr>
</tbody>
</table>
CHAPTER 5

EFFECT OF AUTHENTICATION PROTOCOLS ON HANDOVER LATENCY

Recent years have seen an explosive growth of the number of people accessing the Internet through portable WLAN devices like laptops, Wi-Fi telephones and PDAs. Voice over Internet Protocol (VoIP) and multimedia applications are increasingly delivered on Wi-Fi networks. Due to the limited coverage area of 802.11 networks, frequent handovers of mobile clients are highly probable and it is therefore vital to insure that different services are not interrupted during the handover period.

5.1 Handover Stages

The handover of a client device occurs when the device moves outside the RF coverage area of one AP and the received radio signal falls below a certain threshold. When this happens the client device will start scanning for another AP to associate with and once the proper AP is found, the client device will form association with this new AP. The whole handover process can be divided in two logical stages: The probing stage and the authentication (re-authentication) stage.

Probing stage: This stage starts when the received signal from the current AP falls below the preset threshold. At this point the device will start listening to beacons broadcast regularly (every 10 mS) by other APs trying to find which AP to associate with. This is a passive mode of probing stage. Alternatively the client device may perform active probing in which, apart from just listening to beacons from the APs, it will also send out probes on all its channels broadcasting its need to associate with APs that are within its RF range. The probing stage ends when the new AP to associate with is identified. [28]
**Authentication Stage:** After probing stage is completed and the new AP is identified, authentication to the new AP will start. This stage involves exchange of authentication messages. The number and nature of the massages exchanged depend on the security protocol in force. The total handover latency is the total time taken to complete the probing and authentication handover stages. The processing time of authentication messages, which include time taken to encrypt and decrypt the messages and computing message integrity checks also contribute to the total handover latency but the processing time is usually very small and its impact on the total handover delay is insignificant. [28]

This chapter will focus on the latency introduced by different authentication mechanisms used by the three WLAN security protocols: WEP, WPA and 802.11i. The authentication delay discussed in this chapter will be the total time elapsed from the instant the user device sends out he first authentication request to the time the authentication of the device to the network is complete. An analytical model based on random errors will be developed that will be used to calculate the delay caused by authentication process.

### 5.2 Authentication Delay and Quality of Service

Real-time and interactive applications such as VoIP require very low latencies in ensuring that effective communication is carried out. The guidelines for jitter in VoIP applications as issued by the International Telecommunication Union (ITU) recommend that latency should not exceed 50mS [36], [37], [38], and normal conversation usually becomes impossible when the round trip latency exceed 500mS. For streaming multimedia application, the latency should be maintained below 150mS.

Several studies have been conducted which show that latencies introduced during handover of a client device from one AP to another can adversely affect the quality of service being offered. An empirical study carried out by Mishra A. et al [36] on an indoor 802.11b network found handover latencies exceeding 500mS. This study concluded that the larger part of handover delay was caused by the probing stage of the handover. Another experiment carried out by Aboba B.
[37] show probing delays of 300 – 400ms and authentication delays of 800mS for 802.1X authentication. These studies show that the total handover latencies are intolerable for real-time and interactive applications.

The total handover delay varies according to several factors including the number of client devices attempting to access the desired access point, the level of interference in the air link and the RF characteristics of physical objects like walls, ceiling etc. High data traffic at the desired access point will increase the number of packet collisions, which increases the number of retransmissions of probing and authentication messages, consequently increasing the handover delay. On the other hand, RF characteristics of physical objects, surrounding area and the interference level in the air link will affect the strength of radio signals between the client device and the AP. These will increase the error rate of management frames, which will also increase retransmissions of handover messages, leading to the increase of handover latency.

### 5.3 Delay Analysis Model

The mathematical model developed will consider only the authentication stage of the handover process. Two major factors considered in developing the model are the number of authentication messages that need to be exchanged before for authentication of a user device and the frame error rate. Wireless networks are inherently more erroneous compared to wired networks due to several factors such as signal interference, shadowing, etc. Therefore, authentication and association frames are likely to be corrupted during transmission and will need to be retransmitted to complete the authentication process. The model considers IEEE 802.11b network.

