

**ANALYSIS OF WIFI SECURITY PROTOCOL WITH
CHALLENGES AND SOLUTIONS**

BY

MD. ABDULLAH AL NOMAN SHAKIL

ID: 151-19-1682

HANUFA AKTER NISHU

ID: 151-19-1696

ZINNIA FERDOUS TRITIYA

ID: 151-19-1637

This Report Presented in Partial Fulfillment of the Requirements for the
Degree of Bachelor of Science in Electronics and Telecommunication
Engineering

Supervised By

Md. Taslim Arefin

Associate Professor & Head

Department of ICE

Daffodil International University



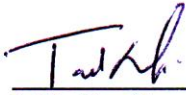
**DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA, BANGLADESH**

January-2019

APPROVAL

This Project titled “**Analysis of wifi security protocols with challenges and solution**” submitted by Md. Abdullah Al Noman Shakil and Hanufa Akter Nishu and Zinnia Ferdous Tritiya to the Department of Information and Communication Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Electronics and Telecommunication Engineering and approved as to its style and contents. The presentation was held in January, 2019.

BOARD OF EXAMINERS



Md. Taslim Arefin

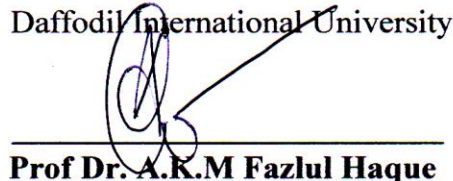
Associate Professor & Head

Department of ICE

Faculty of Engineering

Daffodil International University

Chairman



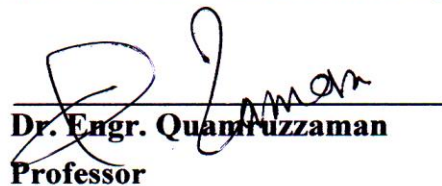
Prof Dr. A.K.M Fazlul Haque

Professor

Department of ICE

Daffodil International University

Internal Examiner



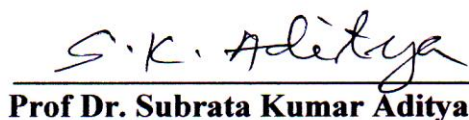
Dr. Engr. Quamruzzaman

Professor

Department of ICE

Daffodil International University

Internal Examiner



Prof Dr. Subrata Kumar Aditya

Professor

Department of EEE

University of Dhaka

External Examiner

DECLARATION

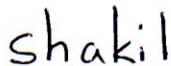
We hereby declare that, this project has been done by us under the supervision of **Md. Taslim Arefin, Associate professor & Head, Department of ICE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

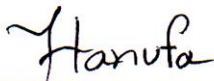


Md. Taslim Arefin
Associate professor and Head
Department Of ICE
Daffodil International University

Submitted by:



Name : Md. Abdullah Al Noman Shakil
ID :151-19-1682
Department of ICE
Daffodil International University



Name : Hanufa Akter Nishu
ID: 151-19-1696
Department of ICE
Daffodil International University



Name: Zinnia Ferdous Tritiya
ID: 151-19-1637
Department of ICE
Daffodil International University

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty Allah for his divine blessing makes us possible to complete this project successfully.

We feel grateful to and wish our profound indebtedness to, **Mr. Taslim Arefin** Associate Professor and Head Department of ICE, Daffodil International University, Dhaka. Deep knowledge and keen interest of our supervisor in the field of wireless influenced us to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to **Dr. A.K.M Fazlul Haque** associate Dean, faculty of engineering, **Dr. Md. Golam Mowla Choudhury** Professor of the Department of Information and Communication Engineering, **Dr. Subrata Kumar Aditya** Professor and Chairman Department of Applied Physics Electronics and Communication Engineering University of Dhaka, **Mr. Taslim Arefin** Associate Professor and head Department of ICE. **Ms. Shahina Haque** Assistant Professor of Department of ICE. And also to other faculty member and the staffs of ICE department of Daffodil International University.

We would like to thank our all course mate in Daffodil International University, who took part while completing the course work.

Finally, we must acknowledge with due respect the constant support and patience of our parents.

ABSTRACT

Wireless local area networks (WLANs) with the gateway to internet services are becoming popular as they are fast, cost effective, flexible and easy to use. There are some challenges of security. The main motive is to know about threats in the wireless security and be aware about the disadvantages of wireless security protocols. There is also a comparative Authentication analysis of many kinds of security protocols. Wireless networking is an emerging technology that will allow users to access information and services regardless of their geographical position. In contrast to infrastructure based networks, in wireless networks, all nodes are can be connected dynamically in a random manner. All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. In This project WiFi Network has been designed by using WEP, WAP and 802.11i routing protocol. The performance of those routing protocols have been investigated by comparing various Simulation parameter such as End2End delay, lost and output. The delay for individual protocol and also collected lost information which is found by simulation. The output which is compared with different protocol to determine that which protocol is the best and standard solution for wifi security protocol.

List of Figures

Figure 3. 1: stream chipper encryption.....	12
Figure 3. 2 Block chipper encryption.....	13
Figure 3. 3 : wep key generation and encryption.....	15
Figure 4. 1: TKIP mixing and encryption stag	25
Figure 4. 2 : Components of 802.11X system.....	29
Figure 4. 3: Message flow during authentication process	30
Figure 5. 1: Key generation for 4 way handshake operation.....	35
Figure 5. 2: Key generation for group key hierarchy	36
Figure 6. 1: 802.11i delay Authentication	43
Figure 6. 2: WEP Open System Authentication	43
Figure 6. 3: WEP Shared Key Authentication.....	44
Figure 6. 4: 802.11i delay Authentication	44
Figure 6. 5: WEP Open System Authentication	45
Figure 6. 6: WEP Shared Key Authentication.....	45
Figure 6. 7: 802.11i delay Authentication	46
Figure 6. 8: WEP Open System Authentication	46
Figure 6. 9:WEP Shared key Authentication.....	47
Figure 7. 1: 802.11i Authentication Delay vs WPA Delay.....	50
Figure 7. 2: WEP Authentication Delay vs 802.11i Authentication Delay	51
Figure 7. 3:WAP Authentication Delay vs WEP Authentication Delay	51
Figure 7. 4:802.11i Lost vs WPA Lost.....	52
Figure 7. 5: 802.11i Lost vs WEP Lost	52
Figure 7. 6: WEP Lost vs WPA Lost.....	53
Figure 7. 7: WEP ,WPA & 802.11i Delay	53
Figure 7. 8: WEP ,WPA & 802.11i Lost	55
Figure 7. 9: WEP ,WPA & 802.11i Output	56

Contents

APPROVAL	ii
DECLARATION	iii
ACKNOWLEDGEMENT	iv
ABSTRACT.....	
.....	v
CHAPTER 1	1
1.1 Introduction.....	1
1.2 Research Motivation.....	2
1.3 Aim and Objectives.....	2
1.4 Report format	3
CHAPTER 2.....	4
LITERATURE REVIEW	4
2.1 Wireless Networks.....	4
2.2 802.11 Physical Layer	4
2.4 WLAN Architecture	7
2.5 Wireless Security Threats.....	8
CHAPTER 3.....	11
3.1 How WEP Works	11
3.1.3 WEP Data Encryption	15
3.2 WEP Security Features	16
3.2.2 information Integrity.....	16
3.2.3 Verification	17
3.2.4 Access Control.....	17
3.3 WEP Vulnerabilities.....	18
3.3.1 Susceptibility to brute pressure attacks	18
3.3.2 assaults because of the reuse Initialization Vector	18
3.3.3 Message change assaults.....	19
3.3.4 Station Association Attacks.....	20
CHAPTER 4.....	22
4.1.3 802.11X.....	28
4.2 WPA-Personal	31
CHAPTER 5.....	33
5.1 Data Confidentiality and Integrity.....	33
5.2 Authentication and Key management	34
5.3 Analysis of Security Offered by IEEE 802.11i.....	38
5.3.1 Eavesdropping, Traffic Analysis and Message Injection	38

5.3.2	Session Hijacking	39
5.3.3	Man-in-the-Middle	39
5.3.4	Security Level Rollback Attack	40
5.4	Comparison of security features of different protocols	40
CHAPTER 7.....		48
PERFORMANCE ANALYSIS.....		48
7.1	Performance of routing protocols.....	48
7.1.1	802.11i Authentication Delay vs WPA Delay.....	48
7.1.2	WEP Authentication Delay vs 802.11i Authentication Delay.....	51
7.1.3	WAP Authentication Delay vs WEP Authentication Delay.....	51
7.1.4	802.11i Loss vs WPA Loss.....	52
7.1.5	802.11i Loss vs WEP Loss.....	52
7.1.6	WEP Loss vs WPA Loss.....	53
7.1.8	WEP ,WPA & 802.11i Loss	54
7.1.9	WEP ,WPA & 802.11i Output.....	54
CHAPTER 8.....		55
CONCLUSION AND FUTURE WORK.....		55
8.1	Conclusion.....	55
LIST OF ACRONYMS		57
References		62

List of Table

Table 4. 1: capabilities the actual contrasts amongst WPA and WEP safety conventions.....	23
Table 5. 1: Comparison of security protocols	41

CHAPTER 1

INTRODUCTION

1.1 Introduction

Remote systems have encountered an unstable development as of late. This quick development is because of expansion of smart phones, Digital Assistants (PDAs) and other handheld gadgets and furthermore because of numerous favorable circumstances offered by remote systems to both the client and the system administrator. To the client remote systems offers portability and the adaptability of having the capacity to get to the system from wherever. Today it is typical to discover individuals perusing their messages, downloading records, audio media and images from through the remote system with support of internet. To arrange administrator, remote systems permits fast sending and adaptability of systems without the need of spreading out links.

The omnipresent utilization of remote systems have likewise carried into center security issues related with these systems. Aside from acquiring all the security issues experienced by wired systems, remote systems have further problems caused by the idea of the media communication. Mails are communicated transparently ended waves of radio and are not ensured by carnal obstructions as in wired systems, capture attempt and hiding by a gatecrasher turns out to be simple for anybody with just essential types of gear. This features the need of guaranteeing that remote systems are legitimately anchored.

The motivation behind this proposition uses to contemplate the issue of security in remote systems with accentuation on IEEE 802.11 systems. The report will begin by talking about security dangers looked by remote systems. The report will at that point take a gander at the security conventions recommended to relieve the dangers. Adequacy and weaknesses of every security convention will be investigated. The proposition will at that point contemplate the inertness presented by confirmation method when a customer gadget needs to connect with a passage. A defer investigation typical figure will be created and utilized for compute delays presented by various security conventions.

1.2 Research Motivation

In the earlier time, wireless networking system has liked a great and progressively increasing popularity in research purpose and industry purpose. Even though simulation is standard tool for analyzing wireless network protocols, and it suffers from lots of problems which is full of information. Firstly, there have fundamental mathematical expression are typically impervious and no available for users. That's why they are often impractical, and its output result can differ broadly between field experiments and different simulators . Therefore, the simulation results can depend upon the simulator. Secondly, simulators generally do not support computational behaviors like non-determinism, yet again foremost to unrealistic results. Really, in some cases non-determinism is treated probabilistically, suggesting incorrect calculations for any environment that do not obey through these expectations. Thirdly, for the optimization of a protocol there have needs thorough comparison of many designs. The comparative studies with simulation it requires statistical explanation of the simulation runs which is expensive, it also making all projected analysis expensive and also difficult . Formal methods applications which is requires for the analysis of computer networks. which is generally motivated by desire to knowing them widely, that is, to increase range, penetration, and dependability of the analysis, increasing attention, practicable system difficulty, and penetration of output. There have lots of successful applications of probabilistic model which is related with the wireless networks. Though, its practicability is naturally incomplete with small networks and an actual representation of this physical features of wireless communication has usually avoidable. Given the recent simulation with network simulator which is applicable for wireless network .we use there some parameters for find out the delay, lost and output. There have given some authentication depend upon simulating time and try to given some comment about challenges which is avoidable for proper solation .

1.3 Aim and Objectives

The purpose of writing this paper is that we discussed the protocols of the wifi and through practical encryption. We tried to show the experimental output to gain knowledge about the WiFi Security Protocol and also Understand the problems about the WiFi Security Protocol in maintaining and absolutely how its works with it challenges and solutions. We have also tried to do proper encryption to deal with

various challenges and provide some best and most collective solution. We will try to show some of the ways in which will provide more security and confidence in the future through our practical work.

The aim of this thesis is are given below:

- To gain proper knowledge about WiFi Security
- To analyze the rules theoretically with Simulation
- Suitable protocol will provided for depend upon situation
- To discuss about Security Features

1.4 Report format

In this paper we have to discuss about wifi security protocol like WEP,WPA and 802.11i Security protocol. Description of this security protocol are given there sequentially.

This thesis paper have 5 chapter individually. In chapter 1 there have given about this paper aim and objectives , Motivation with introduction ,In chapter 2 there have given about wireless network over and security threats in over-all. On the other side chapter 3 and 4 is defines about the WEP protocol and the WAP protocol respectively. In this both chapters are defines about their features ,verification and how they work personally. There have another chapter 5 is discuss about 802.11i security protocol and the chapter 6 of the paper is simulation analysis part which is make up for showing our works what we have done already in screenshots process.At the end chapter 7 is performance analysis

CHAPTER 2

LITERATURE REVIEW

2.1 Wireless Networks

The period of 'Remote systems' on this proposition will allude to the media transmission arrangements in which the relations between various hubs are executed by the wire uses. The maximum widely recognized remote advances can be isolated into various classes as per the inclusion territory of the systems. The biggest remote systems are the cell arranges and can protection the entire nation or after taken together it can asylum the entire world. Following classifications of remote systems is the (MAN) Metropolitan Area Networks has an inclusion region of the entire city. IEEE 802.16(WiMAX) is standard form that can give universal inclusion for the entire Geographic Area. Entire neighborhood, IEEE 802.11(Wi-Fi) is the standard that gives WLAN (Wireless Network Area Network). At long last on the individual region part, IEEE 802.15 standard Bluetooth gives availability to remote systems inside the inclusion separation of up around 10 meters.

Wi-Fi has encountered an unstable development lately because of numerous favorable circumstances offered by these systems. Aside from client versatility, which is the fundamental advantage existing with WLAN, other significant preferred standpoint is adaptability. Clients have same adaptability to build up and disassemble WLAN effectively for providing food for briefly utilization, for example, gatherings, exchange carnivals or meeting. Others preferred standpoint the simplicity with selected topologies is designed to see diverse utilizations from little home used to vast college grounds which permits wandering done extensive territory. WLAN additionally takes into consideration quick establishment, as no wires should be spread out.

2.2 802.11 Physical Layer

Standard of 802.11 utilizes the utilization 2.5 GHz and 5GHz immoral recurrence groups in correspondence. The IEEE discharged the main Wireless neighborhood form, on The Institute of Electrical and Electronic Engineers form 802.11 in 1997. Standard form gave details for WLAN that utilized the 2.5 GHz band. Information charges accomplished by fundamental systems which is 1 Mbps, 2

Mbps. Enhanced forms of IEEE 802.11b working in 2.5 GHz recurrence band and donation information tariffs of up to 11Mbps discharged in 1999. An enhanced information tariffs was practically identical for that existing by cabling LAN. Along these lines unbolted up business reasonability of WLAN. Form of IEEE 802.11a was well along discharged donation information tariffs of 54 Mbps and working on 5 GHz. In spite of the developed information tariffs offered by form of 802.11a. It was not measured as option in contrast to another form of 802.11b as utilized an alternate recurrence form. That utilized by another form 802.11b. 2003, June IEEE authorized form 802.11g which is utilized (OFDM) Orthogonal Frequency Division Multiplexing innovation to proposal information tariffs of up to 54 Mbps in a 2.5 GHz band. Normally it was generally executed by Wireless Local Area Network gadget sellers because of a higher quantity, recurrence band similarity with 802.11b form. Additionally enhance the data, IEEE is dealing with another form, IEEE 802.11n, which flow was distributed in 2007. New form accommodates various alternatives and distinctive setups, which offer diverse information rates. At the point when every ideal choice are utilized, 802.11n form can bolster information s tariffs up to 600 Mbps.

Enhance execution, 802.11n form utilizes Many Input, Many Output procedure. With Many Input, Many Output innovation, various radio wires are utilized on WLAN gadget. Amid broadcast, the broadcasting WLAN gadget parts information hooked on various portions called three-dimensional streams and conveys each three-dimensional stream through isolated reception apparatus to relating receiving wire on less than desirable finish. Expanding the quantity of three-dimensional streams respectively builds the broadcast quantity, the adjustment being expanded power utilization. 802.11n form likewise utilizes different methods, for example, pillar framing, spatial assorted variety, and MIMO control spare to additionally enhance execution. With bar shaping, the radio signs are guided directly to the accepting receiving wire in this manner lessening signal power misfortune and impedance. Assorted variety system puts being used additional reception apparatuses that might be found on a WLAN gadget to join yield signals from those radio wires and along these lines getting a more grounded flag. This empowers a WLAN gadget to work at a more extended territory. A case of this is the point at which a PC with two receiving wires interfaces with (AP) Access Point with four reception apparatuses. Just two

three-dimensional streams can be directed from PC however those will be gotten on the four access Point receiving wires, hence, yield from two AP reception apparatuses might be consolidated to get single three-dimensional stream.

Table 1 Given a Shortest of the core IEEE standards that postulate wireless LAN Media Access Control and Physical Layer are needed.

Table 2.1: To the point of the main features of many WLAN standards approved by IEEE

WLAN Standard	Approved Year	Operational Frequency	Extreme Data Rate	Physical Layer
802.11b	1999	2.4 GHz	11 Mbps	DSSS
Legacy 802.11	1997	2.4 GHz	2 Mbps	FHSS/DSSS
802.11g	2003	2.4 GHz	54 Mbps	OFDM
802.11n	2007	2.4/5 GHz	600 Mbps	MIMO
802.11a	1999	5 GHz	54 Mbps	OFDM

2.3 802.11 Media Access Control sub layer protocol

The essential contact strategy of 802.11 systems is Carrier Sense Multiple Access with (CSMA/CA) Collision Avoidance. On this system get to convention when position needs to broadcast, it initially sends an administration outline referred (RTS) Request to Send. This casing show the term of accompanying broadcast, source and part of this information. Beginning to the receipt of the Request To Send outline, If the Destination is permitted to get information, it is send back the (CTS) Clear to Send outline. Those casing is duplicate transmission period which showed in the Request To Send(RTS) outline. Endless supply of (CTS) Clear To Sound outline, asking for place will begin spreading information. Stations hearing Request To Send (RTS) or potentially Clear To Send (CTS) edges will withdraw sending information for the span demonstrated in this casings. Component lessens likelihood of packages impact for the goal, as all places that is not in asking for radio stations range, and along these lines couldn't found the Request To Send will found the Clear To Send from the goal, and it will cease from broadcasting.

2.4 WLAN Architecture

Fundamental 802.11 of WLAN figure is comprised of (BSS) Basic Service Set. BSS is comprised remote stations (PDAs ,PCs, and so on) speaking with one another over a (AP) Access Point. AP goes about like a base station WLAN, connecting system to wired system. Solid inclusion territory of a Basic Service Set relies upon numerous variables, for example, wellsprings of RF impedance, physical complaints in zone and qualities, Wired LAN gadget power also receiving wire utilization. Entire WLAN should comprised one otherwise a few BSSs. A mix of conveying For the remote system to be secure, the administrations of privacy, validation, trustworthiness and accessibility must be completely assumed by security conventions.

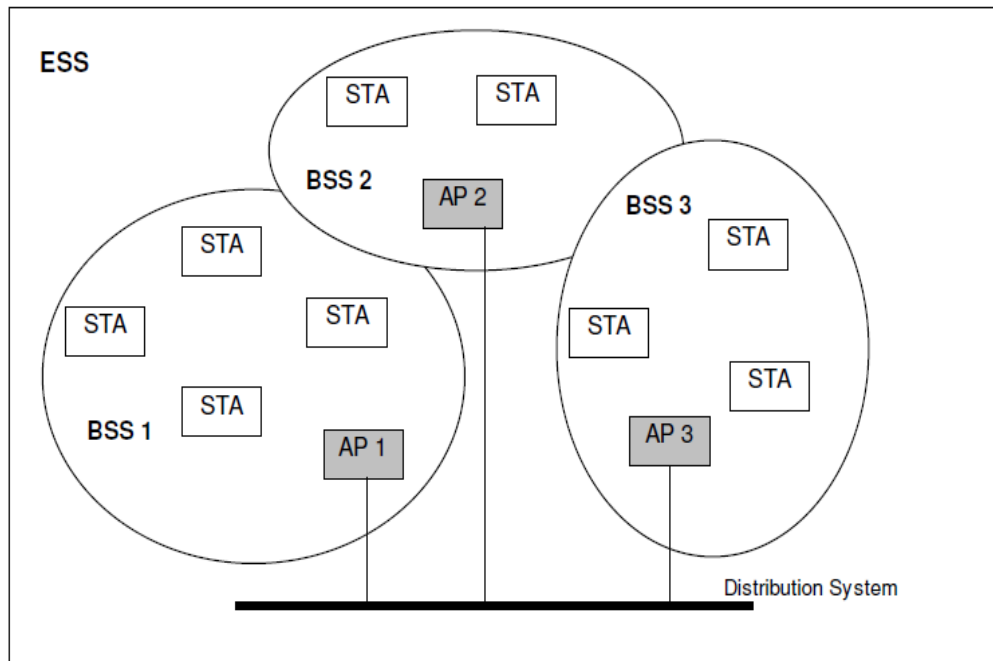


Figure 2.1.: WLAN architecture

Confidentiality :Motivation behind of security benefit is gives guaranteed just approved people can see the information broadcasted on both sender and the collector. Security convention of course equipped for avoiding listening in of the information.

authentication: This security benefit ensure that just the approved people participate in the correspondence procedure; that is just approved gatherings can get to the system and send or get information from the system. The security convention must be fit for building up the characters of gatherings before those gatherings are engaged with correspondence.

Rectitude of Data: Motivation behind of security benefit is guaranteed reliable with information in system. Safety convention should fit for averting expansion, evacuation or alteration of information both of the sender and recipient.

Availability of Network: This administration guarantees which is organize all open assets and serviceable at whatever point required by the approved substances.

2.5 Wireless Security Threats

Assaults with a remote systems will partitioned with two general classifications like uninvolved and dynamic assaults. Detached assaults allude to the security rupture in

which an unapproved individual accesses the system and information being transmitted in the system yet does not adjust the information. Then again, dynamic assaults allude to security ruptures whereby an interloper accesses organize resources and adjusts the substance of information is transmitted for both sender to collector. In the following given deprived of assaults that is propelled on remote systems:

Eavesdropping: This is a uninformed assault in which is approved individual screens traffic in a remote system for message content.

Analysis of Traffic: This sort of assault, an approved individual supplies whole traffic on the remote system, also attempts to carry out in halfway and finish data from gathered data. It is additionally an uninformed assault like there have no endeavors complete to effort to adjust first data.

Masquerading: This kind of assault the attacker mimics an authentic client and increases unapproved entree to system.

Deletion of Message: In this type of active assault, the assailant can expel information after the system earlier it achieves the planned goal. It is normally completed by meddling with information on the recipient reception apparatus or else making information appear as it contains blunders driving the beneficiary to dispose of the information. The enemy can prepare this assault to reject a real gadget entree to system with doing erasing all or else portion of the mails are required toward validate a gadget earlier conceding it entree to system.

Denial of Service (DoS): This DoS assaults, this aggressor keeps genuine clients from the utilization or the board of a system resource. DoS assault more often than not comprises of recurrence sticking whereby the aggressor meddles through the entire of repetition band utilized in broadcast of information by transfer signals through more influence on a similar recurrence. Additionally DoS assaults can be propelled abusing the way in which stations have to dispensed to Wired LAN hubs wanting to convey information. This assailant container make customer gadget think the stations are occupied besides concede transfer information trusting that the station will inert. Moreover, Denial of Service assaults in contradiction of a system can remain propelled through immersing system gadget with solicitations to like an extent .It

can't react toward real circulation and in this manner making that specific gadget inaccessible to genuine clients.

Session Hijacking: The aggressor can trust that the real system gadgets will finish confirming themselves and after that it can capture the session between the gadgets by separating one gadget and taking on the appearance of the detached gadget. In this kind of assault the assailant will have the capacity to get all information bound to the separated gadget and sending information as the genuine gadget. This assault is generally propelled after a genuine gadget is confirmed to the system accordingly a maverick gadget does not need to experience validation.

Message Replay: This is a functioning assault whereby the aggressor accesses system, catches and retransmits messages to at least one goals as the real client. Through re-sending messages, enemy making the expected mark re-play out a similar assignment various occasions and neglect to perform other authentic undertakings. In another shape, the enemy can utilize this assault to access unapproved arrange benefits by catching the secret word provided by the client gadget, and replaying that secret word to the AP, in this manner accessing administrations presented by AP.

Man-in-the-center: This assault an enemy disruptions an immediate association among the remote position and passage and goes about like a center gadget among two gadgets. Toward an authentic client gadget the maverick gadget will show up like an AP although to the genuine AP is the rebel gadget determination show up like the client gadget. On this assault empowers enemy to switch the information transferred among the reliable client gadget and the AP. For instance when the client needs to get to a specific website folio, assailant can alteration the location of asked for page before sending the demand to the AP. Subsequently a real client will get an alternate site folio. Moreover, the conveyed page may require the client to enter touchy data, for example, charge card identification, client designation besides secret phrase, which is the assailant container usage for unapproved resolutions.

CHAPTER 3

THE WEP PROTOCOL

Wired Equivalent Privacy (WEP) is a security protocol, which is provided by IEEE Wireless Fidelity WiFi standard like 802.11b. It is designed to offer a (WLAN) wireless local area network and also contains level of privacy and security comparable which is actually expected with wired LAN. Local area network (LAN) is usually endangered through physical security instruments that are effective for a controlled physical environment.

3.1 How WEP Works

3.1.1 Data Encryption Background

Data encryption is a procedure which is changing information through plaintext to the frame which is confused to unintentional beneficiary containing the cipher text. Encryption uses algorithm to turn normalized plaintext into cipher text that is unreadable without a special key which is decrypt them. Symmetric key encryption is known as private key encryption because it works with private key which is used for encode and decode information for receiver and sender individually. Both receiver and sender have to learn about mystery key controlling the responsibility to happen. A part of prevalent private key encryption calculated incorporate (AES) advanced encryption system. On the other hand Open key encryption generated by (Triple DES) Triple Data Encryption Standard and (RC4) Rivest Cipher calculation. Then again utilizes diverse keys for encryption and unscrambling. Open Key encryption calculation is known as RSA calculation.

Stream and Block Encryption: Cipher texts should be using two systems:

- a) Stream cipher encryption
- b) Block cipher encryption.

On the stream cipher text encryption each bit of data is encrypted using one bit of plaintext.

That is, given a plaintext P and the corresponding cipher text $C = E(P)$, it is possible to generate $C1 = f(C)$ so that ,
 $D(C1) = P1 = f'(P)$

with arbitrary, but known, functions f and f' .

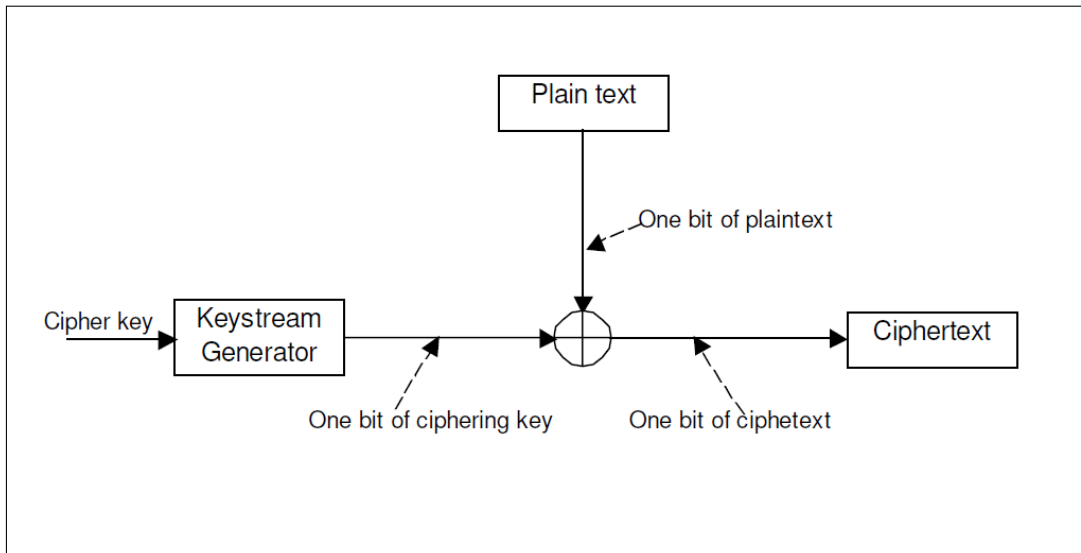


Figure 3. 1: stream chipper encryption

A block cipher is a multipurpose algorithm which apparatuses a key-dependent transformation of values which are arrangements of a fixed number of blocks. This is used for many characters in various kinds of cryptographic protocols. One such role is majority encryption of long streams of data; to gain lie a thing, block cipher essential to used with an appropriate mode of operation the traditional one being CBC, and the trendy newer mode being CTR.

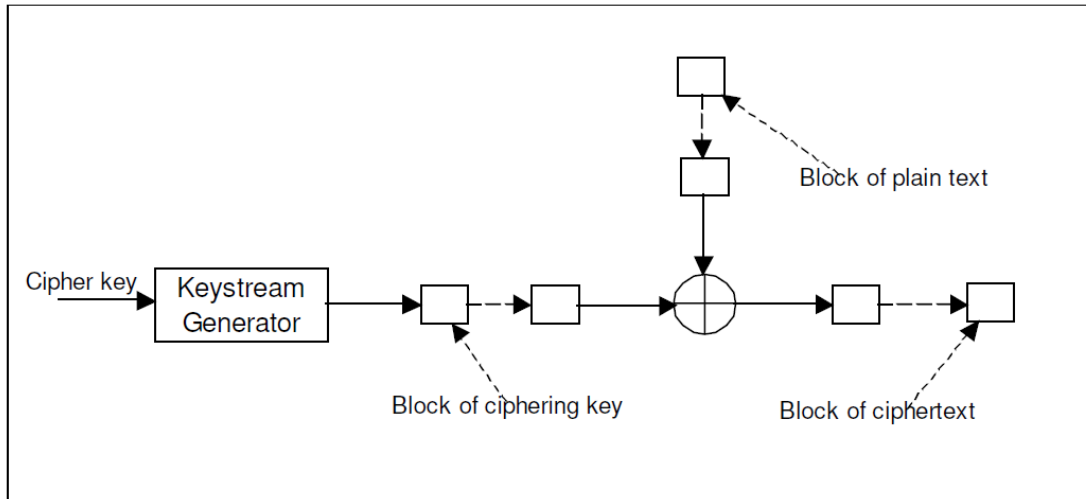


Figure 3. 2 Block chipper encryption

3.1.2 RC4 Algorithm

The RC4 algorithm uses carry with IEEE standards 802.11 with in Wireless Encryption protocol utilizing 40 bits and 128 bit keys. It cracking the security measurement as executed in Wireless Encryption Protocol by existing published procedure.

RC4 is a stream figure, encryption of symmetric key calculation which is planned in 1987. Trademarked to RSA Data Security Inc. It has 1 to 256 bits length variable. Standard generation of Wireless Encryption Protocol application 40 bit key is utilized, albeit diverse sellers have executed distinctive lengths of key to equal to 104 bits. Encryption key used to create 256 piece state-run table which is later utilizing for build up pseudo-arbitrary piece torrent, It is XORed through plain content to produce cipher text.

RC4 calculation works with two stages:

- (1) Key-booking stage
- (2) figuring stage.