The probing stage of the handover process will not be modeled. The model also do not take into account, queuing delay and delay caused by the collision of authentication packets with packets from other client devices.
The management frame is considered to be successfully transmitted when it is sent from the client device to the AP or vice versa and an acknowledgement frame (ACK) is received at the sending device. When either the management frame or the acknowledgement frame is lost or is corrupted, the transmission is considered to be a failure and retransmission is necessary. Retransmission timers for 802.11 devices are set to follow an exponential back-off algorithm, which doubles the retransmission time delay every time a frame is sent and an acknowledgement is not received. This means if the initial retransmission time $Tr(1)$ is set to 1mS, the device will initially wait for 1mS to receive the ACK frame, after which time it will retransmit the management frame, then it will wait for 2mS before retransmitting the frame again. The waiting time before retransmission will continue to double until either an acknowledgement is received or the maximum number of retransmissions have been reached, in which case the timer will be reset to the initial retransmission time. Therefore, the $ith$ retransmission delay will be given by equation 1:

$$Tr(i) = 2^{i-1} * Tr(1)$$

The initial retransmission delay is the configuration feature of the WLAN devices and can be set considering the device data rate and the average distance between the client device and the AP.

The probability of a frame being corrupted or lost during transmission is taken to be ‘p’. The value of $p$ depends on the length of the frame, the distance between the client device and the AP, the interference in the air link and the physical objects between the client and the AP. In the model, the value of $p$ was varied from 0.01% to 1%. The probability of retransmission, $q$, is the probability that either one or all of the management and acknowledgment frames were corrupted or lost during transmission. The value of $q$ is given by equation 2:

$$q = 1 - \left(1 - p\right)^{2}$$

The model considers 10 to be the maximum number of retransmissions for any one management frame. The number of retransmissions is a configuration factor [39] and can be changed according to the network requirements. Usually the number of retransmissions is set to be 8. [39]

If $D$ denotes the total delay due to propagation of a management frame from the client device to the AP and the propagation of the acknowledgement in the reverse direction, then the delay caused by the successful transfer of the first frame, $T_{11}$ is given by equation 3:
\[ T_{r1} = (1 - q) \cdot D \]  

- The delay caused by a successful first retransmission of a frame is given by:
\[ T_{r2} = (1 - q)(q) \cdot [Tr(1) + D] \]

- The delay caused by a successful \( nth \) retransmission of a frame is given by:
\[ T_{r(n+1)} = (1 - q)(q) \cdot 2^{n-1} \cdot [Tr(1)] + D \]

Therefore, considering the maximum of 10 transmissions for any one frame, the normalized delay, \( T_n \), for a successful transmission of a frame is given by equation 4:
\[
T_n = \frac{1}{1 - q^{10}} \left\{ (1 - q) \cdot D + (1 - q)(q) \cdot [Tr(1) + D] + \cdots + (1 - q)(q)^9 \cdot [2^9 - 1]Tr(1) + D \right\} 
\]

Thus, for a security protocol with \( N \) authentication frames, the average authentication delay, \( T_D \), will be given by multiplying the number of authentication frames with the average delay as calculated in equation 4.

### 5.3.1 Authentication Delay for WEP Open System Authentication

In open system authentication all devices that request authentication are authenticated. Only two authentication messages are transmitted between the client device and the AP as depicted in figure 11.

![Figure 11: WEP open system authentication messages](image-url)
5.3.2 Authentication Delay for WEP Shared Key Authentication

In a shared key authentication, a total of 4 management frames are transmitted between the client device and the Access Point. In the first message, the client sends an authentication request to the AP. The AP will respond by sending a challenge text. The client will encrypt the challenge text using the secret key and send the encrypted text as message number three. The AP will then decrypt and compare the decrypted text with the original challenge text and send the authentication success or failure message to the client device in accordance with the results of the comparison. The flow of messages is depicted in figure 12.

![Figure 12: WEP shared key authentication message]"
5.3.4 Delay Introduced by 802.11i Authentication

As depicted in figure 10, authentication in 802.11i-based system has three main stages: 802.11 authentication and association stage, 802.11X/server authentication and the 4-way handshake. The total number of authentication messages involved in all three stages is 13.

5.4 Results Analysis

The results of analysis of authentication delay using equation 4 are depicted in figure 13, 14 and 15. The average authentication delay increases with the increase of authentication message making the 4-way handshake employed by 802.11i to have the highest delay. Therefore the improved security offered by 802.11i protocol comes at the expense of the increased authentication delay.
Figure 14: Authentication delay for WEP shared key authentication and WPA 802.1X authentication
The obtained results are consistent with other studies carried out where it was found that latencies of about 840mS are obtained in the authentication stage and latencies of 300-400mS results from probing stage. [38]

**Limitations:** As explained in the preceding section, the authentication delay will depend on several factors including the number of authentication messages to be exchanged, the packet collision level at the access point, the queuing delay at the AP and the frame error rate. The model developed considered only the factors of frame error rate and the number of messages. The real-life authentication delay therefore is expected to be higher than the values found here.
CONCLUSION AND FURTHER WORK

The study presented in this thesis has analyzed the effectiveness and shortcomings of WLAN security protocols. The study have shown that while protocols IEEE 802.11i offers the best security of all protocols there are still some attacks that can be successfully launched against a 802.11i-secured network. The choice of a proper security protocol therefore, should be based on the importance of data being transmitted in the network.