In key planning stage, the 256 piece state-run table, T is inhabited utilizing k. Every component on the state-run table is then exchanged at any rate when to guarantee irregular estimations of that table. Key-planning calculation should be utilizing this pseudo code which is given underneath:

b = 0;

for a = 0 to 255 T[a] = a;

for a= 0 to 255

b = (b + T[a] + k[a mod *keylength*]) mod 256 swap T[a] and T[b]

end

When the key-planning stage is finished, figuring will follow, which is incorporates and gives randomization of table qualities to acquire figuring key, which is XORed through plain content to get ciphertext. The pseudo code is underneath which is used for outlined of this stage :

b= a = 0;

for k = 0 to N-1

a = (a +1) mod 256

b = (b +T[a]) mod 256 swap T[a] and T[b]

ck = T[(T[a] +T[b]) mod 256] output M[k] XOR ck

end

Here, M[0...N-1] is input message containing of N bits and cipher key *ck*

Because of speed of implementation and effortlessness in programming and equipment usage, the RC4 is a standout amongst the maximum broadly utilized stream structure. This is utilized for security conventions, for example: Microsoft

Point-to-Point Encryption (MPPE), WEP, WPA, Cipher saber and (SSL) Secure Socket Layer.

3.1.3 WEP Data Encryption

the RC4 symmetric stream cipher algorithm is uses for WEP encryption with 40 bit and 104 bit keys of encryption. 40 bits keys are standard 104bit are not standard, but maximum wireless AP vendors backing them. The mystery key (k) is provided on WEP with approved station which is ensure system information.

Period 1: The (ICV) Integrity Checksum Value is determined with message outline (M), at that point the Integrity Checksum Value and M are linked with frame plaintext P = [M, c(M)] which is scrambled.

Period 2: RC4 calculation utilizes a typical mystery key and instatement vector (IV) to create a stream key meant by RC4 . The Initialization Vector is different for every casing while mystery key is maintain consistent. On the performance An XOR activity is shown . It also performed on the RC4 key stream and plaintext, p to deliver a cipher text ,
 $C = P \oplus RC4(IV, k)$

Period 3: (IV) Initialization Vector with the Cipher text (C) together are communicated with the radio connection. The Initialization Vector isn't encoded and transmitted like plaintext.

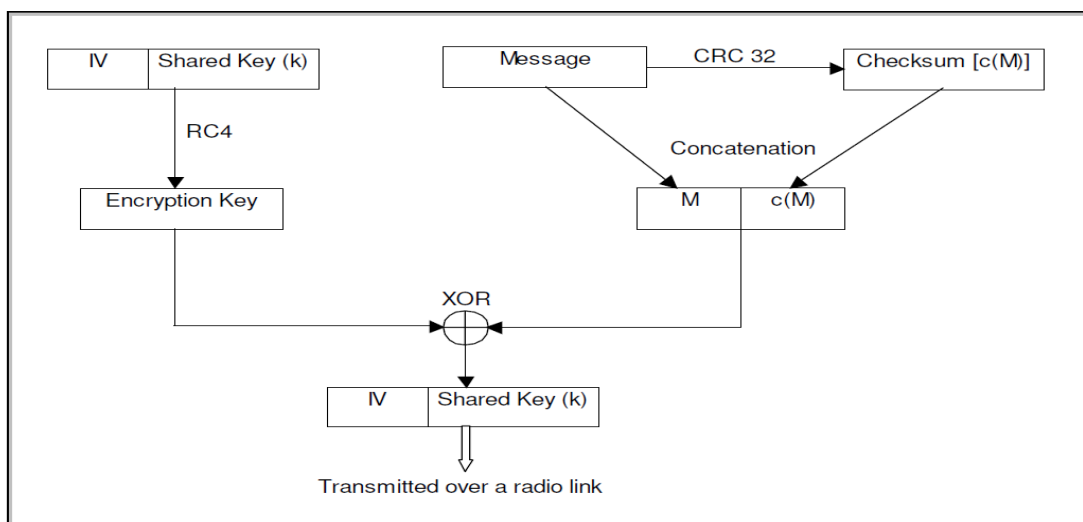


Figure 3. 3 : wep key generation and encryption

On the less than desirable closing the accompanying procedures is comprised to recoup check the uprightness and the first message and of the information which have got:

Period 4: Getting station becomes the (IV) Initialization Vector from the messages and uses it composed with (k) mystery key and the RC4 calculation to acquire the key stream which is known RC4. Key stream is connected happening the gotten between cipher text and the recuperate plaintext as demonstrated as follows:

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

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

Period 5: Beneficiary station at that point parts the plaintext to message and the (ICV) Integrity Check Value. The Checksum is formerly figured in the message besides contrasted and one got on the plaintext. On the event that the given checksums is equivalent message is acknowledged and correspondence is finished.

3.2 WEP Security Features

3.2.1 Confidentiality

The first WEP utilizes a 24 bit Initialization Vector (IV) and 40bit key together with a in framing a RC4 traffic to enter utilized trendy encoding messages. Whole gadgets of a system, passages and positions, utilized a similar key, which is intended to remain a mystery for given system. Changing the mystery key required physically changing the key location for all gadgets, troublesome assignment for vast system.

3.2.2 information Integrity

WEP turned into supposed to avoid alteration and altering of transmitted messages by means of figuring and the Integrity take a look at a (CRC) Cyclic Redundancy Checksum through value over at tmessage outline. ICV together with message outline are altogether scrambled and conveyed to the intention in which the encoded casing is decoded and the primary ICV is recuperated. Brand new ICV is then decided on unscrambled message and contrasted with the got ICV. At the off chance that the

two are same a message is recounted as credible usually the were given message is disposed of.

3.2.3 Verification

previous to portable stations (PDAs ,computers and so forth) are authorized to get to the system, they need is tested into the gadget. For done this, the WEP relies upon on the information of a thriller shared key many of the flexible stations. simply stations with the records of the thriller key may be accepted to connect with device.

A test and response method is utilized before accomplice a station. at the factor when a station demands affiliation, the serving get entry to factor will send a check to the station comprising of 128 bits of clear text. On accepting the check, the flexible station will scramble it utilizing the thriller key and ship the encoded flag back to the get admission to factor. The get admission to factor will at that factor unscramble the flag and comparison the decoded content and the primary plaintext. on the off hazard that the two are equal the station might be considered to have the right key and could be accredited to connect with the gadget. IEEE 802.11 general additionally carries a discretionary aspect that permits stations to put off all parcels that are not accurately encoded utilizing WEP.

3.2.4 Access Control

First the 802.11 supports the open access control design. Through this setup, somewhat client is equipped for getting to the system, which is proportionate to having no entrance control by any stretch of the imagination. Be that as it may, distinctive remote gear merchants actualized two noteworthy methods for controlling the clients' entrance to the system.

Access Control List

This is any other gadget used by sellers. Through this gadget, a passage keeps up a rundown of clients approved to get to the device. The rundown depends on customers' MAC addresses and simply customers whose the MAC addresses are at the rundown may be fit for getting to the gadget. on the off chance that the MAC address of the patron isn't recorded at the get entry to point the client isn't always allowed get admission to to the system. This approach for get admission to control has its very personal deficiencies. seeing that 802.eleven gadget interface playing cards permit

their MAC delivers to be modified, an aggressor can without an awful lot of a stretch detour this thing by way of latently checking the transmissions inside the machine and making up a rundown of MAC grants permitted to get to the device. The aggressor may additionally then exchange his MAC supply to one of the authorized locations and alongside these strains gaining access to gadget.

3.3 WEP Vulnerabilities

The WEP as defined in the authentic IEEE 802.11 fashionable form has stood recognised to fail in all the 3 protection dreams it turned into meant to offer. underneath is a discussion of the susceptibilities encountered when usage of WEP.

3.3.1 Susceptibility to brute pressure attacks

WEP conference characterized in IEEE 802.11 popular makes use of a 40bit key and 24bit together with the instatement Vector in generating the RC4 stream key. since Initialization Vector is communicated transparently and are like a result available to the ability assailants, main piece of the key this is thriller is 40 bit key. it's been indicated that an interloper through an outstanding computer may additionally decode the message by using generating each conceivable change of the key. anyway extended renditions of WEP had been created that deliver key lengths of as much as 104 bits collectively with 24 bit advent vector. Its makes a savage assault for all intents and functions hard to finish despite the most brilliant pcs currently in marketplace.

3.3.2 assaults because of the reuse Initialization Vector

Wireless Encryption Protocol works with the aid of using a regular mystery key (k) to all positions on the machine besides an open introduction Vector. The RC4 calculation resolve at that point utilize the thriller enter and the IV to developing a stream key utilized in scrambling reply's. The entanglement on this technique is it at anything factor the Initialization vector is utilize again,RC4 calculation is produce equivalent stream key and the 2 scrambled reply's is probably utilized to get statistics approximately the primary messages as confirmed as follows

$$C_1 = P_1 \oplus RC4(IV, k)$$

$$C_2 = P_2 \oplus RC4(IV, k)$$

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

$$C_1 \oplus C_2 = P_1 \oplus P_2$$

thus gambling out an XOR activity on two cipher texts produced using a comparable (IV) Initialization Vector resolve create a yield of XOR project to the first plaintexts from which the primary messages may be gotten uncertainty fractional mastering of single of the plaintexts is thought. Toward preserve this form of the WEP standard prescribes the Initialization Course be transformed for each package. in any case, (NICs) most network Interface playing cards execute the thought by using resetting the IV on every occasion the cardboard is embedded to the pc and increasing the IV by way of one for each modern message outline. within the normal interest of a far off station, the PCMCIA card is probably going toward be embedded and expelled diverse events in multi day prompting low estimations of IV vectors to be reused among the day at some thing point the cardboard is embedded inside the laptop. besides, however whilst the IV is no added amid the day it simple to discover examples of vector reuse because the vector has simply 24 bits, and for bustling position every single attainable change (224-1 precise vectors) may be applied earlier than lengthy and vectors will start to be recycled afterward to that point. Percentages of IV and thus stream key uses again moreover extended through the manner that every one stations in a machine below WEP proportion a comparable thriller key. in this manner at anything point stations in a unmarried system pick a similar IV, comparative key streams might be created and these might be utilized to select up getting to know of the mystery key. Again utilizing of IV makes WEP conference at risk of attacks paying little heed to the thriller key length.

3.3.3 Message change assaults

The (CRC-32) Cyclic Redundancy Checksum utilized by WEP toward guarantee message legitimacy isn't adequate by way of messages may be changed in-travel with out modifying the checksum esteem. The defenselessness of checksum esteem deceits in its assets that is a straight capability of message. This is for all selections of messages 'a' and 'b' we've:

$$c(a \oplus b) = c(a) \oplus c(b)$$

in which $c(a)$ demonstrates cyclic repetition checksum for message 'a'.

Aftereffect of overhead linearity assets is that the aforementioned permits the (C) cipher text designate reformed with out changing the checksum esteem and as a consequence crushing the ability of Cyclic Redundancy Checksum.

altogether the assailant has to realize in vanquishing checksum esteem is actual (C) cipher text and the (E) precise plaintext, which is picked discretionarily with the aid of the aggressor. The ideal plaintext is then utilized to figure the brand new ciphertext (C') with a view to activate every other message M' being conveyed towards the beneficiary. the brand new (C) ciphertext and message are showed there with the aid of:

$$C' = C \oplus [E, c(E)] \quad M' = M \oplus E$$

The brand new ciphertext (C') might be transmitted in preference to the (C) primary plaintext. Arranged unscrambling the plaintext P' could be a hyperlink of another message M' and any other checksum esteem b(M') with a purpose to be a proper checksum for message M'. that is tested as follows:

$$C' = C \oplus [E, c(E)]$$

$$= \text{RC4}(\text{IV}, k) \oplus [M, c(M)] \oplus [E, c(E)]$$

$$= \text{RC4}(\text{IV}, k) \oplus [M \oplus E, c(M) \oplus c(E)]$$

$$= \text{RC4}(\text{IV}, k) \oplus [M', c(M \oplus E)]$$

$$= \text{RC4}(\text{IV}, k) \oplus [M', c(M')]$$

This exhibits changes can be complete on a scrambled flag and the checksum esteem won't have the capacity to distinguish the adjustment.

3.3.4 Station Association Attacks

The assailant wanting to hook up with a remote gadget may be do as such with out the development data of commonplace thriller key. This may be practiced through the records one plaintext and this comparing ciphertext. Through the studying of plaintext and ciphertext in shape, the aggressor can without lots of a stretch infer the key utilized in getting the encoding the plaintext. Assailant may also then utilize the

manner to attach the system with the device by way of accurately scrambling the check from the get admission to point. With the facts of the ciphertext C and plaintext, P, the assailant may additionally accumulate the thriller key as under:

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

$$= RC4(IV, k)$$

In this way playing out an XOR activity in plaintext and ciphertext will empower aggressor to acquire the key that might be utilized in partner the station.

CHAPTER 4

WI-FI PROTECTED ACCESS (WPA)

To understand security blemishes knowledgeable on WEP conference, Wifi Association created Wifi Protected Access security convention. WPA remained discharged as between time solution for WEP protection defects even as an increasingly hearty association 802.11i was existence produced. Offer in opposite similarity to frameworks assisting WPA, WEP reinforced indistinguishable encryption calculation from WEP, then it obligatory simply the product change to overhaul a framework from WPA and WEP. WPA addresses protection defects experienced on WEP with the aid of offering a few new security highlights. This contain an upgraded statistics category convention called (TKIP) Temporal Key Integrity Protocol the usage of a 48 bit data format Vector and a 128 piece input in framing encryption key. WPA additionally makes use of EAP/ 802.11X affirmation conspire. except, WPA consists of Message Integrity take a look at (MIC) to make sure the transmission towards package frauds.

Table 4. 1: capabilities the actual contrasts amongst WPA and WEP safety conventions.

	WEP	WPA
Encryption	40 bit keys	128 bit keys
	Static key : Same key used by everyone in the network	Dynamic key : Keys change per user, each session, each packet
	Manual distribution of keys	distribution of keys with automatic
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication utilizing 802.11X and EAP

4.1 WPA Security Features

4.1.1 TKIP and Encryption Key control

notwithstanding utilizing an all-encompassing data format Vector and a greater prolonged key, TKIP substitutes static shared key utilized by WEP through a powerfully dispersed key. Afterward the confirmation server relates a station, a consultation among station and the serving get admission to point is set up. 802.11X conference is before castoff to create a considered one of a kind ace key in any other case known as a couple insightful key aimed at this precise consultation and disseminated to station and the get admission to factor. Ace key is complete up from t

AP and purchaser machine MAC locations then uncommon mystery variety for the session. Hash paintings is formerly connected to the ace key and an arbitrary wide variety to deliver a (TK)Temporal Key for the session. Temporal Key for the assembly will at that point be utilized to regularly create awesome facts encryption numbers for each package transmitted amid the consultation as delineated in discern. On the point when the session closes, the grasp scratch disposed of and some other master key could be appropriated for the following consultation. along those strains certainly one of a kind keys are utilized aimed at each consultation, for every client then for every package deal transmitted.

Encryption:

As with TKIP and WEP , moreover utilizes the XOR project to create the cipher text from simple content material and arbitrary stream key. TKIP makes use of a 128 (TK) fleeting key together with a 48 bits IV and the consumer gadget MAC cope with in determining the abnormal key stream. In the direction of the start of every transmission, IV is rearrange to 0 and improved with the aid of one for each package transmitted. The duration of IV (48 bits) guarantees a little IV might not be again use with the equivalent (TK), because it will yield the transmission of 248-1 parcels in a single meeting for IVs to be use again. This could take more or less 600 years at an statistics alternate exchange amount of 54Mbps .The usage of more prolonged IV and a worldly key disposes of one of the sizeable blemishes of WEP protection convention. TKIP creates the arbitrary stream key with the aid of blending keys on two stages. mixing is finished utilizing (Sboxes) substitution bins in which a m bit input movement is modified hooked on n bit yield move utilising look-into tables. within the foremost level, the TK is mixed with the purchaser's MAC cope with and initial four bytes of IV to acquire an (ITK) Intermediate Temporal Key(ITK).stream key. The motive for the second section of key blending is to evacuate any relationship among the IV and the important thing nourished to the RC4 calculation and alongside those traces keeping the utilization of powerless key to recuperate (TK). Afterward the stream key is produced making use of RC4 calculation, plaintext is gotten by using XORing the streamkey with the plaintext. Figure 5: gives a linguistic creation of key mixing and encryption forms performed by (TKIP). The utilization of powerfully disseminated key additionally expels the

necessities to physically trade the keys for all passageways and flexible station, procedure this is critical once a difference in WEP static keys is essential.

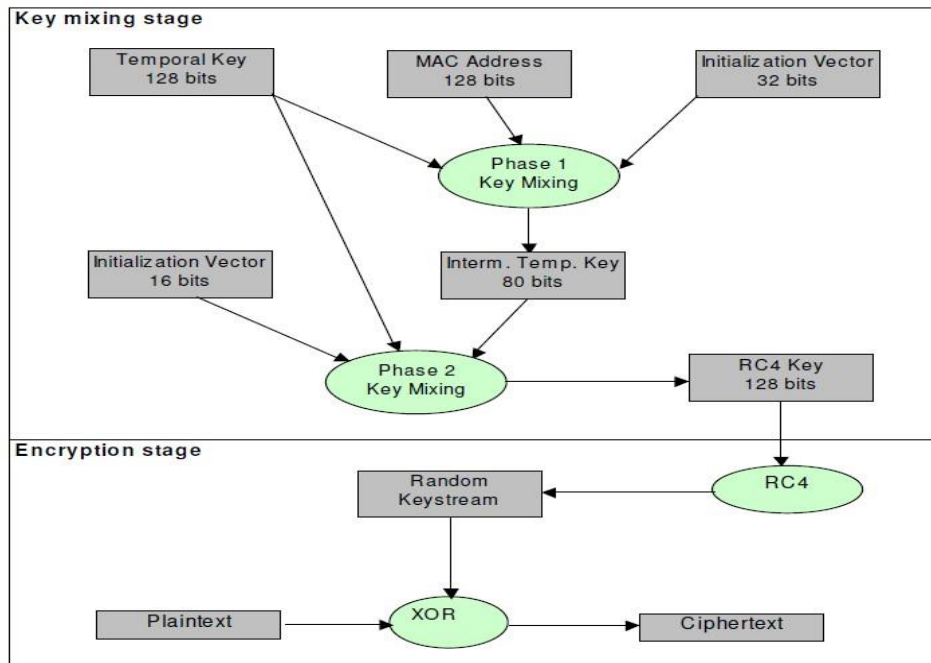


Figure 4. 1: TKIP mixing and encryption stag

4.1.2 Authentic and MIC

WPA makes use of IEEE 802.11X authentication with one of (EAP) Extensible Authentication Protocols handy. 802.11X is a port based device manage get to convention that may be utilized each in stressed and far off LAN. IEEE acquired 802.11X like a preferred in 2001. Through 802.11X consumer's accreditations are displayed as automatic endorsements and that they can be based on usernames, customer passwords, savvy cards or anything different superior personality that the gadget head will get a kick out of the threat to utilize. collectively with EAP, 802.11X empowers shared verification of stations through the validation server. This maintains the probability of a customer station partner with a rebel passageway. This case is a chance below WEP where in there is no common validation and simply customer stations are established earlier than making courting with any passageway inside the gadget. on the factor while clients demands affiliation, the client's accreditations might be sent to the Authentication server thru the passageway. at the off threat that the Authentication server approves the client, TKIP will produce an ace key with the intention to be sent to the customer and the passage. to complete the affirmation process, a four-manner handshake will arise between the AP and the client.

Message Integrity take a look at : WPA presented as a methods for making certain that parcels aren't modified or long-established amid transmission. At the off danger that the message honesty is endangered, the error should be prominent and the altered edges are to remain disposed of. MIC become meant to conflict the imperfections skilled in the usage of CRC substantiation utilized in WEP protection conference. MIC is figured utilizing a cryptographic calculation called Michael. Michael utilizes a 64 bit key and a message of self-assertive period to create a 64 bit MIC esteem, that is cushioned in the direction of the end of the 802.11 edges. Message our bodies collectively with the figured 64 bit MIC esteem are scrambled utilizing RC4 movement determine and transmitted to the beneficiary. The collector will deduct the MIC esteem from message frame and evaluation the final results and the esteem that observed the message. The collector will acknowledge the message if two features coordinate, usually the returned rub will be rejected.

Given a message, Michael calculation cushions the end of a message with 1 byte of hexadecimal esteem 5a and diverse zeros to make overall length of cushioned message distinct into gatherings of 4-bytes. finally, a blending potential actualizing turns, bit swap and EXOR obligations is attached to each amassing of 4 bytes and key to create a 64 bit association that serves as substantiation of the parcel.

MIC calculations may be delineated utilizing the rearranged pseudo code demonstrated as follows. K0 and K1 communicate to two gatherings of 32 bits each received by using separating the thriller MIC key. M0, M1, ... MN - 1 remain N gatherings of 32 bits got from the cushioned message. V0, V1 are the 2 gatherings if 32 bits make up the remaining MIC esteem. capacity 'b' is unkeyed 4round Feistel shape utilized to change, turn and EXOR gatherings of 32-bits.

Procedure Michael((K0,K1),(M0,M1,...,MN-1)) *Input:MIC Key(K0,K1);Padded Message(M0,...,MN-1) Output:MIC Value(V0,V1)*
(l,r)←(K0,K1)
for i=0toN-1 do l←l ⊕Mi (l,r)←b(l,r) return(l,r)

Procedure $b(l,r)$ $r \leftarrow r \oplus (l \div 17)$ $l \leftarrow (l+r) \bmod 232$ $r \leftarrow r \oplus XSWAP(l)$ $l \leftarrow (l+r) \bmod 232$
 $r \leftarrow r \oplus (l \div 3)$ $l \leftarrow (l+r) \bmod 232$ $r \leftarrow r \oplus (l \div 2)$ $l \leftarrow (l+r) \bmod 232$ *return* (l,r)

Weaknesses: 802.11 (NIC) Network Interface Cards and Admission Points do Michael calculations. This gadgets have low computing power, which is prompted the structure of calculation through low calculation overhead to decrease the framework delay. Weakness of this approach was that the protection existing by Michael in contradiction of message phony was debilitated. regardless of the fact that the substantiation esteem is produced from 64-bits, it may deliver simply 220 wonderful checksum esteems. anyway it has been tested that trustworthiness test estimations of up to 229 special qualities are defenseless to cryptographic assaults. every other shortcoming of Michael calculation is the mixing ability is unkeyed Feistel shape. A Feistel shape is a cryptographic shape utilized in diverse rectangular figures, for example, Feistel parent and DES. With shape a rectangular of records to be is separated hooked on 2 parts (proven by way of 'l' and 'r' within the pseudo-code under). various rehashed sports, as an example, bit revolutions and byte swap are then related to 1 half and the outcome is EXORed with the alternative half. Fashionable Michael calculation the Feistel figure has 4 EXOR obligations and is in this manner referred to as a 4 round Feistel shape.

because the Feistel shape applied on Michael calculation does now not rely upon any key, it may eventually be altered . making use of the MIC esteem, the mixing capability can be related backward request to touch base on the MIC enter as seemed in the pseudo-code below

Procedure $InvMichael((K0,K1),(M0,M1, \dots, MN-1))$ *Input:* MIC $Key(V0,V1); Padded$
 $Message(M0, \dots, MN-1)$

Output: MIC Value(K0,K1) (l,r)←(V0,V1)
for i=N-1 down to 0 do (l,r)←b-1(l,r)
l←l ⊕ Mi return(l,r) Procedure b-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)

4.1.3 802.11X

IEEE 802.11X is a preferred that characterizes the instrument for port-primarily based system get to manipulate. It gives a device to validate and approve gadgets expecting to get to t WLAN. 802.11X relies upon on EAP to offer get to govern, simple key administration , verification. In fee of activity of the calculations and conventions associated with confirmation aspect before the applicant is showed, the skillful port could be open and 802.11X fashionable characterizes the manner on which validation messages will be advised thru various framework segments even though the real affirmation messages directed will depend upon an specific EAP verification element applied. on the stop of the day, the 802.11X is honestly the automobile for verification messages. This route of movement lets in converting of verification usage with out the AP being discerning of the exchange. numerous usage of EAP conventions can be utilized; these contain (EAP-TLS) EAP shipping Layer protection, (EAP-MD5) EAP Message Digest 5, (EAP-TTLS) EAP — Tunneled shipping Layer protection and (PEAP) guarded Extensible Authentication Protocol. The 802.11X confirmation framework is made out of to a incredible quantity three noteworthy parts: the supplicant, the authenticator and the verification server. The supplicant is generally

the flexible station like a Pc or PDA that expects access to device. The authenticator is generally the machine AP whose purpose at validation arrange is toward get confirmation messages from applicant and pass it to the verification server within the essential configuration. The closing segment is the validation server, additionally called configuration, approval , bookkeeping (AAA) server. this is typically a radius server, albeit one of a kind types of servers like Diameter server may be applied. The term port in the 802.11X speaks to relationship among the authenticator and the supplicant. supplicant won't have the ability to get to any of system's administrations. all of the verification messages among the supplicant and validation server will go through unrestrained port. while verification server acknowledges the character of the supplicant, it will endorse the authenticator of fulfillment of interest and key records can be passed to applicant. The controlled port will at that factor be shut and the gadget administrations may be available to the applicant. The 802.11X additionally characterizes the exemplification of (EAPOL) EAP messages over LAN to be applied in message trades between the authenticator and the supplicant .

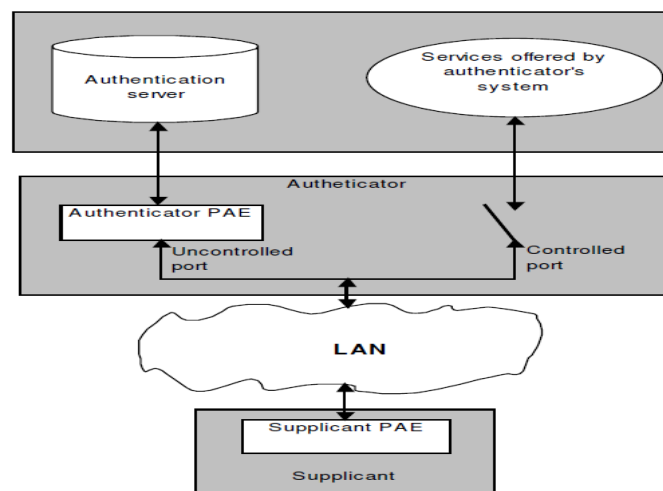


Figure 4. 2 : Components of 802.11X system

Message-flow during authentication manner:

The affirmation system start when the applicant sent the validation ask for (EAPOL start) to the authentication. The authenticator would be react (EAP ask for) via asking for that the applicant give its identity. In this degree every single other message from the supplicant are blocked .The patron machine cannot get to any administration in the

system. Within the third section of the method, the supplicant sends the EAP reaction message, which contains its recognizable evidence to the confirmation server. The validation server at that factor makes use of the actualized verification calculation like secret phrase, sensible card, username, and so forth to confirm the persona of the supplicant. The server will at that factor ship EAP success or EAP unhappiness message to supplicant depending upon end result of the affirmation. within the occasion that the validation was a win, the controlled port might be close and the supplicant will at that factor have the ability to get to the system administrations. Following determine delineates the message movement among the authenticator, supplicant and the confirmation server amid verification procedure.

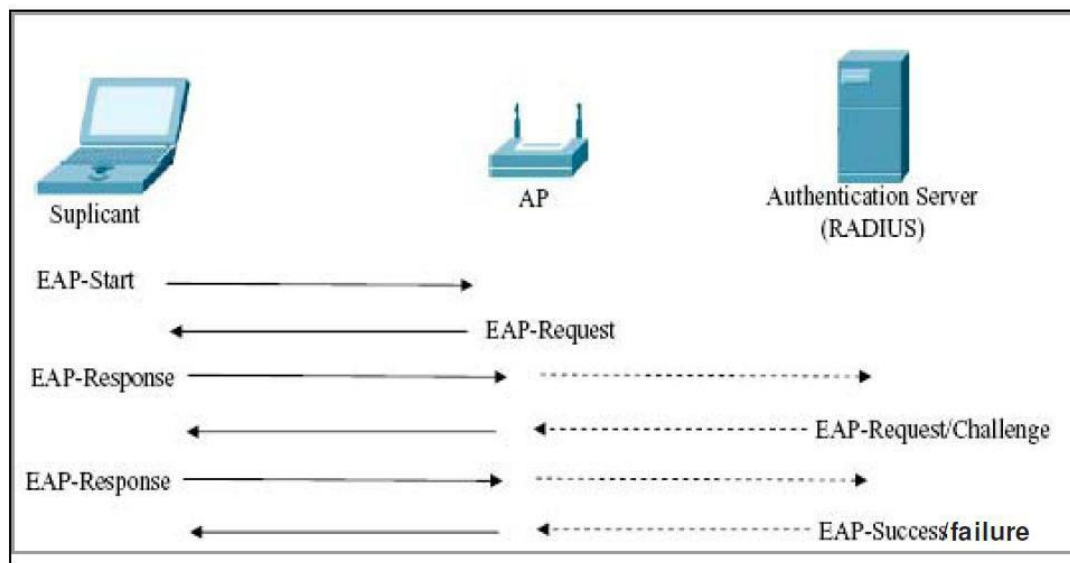


Figure 4. 3: Message flow during authentication process

Weaknesses: Numerous powerful attacks may be propelled at the 802.11X confirmation and get right of entry to manage conference. Refusal of administration, consultation shooting and guy-in-the-middle assaults might all be capable of be propelled on a 802.eleven system executing 802.11X affirmation conference. at the factor while the supplicant has not noted to confirm and has gotten an EAP unhappiness message, this should sit down tight for 60 seconds before sending other verification message. A gatecrasher wishing to dispatch a DoS attack can misuse this system through caricaturing the EAP sadness message and sending it to supplicant like clockwork. On accepting this message, the supplicant will assume that it originates from an proper AP and it'll sit down tight for 60 second before sending other confirmation demand to which every other verification sadness message may be

sent from a rebel machine. some other DoS assault can be propelled through continuously sending EAP start messages to authenticator. The authenticator will be over-burden with verification dourse from a maverick device and it's going to forget to deal with real site visitors. DoS attack can likewise be propelled through means of mocking proper supplicant's MAC cope with and sending the logoff call for to the serving AP (EAP Logoff). AP will expect the demand originates from the real gadget and it'll disassociate the machine. 802.11X validation conference offer just a single way confirmation just supplicant is related with suspicion that authenticator is a confided in substance in the device. An enemy wishing to dispatch a man-in-the- center attack can abuse this supposition by using going approximately as an AP and the accepting all facts visitors from the authenticator. To keep this type of assault, commonplace confirmation between the authenticator and the supplicant is critical.

4.2 WPA-Personal

WiFi Protected Access convention may be actualized in two modes: the main mode and the one is talked about so far in this part is known as a WPA Enterprise. These mode utilizes the utilization of the 802.1X confirmation convention and verification server. Because of mind-boggling expense and convoluted design of validation servers, WPA-Enterprise execution of WPA convention isn't proper for little home and office employments. Its prompted second method of WPA usage known WPA individual. WPA Personal uses a (PSK) Pre Shared Key, which is comprised of a pass expression whose distance extend from 8 to 63 ASCII characters and 64 hexadecimal digits like 256 bits. In the event that ASCII character is picked, hash work is utilized to lessen the quantity of bit from 504 bits got from 63 characters to 256 bits. PSK is entered in WLAN gadgets in the system and after gadget is validated, The TKIP will utilize the PSK, Service Set Identity and nonces to create the (PMK) Pair wise Master Keythat will be utilized to create information encryption enters as talked about in area TKIP and Encryption Key Management. Along these lines the fundamental distinction between the two methods of activity is that with WPA Enterprise the validation server produces the PMK though with the WPA Personal, the PMK is created from the pass expression. Despite the fact that TKIP guarantees that encryption keys for WPA Personal are frequently transformed, it has been demonstrated that security offered by this usage of WPA generally depends on the length of the pass expression utilized as the (PSK)Pre Shared Key.Pass expression

that is under twenty characters in length is defenseless to lexicon assaults. Utilization of one pass express for all gadgets in the Extended Service Set (ESS) builds the harm the aggressor can do to the system, since in the wake of getting hold of PSK, the assailant can peruse and adjust any traffic in the ESS. Accordingly to guarantee legitimate dimension of security for WPA Personal usage, long pass expressions ought to be utilized.