Authentication latencies resulting from different security protocols were then analyzed. A mathematical model was developed to calculate the authentication delay depending on the number of authentication messages used in the protocol and the probability of the authentication frame being in error. It was found that highest authentication delays are found when 802.11i security protocol is employed. Authentication delay and probing delay make up the total handover latency, which is a vital measure to ensure proper handover of the WLAN mobile station from one AP to another.

This study has identified reduction of handover latency as the area where more research needs to be carried out. Different approaches towards this goal have been suggested in different researches. One approach suggested is to use cryptographic credentials that will indicate user’s behavior with the previous access point. In associating with the new AP within the same network, the client device only presents the credentials and it will be granted instant access instead of going through the whole authentication process [28]. Joshi, T. et al [31] proposes to exploit the predictability of user mobility and to distribute keys before the actual handover to necessary APs according to the predicted movement pattern. However most of the proposed approaches have a negative impact on the effectiveness of security protocol and others greatly increase the network overhead, which reduces network performance. IEEE Task Group r (TGr) is currently working on a standard for fast Basic Service Station (BSS) handoff that will enable client devices to seamlessly move between Access Points.
This study proposes soft handoff to be employed when the device is to be handed over to another BSS. In this approach the client device will continue receiving network services through the first AP while at the same time probing and authentication processes are carried out with the targeted AP. This approach will completely eliminate handover latencies. However for this approach to be practical, client devices need to be capable of communicating on two radios at the same time.


[7] IEEE Standard 802.11g, 2003; Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendments 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band


[18] Changhua He, John Mitchell; Analysis of the 802.11i 4-way handshake; Proceedings of the 3rd ACM workshop on Wireless security; 2004


[20] Jyh-Cheng Chen; Ming-Chia Jiang; Yi-wen Liu; Wireless LAN security and IEEE 802.11i; Wireless Communications IEEE; Feb 2005


[23] KeunSoon Lee, HyoJin Kim, JooSeok Song; Lightweight packet authentication in IEEE 802.11; Wireless Telecommunications Symposium, 2005; April, 2005


[26] Hiertz, Guido R.; Max, Sebastian; Zhao, Rui; Denteneer, Dee; Berlemann, Lars; Principles of IEEE 802.11s; Proceedings of 16th International Conference on Computer Communications and Networks, 2007. ICCCN 2007; Aug. 2007


[31] Tarun Joshi, Anindo Mukherjee, Agrawal, D.P.; Exploiting Mobility Patterns to Reduce Re-Authentication Overheads in Infrastructure WLAN Networks; Canadian Conference on Electrical and Computer Engineering; May 2006


[33] Andrew S. Tanenbaum; Computer Networks; Fourth edition; Prentice Hall, 2003

[34] Robert Moskowitz; Weakness in Passphrase Choice in WPA Interface; Online at: http://www.wifinetnews.com/archive/002452.html; 2003


[37] Aboba, B.; Fast Handoff Issues; IEEE-03-155r0-1 IEEE 802.11 Working Group; March 2003

[38] Chen, J., Tseng, Y., Lee, H.; A Seamless Handoff Mechanism for DHCP-Based IEEE 802.11 WLANs; IEEE Communication Letters; August 2007.
[39] Barsocchi, P., Oligeri, G., Potorti, F.; Frame Error Rate in Rural Wi-Fi Networks; IEEE WiNMee/WitMeMo Workshop; April 2007

[40] Huang, J., Seberry, J., Susilo, W., Bunder, M.; Security Analysis of Michael: The IEEE 802.11i Message Integrity Code; International Conference on Embedded and Ubiquitous Computing, EUC 2005; December, 2005;
BIOGRAPHICAL SKETCH

Donation Mkubulo was born on November 29, 1975 in Tanzania, a country in East Africa. He received a Bachelor of Science degree in Telecommunication Engineering from the University of Dar es Salaam in 2003. During his undergraduate studies, he worked for a wireless communication company as an engineering intern acquiring a hands-on experience in different area of GSM wireless network. These areas include installation of RF equipments, network performance analysis, and GSM cell planning and RF interference analysis. He joined Florida State University in January 2006 to pursue a Master of Science degree in Electrical Engineering. His research interests include wireless networks security protocols, routing algorithms in ad hoc networks and cellular networks. Donation Mkubulo is a member of the National Society of Black Engineers (NSBE).