CHAPTER 5

802.11i SECURITY PROTOCOL

It is most recent WLAN security normal confirmed through IEEE in 2004, June. The 802.11i is otherwise called WPA2 meanwhile WPA depended on underlying draft of the 802.11i. In this manner numerous security highlights found in the WPA are additionally accessible in 802.11i including TKIP and Michael calculation. Anyway the 802.11i utilizations upgraded encryption, confirmation key administration conventions this give improved security to WLAN.

The 802.11i details characterizes 2 classes of security calculations:

1. (RSNA) Robust Security Network Association: It gives TKIP and counter mode or CBC-MAC convention as information classification conventions. It additionally gives the 4-way handshake verification methodology, the 802.11X confirmation and the key administration conventions.
2. (Pre-RSNA) Pre-Robust Security Network Association: The data secrecy here is given through WEP and here have no 4-way handshake. Execution of PreRSNA is important to make the 802.11i in reverse perfect. Task of other Pre-RSNA and WEP natives are examined in past parts and won't be shrouded in this section.

5.1 Data Confidentiality and Integrity

The 802.11i standard characterizes 2 information secrecy conventions under RSNA security calculation: CCMP and TKIP. Since the TKIP has been talked about on the past parts, it area will keep its discourse happening CCMP.

(CCMP) convention generates encryption of remote information then parcel validation. For the encryption, CCMP utilizes (AES) Advanced Encryption Standard in the hostage mode rather than RC4 utilized in TKIP and WEP conventions. AES is progressively secure normal and is affirmed by (FIPS) Federal Information Processing Standard. The (CBC-MAC) Cipher Chain Blocking Message Authentication Code gives parcel confirmation rather than Michael utilized in WPA convention.

AES calculation is a symmetric square figure equipped for utilizing cryptographic keys of 128, 192, 256 bit to encode and unscramble information in squares of 128 bits. The counter mode through CBC-MAC activity of AES calculation utilizes 128 bits figure keys making it protected in contradiction of savage power assaults. AES permits the utilization of one encryption enter in encoding of all bundles, which disposes of the issues related through key booking and key circulation as in TKIP and WEP conventions.

The (MIC) Message Integrity Check is given to the casing body and also the decoded MAC header, which keeps aggressors from ridiculing source and goal MAC locations. Utilizing it in propelling assaults. Besides (CCMP) utilizes a 48bit parcel number, which is augmented each time a bundle transmitted. It averts bundle replay assaults like any redundancy of (PN) parcel number will be note down and parcel will be disposed of. Length of a PN field 48 bit guarantees it a specific bundle number won't be use again in any affiliation. The CBC-MAC is 8 bytes, the nonce and 2 bytes of the 802.11 overheads make measure of CCMP parcel to be 16 byte bigger than the decoded the 802.11 bundle. CCMP to a great extent takes out the danger of uninvolved spying and traffic examination since in spite of the fact that the assailant can listen stealthily on the traffic however this will be hard to decode the bundles as there are no real method to find the (TK) Temporal Key utilized for the encryption. Anyway meanwhile the MAC header isn't encoded, the interloper can pick up learning of the bundle size and recurrence of transmission. Luckily, learning of the data can't prompt any assault that can bargain the classification of information.

5.2 Authentication and Key management

The 802.11i EAPOL-key alternate uses some of keys and has key hierarchies that divide up initial keys into beneficial keys. the two key hierarchies are: four-way handshake and group key handshake.

4-route handshake: For 4-way handshake the beginning stage is a (PMK) Pair-wise Master Key. In the event that the 802.11i executes the 802.11X, the PMK would originate from the confirmation server and when Pre-Shared key (PSK) is utilized, 802.11i will outline secret phrase to the PMK. PMK will at that point be a

contribution to a pseudorandom work, together with the nonces and the MAC addresses from each the AP and the customer system to get the (PTK)Pair-wise brief Key. PTK will at that factor be partitioned to 3 keys. The most important secret is the EAPOL (KCK) Key confirmation Key, that's applied in EAPOL key trades to present statistics starting genuineness. the second one key is EAPOL (KCK) Key Encryption Key, which is applied in EAPOL key trades to offer type. The final key got from PTK is Temporal Key, which is utilized for statistics type.

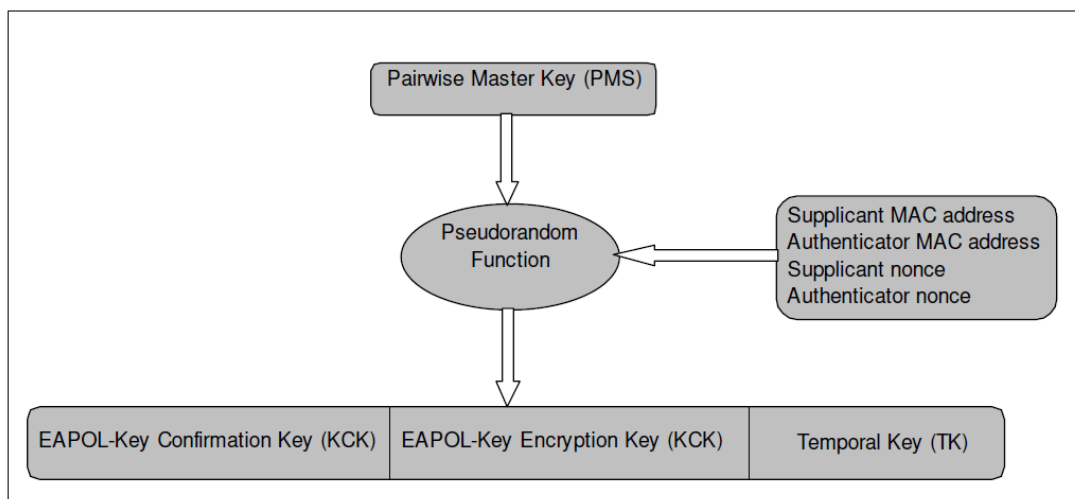


Figure 5. 1: Key generation for 4 way handshake operation

Gathering Key Hierarchy: Beginning stage for gathering key chain of commands an irregular number called the (GMK) Group Master Key. At that point authenticator MAC address, authenticator nonce and GMK is contribution to an irregular capacity to create the Group Temporal Key (GTK).As talked about above, IEEE 802.11i characterizes RSNA methodology that accommodate shared verification and key administration convention that guarantees new Temporal Keys are produced to guarantee information privacy. Given Figure portrays the messages traded between and condition of the verification server, authenticator and the supplicant amid RSNA foundation Process.

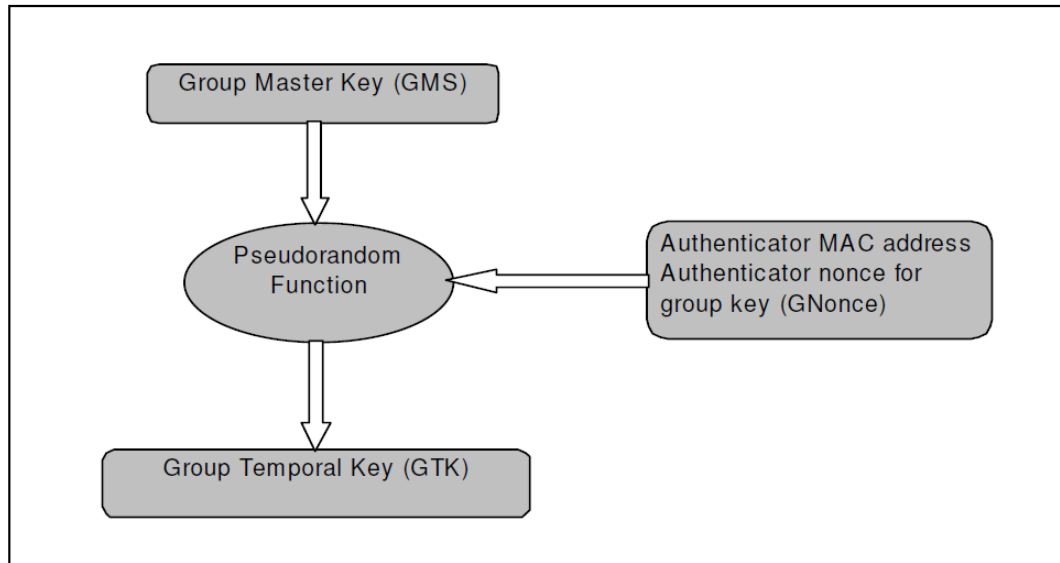


Figure 5. 2: Key generation for group key hierarchy

stage 1: community and protection capability Discovery

This level is in any other case called arrangement arrange like the supplicant and the authenticator make use of this phase to envisage to the safety convention to be applied of their correspondence. Stage contains of messages numbered (1) to (2). since the 802.11i accommodates three statistics privacy conventions: TKIP , CCMP and WEP there have to be a course for a consumer system and the AP to concur on which conference to make use of. customer devices additionally utilize this convention transaction level to locate different safety highlights legal by means of the AP.AP communicates its safety highlights, established via robust protection community information element (RSN IE) at the reference factors it sends continuously. It could likewise supply its safety includes as a response to a check ask for from a supplicant with a Probe reaction define. A part of the safety parameters that AP communicates are the rundown of all facts secrecy conventions that it bolsters in unicast correspondence, the records privacy conference applied in communicate correspondence (this may's be arranged) and whether or not the (PSK) Pre-Shared key or the 802.11X is utilized.

stage 2: 802.11 Authentication and affiliation

The level contains of messages numbered (4) to (7). Subsequently the consumer machine realizes parameters upheld by using the AP it at that factor sends the partner

ask for distinguishing the security include it needs to utilize. It is message (8) (SPA RSN IE +affiliation Request).The safety highlight picked by the patron device have to be incorporated into the rundown of upheld includes generally the affiliation will arise quick. Subsequently the supplicant receives the association reaction (message 7) the 2 gadgets (supplicant and authenticator) will be in association and affirmation kingdom but 802.11X port determination stay blocked and there have no statistics parcels may be traded. Messages (4) and (6) are applied in the 802.11 Open system Authentication and are incorporated to allow in reverse similarity.

Stage3 : EAP/802.11X/RADIUS Authentication

The level includes messages range (8) to (14). In this level the applicant and the verification server effect shared validation. Authenticator is going approximately like the hand-off point for messages from server to supplicant. Authenticator likewise embodies the messages inside the required organization before conveying them to anticipated goal. After supplicant and verification server has demonstrated every different an average thriller key called the(MSK) master consultation Key might be shared among the devices. The supplicant will at that factor make use of the MSK to create the (PMK) Pair-wise master Key. affirmation highlights will likewise be handed to the authenticator via message (15) to empower it to supply PMK.

Stage 4: 4-Way handshake

A 4 route handshake as characterized with the aid of the IEEE 802.11i plays out a few capacities including declaring the PMK between the authenticator and the supplicant, building up the transient keys to be used by the records secrecy conventions and verifying safety parameters consented to among the authenticator the supplicant . Amid 4 route handshake system four messages(16) through message (19) are traded among the authenticator and the supplicant:

Message 16: on the message, authenticator sends a nonce to supplicant. This nonce is known as A Nonce. At this degree supplicant makes its very very own nonce called SNonce and computes the PTK.

Message 17: inside the second 4-manner handshake message supplicant sends SNonce into authenticator. Supplicant likewise sends protection parameters utilized amid affiliation the (SPA RSN IE). A affirmation check can be linked at the were

given message making use of KCK. Now authenticator can test the legitimacy of protection parameters applied amid affiliation and determine a new (PTK) Pair-wise temporary Key to be utilized within accompanying records session. If there have to be an incidence of gathering correspondence, the institution brief secret's created after the authenticator gets this message.

Message 18: inside this third 4-manner handshake message, authenticator sends to supplicant the safety highlight its communicates in this reference factors the (AA RSN IE). Authenticator additionally sends the Group Transient Key scrambled utilising KEK. Complete message will get affirmation test on the supplicant to verify that authenticators security parameters are sizeable and like those applied at affiliation.

Message 19: Fourth message demonstrates that the worldly keys, GTK and PTK are currently shared among supplicant and authenticator and are set up to be utilized for facts category functions. The 802.11X ports can be unblocked and supplicant can get to administrations provided through the authenticator.

stage 5: organization Key Handshake on this stage is simply applicable amid multicast programs. The (GTK) accumulating transient key is conveyed to the supplicants on this degree.

stage 6: at ease information communication using the GTK or PTK and arranged protection convention, supplicant and authenticator will expand a covered correspondence channel into transmit information bundles.

5.3 Analysis of Security Offered by IEEE 802.11i

In IEEE the 802.11i was intended to battle of all the security defects experienced in WPA and WEP conventions. It was practiced in substantial part and the 802.11i offers preferable security ended all the past conventions. The following is an investigation of the vigor of security offered by the 802.11i to basic remote dangers.

5.3.1 Eavesdropping, Traffic Analysis and Message Injection

This is as yet workable for a foe to the snort and the store every one of the information traffic in the 802.11i ensured WLAN. Anyway because of the utilization of (TK) Temporal Keys, the foe won't have the capacity to unscramble the information. Hence the negligible spying of information won't trade off information

secrecy and traffic examination can't be completed. The executives outlines anyway represents another issue, like they are not secured by the TK encryption. The assailant accordingly can snort messages imparted between customer gadget and AP amid security capacity disclosure stage and affiliation phase of the RSNA foundation system .Assailant would then be able to utilize the sniffed security abilities and send them to the customer gadget driving the gadget to connect with rebel AP or utilize improper security limits in partner with genuine AP. In any case, common verification and 4 route handshake as executed is previous of RSNA foundation system will evacuate the dangers presented by assailant snorting the board outlines.

5.3.2 Session Hijacking

This assault is propelled after a customer gadget has finished validating itself and hence can't be secured against by solid confirmation system. To dispatch this assault, a foe can manufacture dissociate the message then send it to customer gadget. Then the genuine gadget is disassociate the rebel gadget will assume control ended the session and the proceed with correspondence with serving AP. On the off chance that the rebel gadget will just get information from AP, TK executed by the 802.11i will keep maverick gadget from decoding the information and no damage will be caused on information classification. Maverick gadget can't likewise sent traffic to AP, as it won't have information of (PTK) Pair-wise Transient Key required for production of adequate traffic.

5.3.3 Man-in-the-Middle

Toward dispatch an effective Man in the center assault, interloper require first to break relationship between customer gadget and the AP. For done this, the interloper can send devalidation message to genuine gadget and verify rebel gadget with the AP. Real gadget will begin sending tests searching for another and aggressor will connect the maverick gadget with real gadget. In this way the assailant's gadget will go about as an AP to the customer gadget and a supplicant to the authentic gadget. Anyway when a solid shared validation instrument as a EAP-TLS is actualized with the 802.11i the maverick gadget won't have the capacity to confirm itself with the genuine AP. Feeble common confirmation conventions can prompt a fruitful man in the center assault.

5.3.4 Security Level Rollback Attack

The 802.11i accommodates 2 classes of security components:

- (1) RSNA
- (2) Pre-RSNA.

The Pre-RSNA is actualized toward give in reverse similarity when the 802.11i is conveyed in circumstances in which there is heritage gadgets that just help the WEP security convention. Additionally for provide food for usage of the 802.11i wherever there have numerous supplicants, approximately through heritage gadgets, standard characterizes the (TSN) Transient Security Network that underpins both RSNA and Pre-RSNA calculations. The supplicant may be designed to help the two calculations to permit relationship with any AP inside the serving range paying little mind to the calculation. The AP can likewise be designed like TSN to give administrations to however many supplicants like could be expected under the circumstances in the system. The TSN permits the security rollback assault to propelled against system. To dispatch this assault, the enemy can imitate supplicant and send the Associate Request messages to genuine AP prosecuting that just Pre-RSNA calculation is upheld. Then again, the assailant can mimic the AP and send reference points to the supplicant demonstrating that just is Pre-RSNA security highlights is bolstered. This empower the assailant to build up the Pre-RSNA relationship with real gadget. Aggressor would then be able to abuse the shortcomings of WEP convention to totally weaken the security of the system. The answer for those security danger relies upon the dimension of security the system overseer and clients need. At the point when organize security is of most extreme significance, the arrangement is to design the supplicants and the authenticator so just the RSNA calculation is permitted in the system. Drawback of this arrangement is that organize access will accessible just to those gadgets that help the RSNA calculation.

5.4 Comparison of security features of different protocols

We can see the comparison of security features of different protocols below.

Table 5. 1: Comparison of security protocols

Security Protocol	WEP	WPA -TKIP	802.11i -CCMP
Encryption key size	40 bits	128 bits for encryption 68 bits for authentication	128 bits
Encryption algorithm	RC4	RC4	AES
Key management	Not available	802.1X/EAP	802.1X/EAP
IV size	24 bits	48 bits	48 bits
Message Integrity	CRC-32	Michael	CCM
Per packet key	IV concatenation	Mixing function	Not required

CHAPTER 6

SIMULATION AND ANALYSIS

6.1 Results Analysis

To understand practically how wifi security protocol like WPA and WEP perform in really following processes have been carried out with 8, 10, 12 nodes . All other factors have been remain same f both protocols are executed and Also when numbers of nodes in wireless LAN are considered as 8, the variation can be plotted as shown. Finally, a network comprising of 10 nodes is measured using WEP as a security algorithm. Total simulation time taken is 22 and 32 seconds and all nodes are wirelessly connected to each other. The variation is plotted as given where it is noticed that the throughput increases gradually after 12-16 seconds of simulation. The results have been computed for WPA security algorithm, paying different number of nodes. The results obtained are plotted using X-graph as frame rate and Y-graph as authentication delay. results demonstration the variation in throughput when this situation comprises of 10 numbers of nodes. In this case WEP and WPA is same to each other there have some different with 802.11i. In this simulation here three routing protocols are used and which routing protocol is suitable and best for this situation and we take the same parameters for all the routi protocols. We find out the suitable routing protocol for wifi security protocol. Then we concentarte about the performance of all routing protocols like WEP, WPA,802.11i which provided by the IEEE standard form. Then we investigate by comparing the Simulation End2End delay in seconds, lost and then comparing with output. we concentrate WEP vs WPA ,WEP vs 802.11i,WPA vs 802.11i delay .Then we concentrate WEP vs WPA ,WEP vs 802.11i,WPA vs 802.11i lost. we concentrate WEP,WPA,802.11i Output and compare with each other. After compared it has been determined 802.11i offers good security of whole conventions there are motionless a few assaults it can be effectively propelled opposite the 802.11i-anchored arrange. The decision of an appropriate security convention in this manner, tought to be founded on the significance of information being transmitted in the system. It is more standard and suitable to provide security for wifi .So, we can say that who uses wifi system they can use 802.11i routing protocol which is more secure then others.

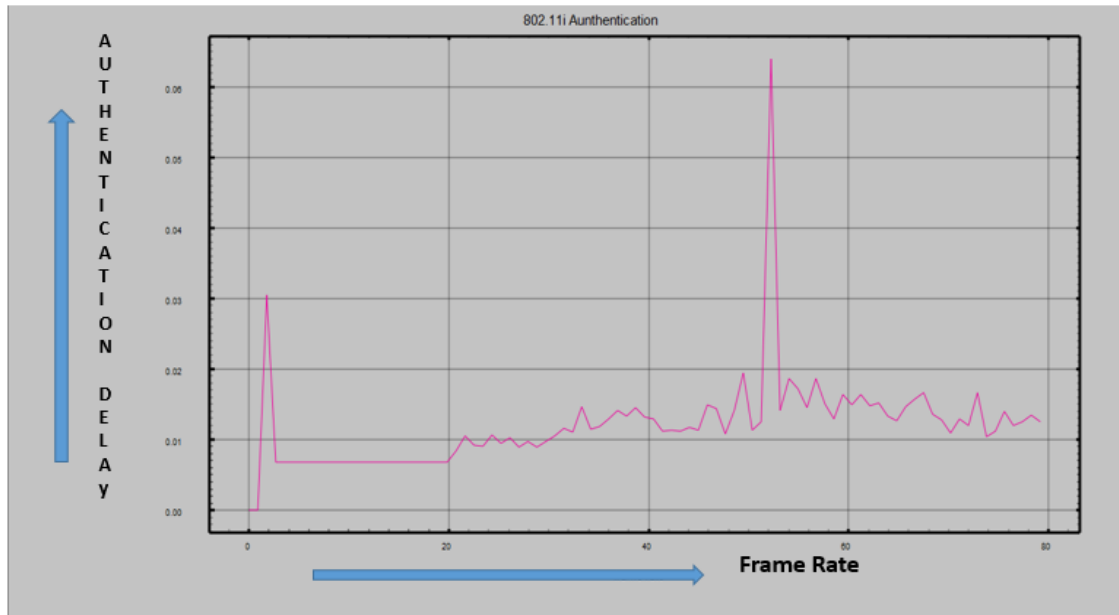


Figure 6. 1: 802.11i delay Authentication

Fig 6.1 showed that authentication delay vs frame rate for 802.11i protocol. In this simulation the highest delay is found in 45-50ms

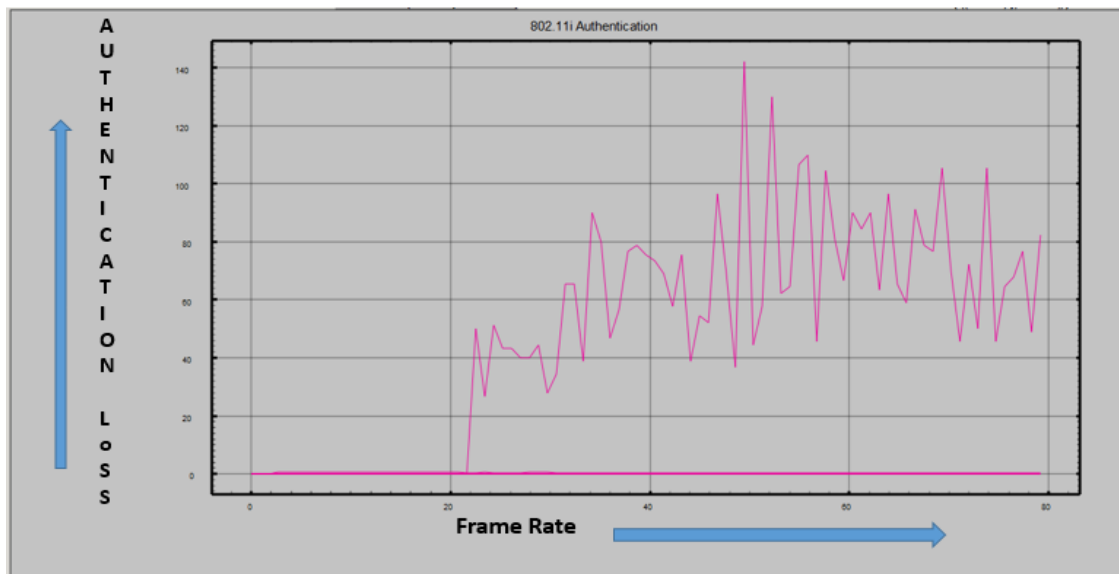


Figure 6. 2: 802.11i Authentication loss

Fig 6.2 showed That Authentication loss VS Frame rate for 802.11i protocol. In this simulation 0-30 there have no loss, after the highest loss is found in 45-50 ms.

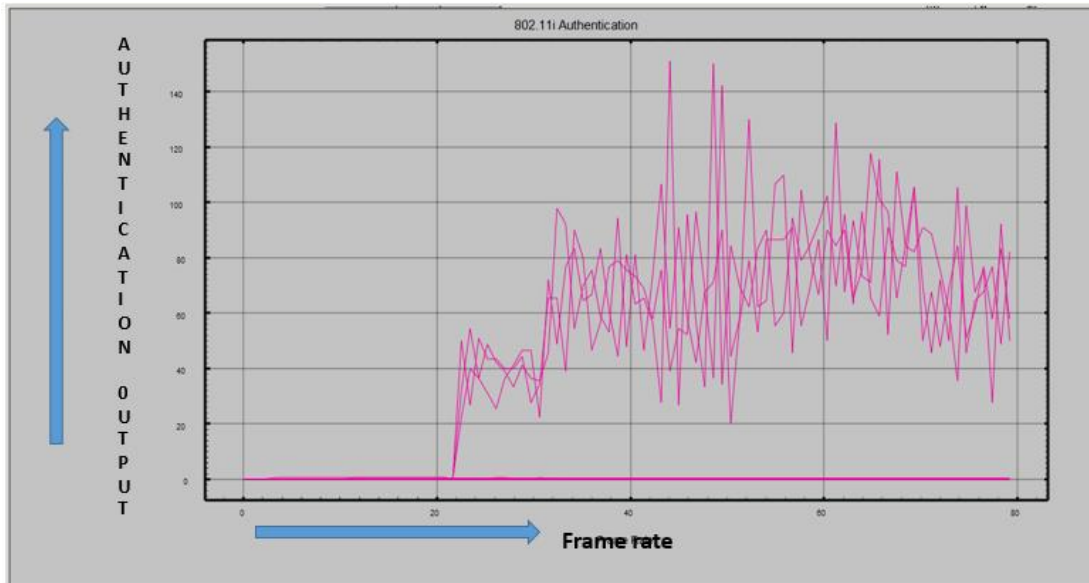


Figure 6. 3: 802.11i Shared Key Authentication output

Fig 6.3 showed That Authentication output VS Frame rate for 802.11i protocol. In this simulation 0-25 there have no output but it increased 45ms & the highest output is found in 55-80 ms

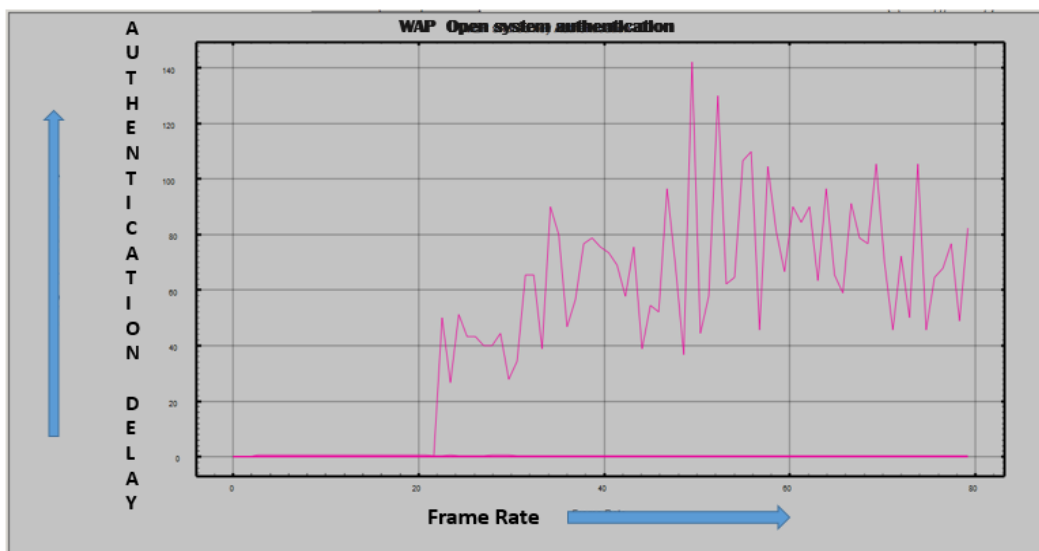


Figure 6. 4: WPA delay Authentication

Fig 6.4 showed That Authentication delay VS Frame rate. In this simulation 0-20 there have no delay but 22-80ms it increase continuously there have highest authentication delay

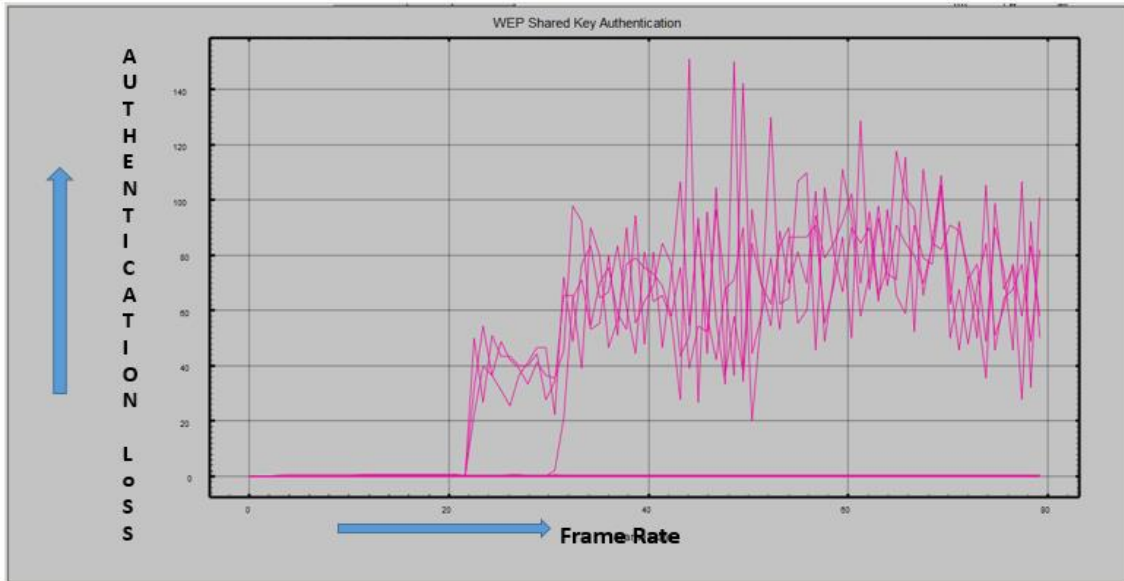


Figure 6. 5: WPA Open System Authentication loss

Fig 6.5 showed That Authentication loss VS Frame rate. In this simulation 0-20 ms there have no loss but 22-80 ms its increased ups and down.

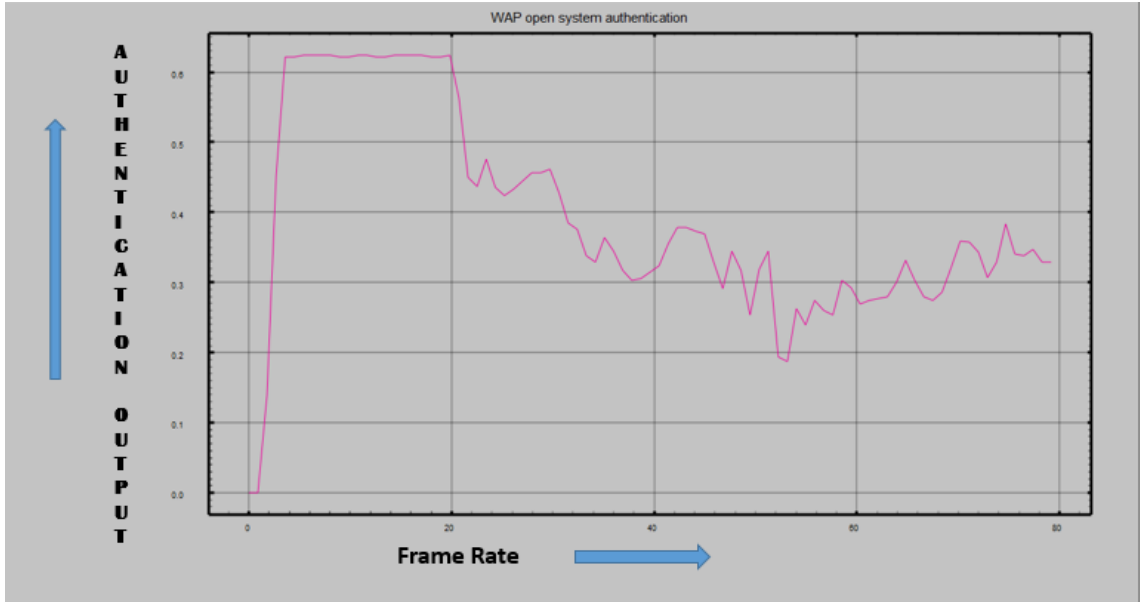


Figure 6. 6: WPA Shared Key Authentication output

Fig 6.6 showed That Authentication output VS Frame rate. In this simulation the highest output is found in 10-20ms but the output decreased continuously when the frame rate is increased.

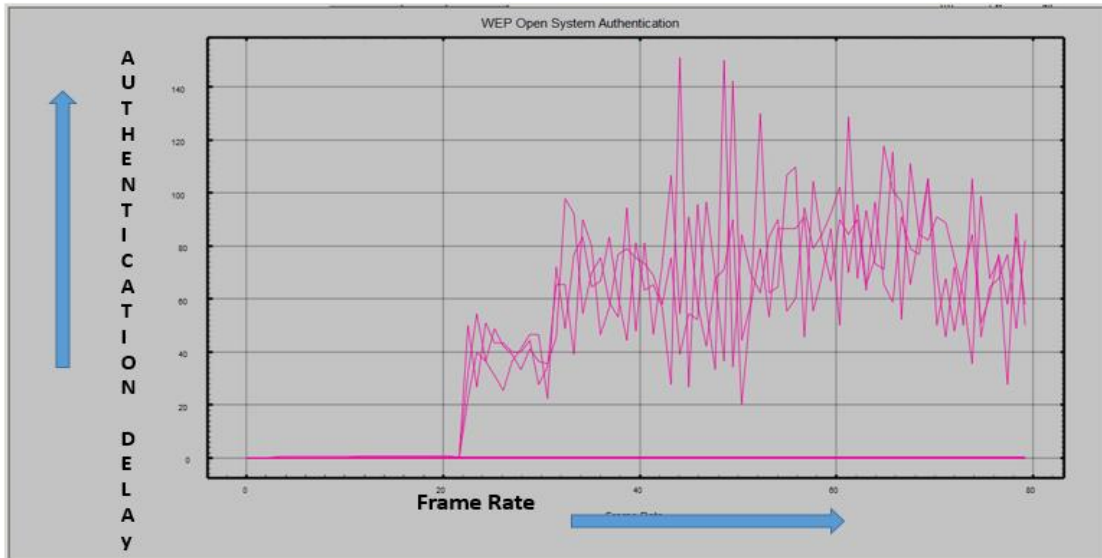


Figure 6. 7: WEP delay Authentication

Fig 6.7 showed That Authentication delay VS Frame rate. In this simulation 0 to 25 ms there have no delay but 22-78 it is increased.

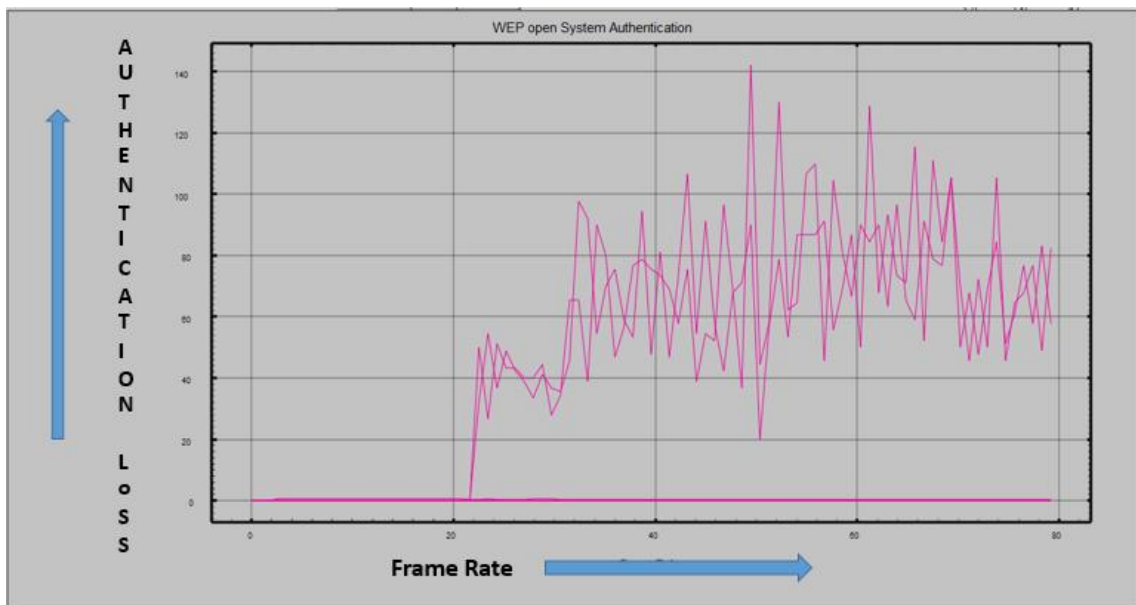


Figure 6. 8: WEP Open System Authentication loss

Fig 6.8 showed That Authentication loss VS Frame rate. In this simulation 0-20 there have no loss, after 22-80ms it is increased.

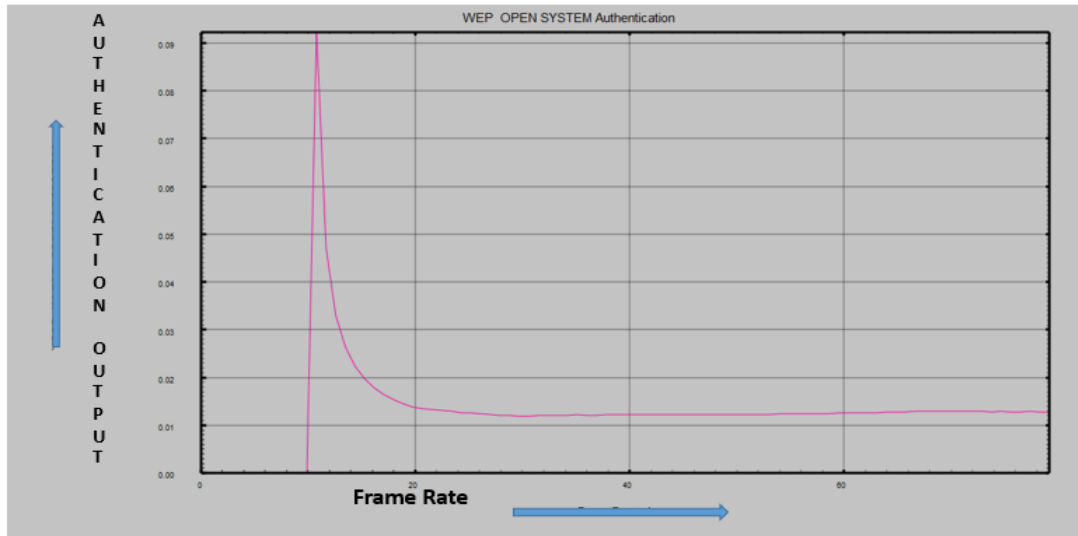


Figure 6. 9: WEP Shared key Authentication output

Fig 6.9 showed That Authentication output VS Frame rate. In this simulation the highest output is found in 10-20ms but the output is decreased continuously when the frame rate is increased.

CHAPTER 7

PERFORMANCE ANALYSIS

The routing protocols that we consider for analysis is WEP, WPA and 802.11i . which is individual use for secure routing protocol and create a good relationship with a large amount of user.

7.1 Performance of routing protocols

After simulation the performance of considered routing protocols (WEP, WPA and 802.11i) are given below:

7.1.1 802.11i Authentication Delay vs WPA Delay

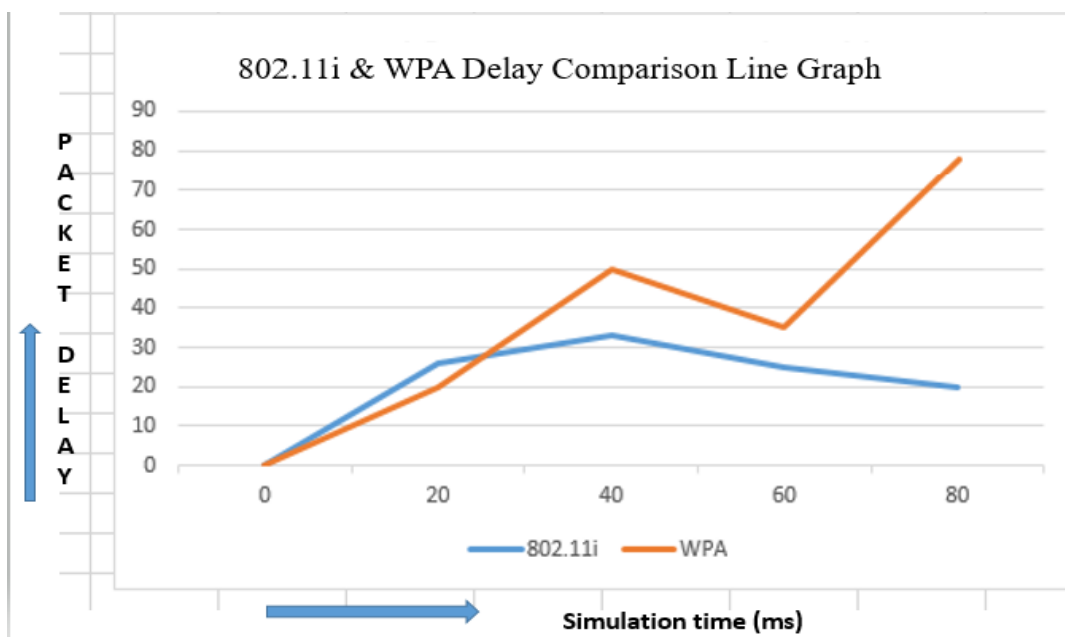


Figure 7. 1: 802.11i Authentication Delay vs WPA Delay

Fig 7.1 shows line graph where vertical axis is packet delay and horizontal axis is simulation time and showed about 802.11 delay VS WPA delay. In this fig of 802.11i delay is lower than WPA.

7.1.2 WEP Authentication Delay vs 802.11i Authentication Delay

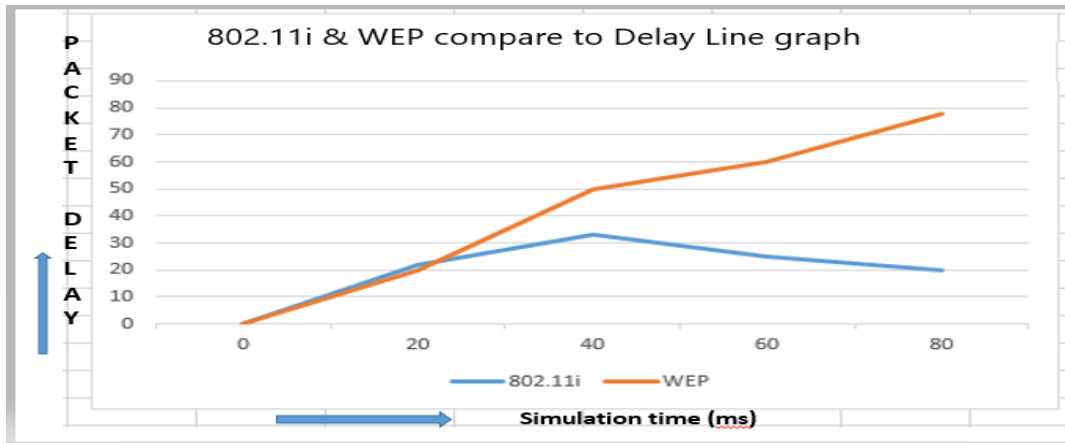


Figure 7. 2: WEP Authentication Delay vs 802.11i Authentication Delay

Fig 7.2 shows line graph where vertical axis is packet delay and horizontal axis is simulation time and showed about 802.11 authentication delay VS WEP authentication delay. In this fig of 802.11i delay is lower than WEP.

7.1.3 WAP Authentication Delay vs WEP Authentication Delay

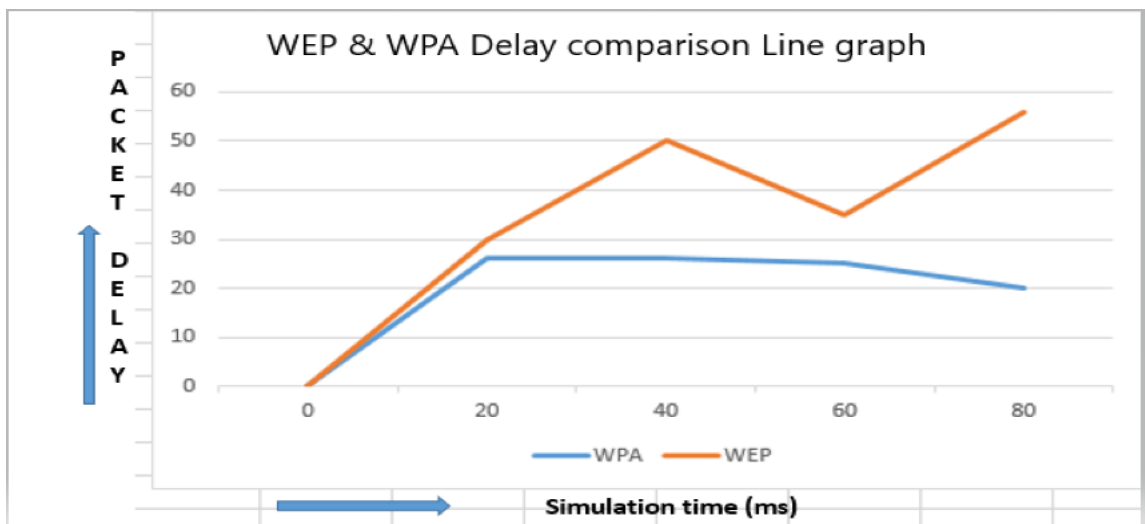


Figure 7. 3: WAP Authentication Delay vs WEP Authentication Delay

Fig 7.3 shows line graph where vertical axis is packet delay and horizontal axis is simulation time and showed about WPA authentication delay VS WEP authentication delay. In this fig of WPA delay is lower than WEP.

7.1.4 802.11i Loss vs WPA Loss

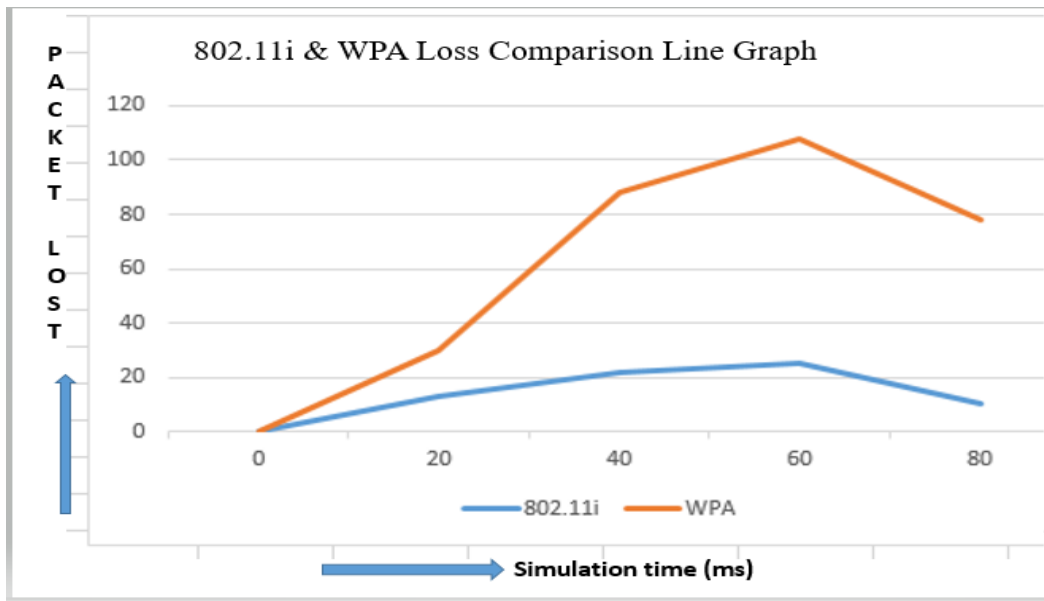


Figure 7. 4:802.11i Loss vs WPA Loss

Fig 7.4 shows line graph where vertical axis is packet loss and horizontal axis is simulation time and showed about 802.11i loss VS WPA loss. In this fig of 802.11i loss is lower than WPA.

7.1.5 802.11i Loss vs WEP Loss

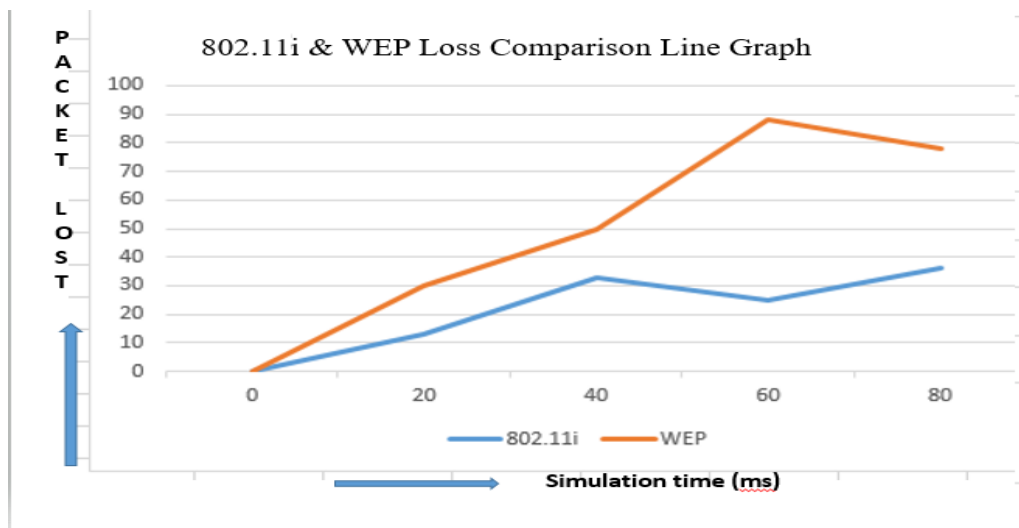


Figure 7. 5: 802.11i Loss vs WEP Loss

Fig 7.5 shows line graph where vertical axis is packet loss and horizontal axis is simulation time and showed about 802.11i loss VS WEP loss. In this fig of 802.11i loss is lower than WEP.

7.1.6 WEP Loss vs WPA Loss

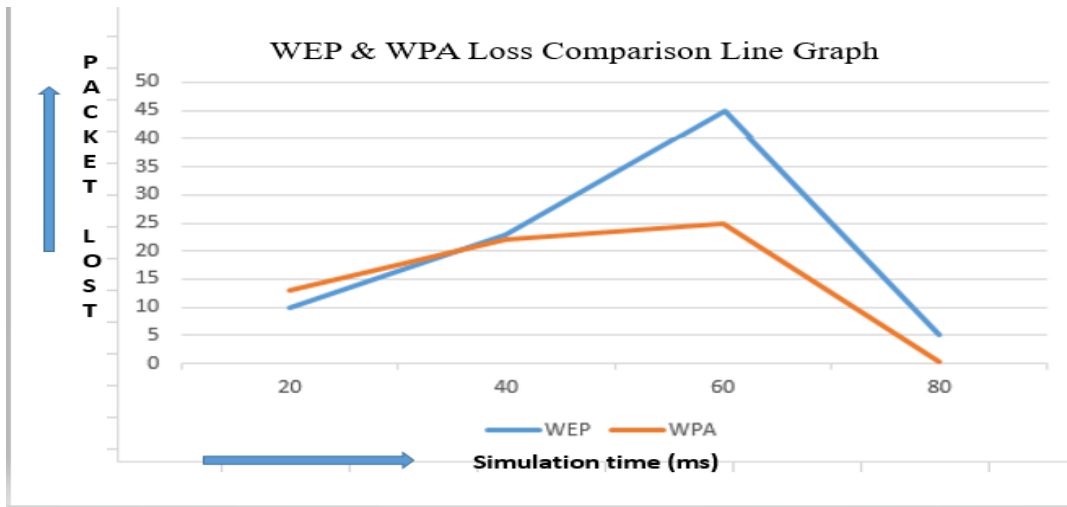


Figure 7. 6: WEP Loss vs WPA Loss

Fig 7.6 shows line graph where vertical axis is packet loss and horizontal axis is simulation time and showed about WPA loss VS WEP loss. In this fig of WPA loss is lower than WEP.

7.1.7 WEP ,WPA & 802.11i Delay

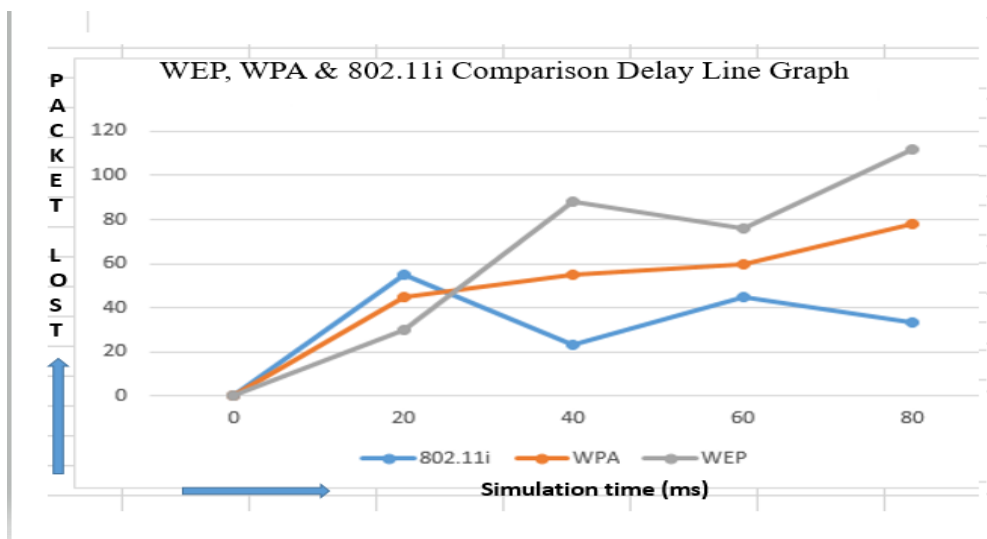


Figure 7. 7: WEP ,WPA & 802.11i Delay

Fig 7.7 shows line graph where vertical axis is packet delay and horizontal axis is simulation time and showed about WPA ,WEP and 802.11i delay comparison. In this fig the delay of different protocol is in graphical way and showed that WEP have much delay than WPA and 802.11i and 802.11i have little than WPA and WEP.

7.1.8 WEP ,WPA & 802.11i Loss

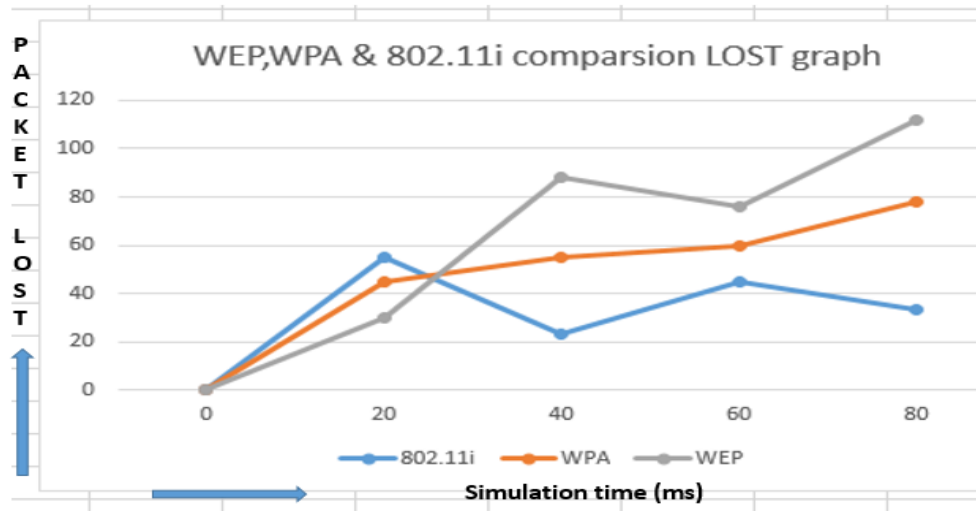


Figure 7. 8: WEP ,WPA & 802.11i Loss

Fig 7.8 shows line graph where vertical axis is packet loss and horizontal axis is simulation time and showed about WPA ,WEP and 802.11i loss comparsion.In this fig the loss of different protocol is in graphical way and showed that WEP have more loss than WPA and 802.11i and 802.11i is little loss thn WPA and WEP.

7.1.9 WEP ,WPA & 802.11i Output

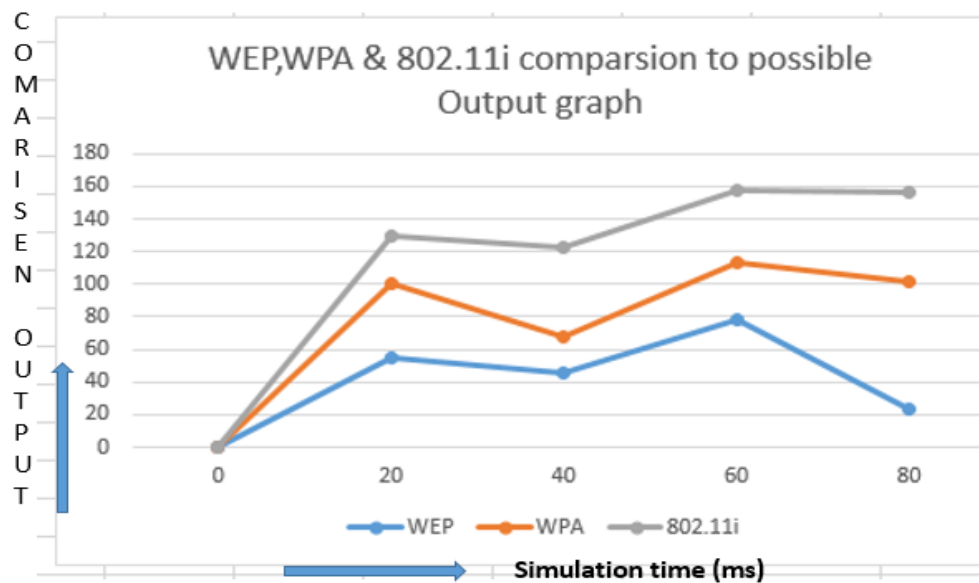


Figure 7. 9: WEP ,WPA & 802.11i Output

Fig 7.9 shows line graph where vertical axis is packet output and horizontal axis is simulation time and showed about WPA ,WEP and 802.11i output comparsion.In this fig the output of different protocol is in graphical way and showed that 802.11i is best protocol.

CHAPTER 8

CONCLUSION AND FUTURE WORK

8.1 Conclusion

Examination introduced in its proposition has broke down adequacy and inadequacies of WLAN security conventions. Investigation have demonstrated that while conventions the IEEE 802.11i offers good security of whole conventions there are motionless a few assaults it can be effectively propelled opposite the 802.11i- anchored arrange. The decision of an appropriate security convention in this manner, ought to be founded on the significance of information being transmitted in the system.

Confirmation latencies coming about because of various security conventions were then broke down. A scientific model was produced to compute the verification delay contingent upon the quantity of confirmation messages utilized in the convention and the likelihood of the validation outline being in blunder. It was discovered that most elevated confirmation delays are discovered when 802.11i security convention is utilized. Verification delay and examining defer make up the aggregate handover idleness, which is a fundamental measure to guarantee appropriate handover of the WLAN versatile station starting with one AP then onto the next.

This investigation has distinguished decrease of handover inactivity as the territory where more research should be completed. Distinctive methodologies towards this objective have been recommended in various looks into. One methodology proposed is to utilize cryptographic accreditations that will show client's conduct with the past passageway. In partner with the new AP inside a similar system, the customer gadget just introduces the qualifications and it will be conceded moment access as opposed to experiencing the entire confirmation process. Joshi, T proposes to abuse the consistency of client versatility and to disperse keys before genuine handover to vital APs as indicated by the anticipated development design. Anyway the greater part of the proposed methodologies negatively affect the adequacy of security convention and others extraordinarily increment the system overhead, which diminishes organize execution. IEEE Task Group r (TGr) is right now dealing with a normal for quick

(BSS) Basic Service Station handoff which will empower customer gadgets to flawlessly move among Access Points. Investigation proposes delicate handoff to be utilized when gadgets is to be given over to another BSS. In this methodology the customer gadget will keep getting system benefits through the first AP while in the meantime examining and confirmation forms are done with the focused on AP. This methodology will totally wipe out handover latencies. Anyway for this way to deal with be useful, customer gadgets should be fit for conveying on two radios in the meantime.

LIST OF ACRONYMS

AAA-Authentication, Authorization, and Accounting
AES-Advanced Encryption Standard
AP-Access Point
BSS-Basic Service Set
CBC-MAC Cipher Block Chaining Message Authentication Code
CCMP-Counter-mode/CBC-MAC Protocol
CSMA/CA-Carrier Sense Multiple Access with Collision Avoidance
CRC-Cyclic Redundancy Check
DoS-Denial of Service
DSSS-Direct Sequence Spread Spectrum
EAP-Extensible Authentication Protocol
EAPOL-Extensible Authentication Protocol Over LAN
ESS-Extended Service Set
FHSS-Frequency Hopping Spread Spectrum
FIPS-Federal Information Processing Standard
GTK-Group Transient Key
ICV-Integrity Check Value
IEEE-Institute of Electrical and Electronics Engineers
IETF-Internet Engineering Task Force
IV-Initialization Vector
LAN-Local Area Network
MAC-Medium Access Control

MAN-Metropolitan Area Network
MIC-Message Integrity Code
MIMO-Multiple Input, Multiple Output
MSK-Master Session Key
OFDM-Orthogonal Frequency Division Multiplexing
NIC-Network Interface Card
PCMCIA-Personal Computer Memory Card International Association
PDA-Personal Digital Assistant
PEAP-Protected EAP
PHY-Physical Layer
PMK-Pair-wise Master Key
PSK-Pre-Shared Key
QoS-Quality of Service
RADIUS-Remote Authentication Dial In User Service
RC4-Rivest Cipher 4
RF-Radio Frequency
RSNA-Robust Security Network Association
RSN IE-Robust Security Network Information Element
SSID-Service Set Identifier
SSL-Secure Socket Layer
TK-Temporal Key
TKIP-Temporal Key Integrity Protocol
TLS-Transport Layer Security
WEP-Wired Equivalent Privacy
WiMAX-Worldwide Interoperability for Microwave Access
Wi-Fi-Wireless Fidelity
WLAN-Wireless Local Area Network
WPA-Wi-Fi Protected Access
XOR-Exclusive-OR operation

References

- [1] Selim, G., El Badawy, H.M.; Salam, M.A; New protocol design for wireless networks security; The 8th International Conference of Advanced Communication Technology, 2006. CACT 2006.
- [2] Shin, M.; Ma, J.; Mishra, A.; Arbaugh, W.A.; Wireless network security and interworking; Proceedings of the IEEE; Feb. 2006
- [3] IEEE Standard 802.11, 1999; Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
- [4] IEEE Standard 802.11i, 2004; Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendmends 6: Medium Access Control (MAC) Security Enhancements; July 2004
- [5] IEEE Standard 802.11a, 1999; Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendmends 1: High-Speed Physical Layer (PHY) Extension in the 5 GHz Band
- [6] IEEE Standard 802.11b, 1999; Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendmends 2: High-Speed Physical Layer Extension in the 2.4 GHz Band
- [7] IEEE Standard 802.11g, 2003; Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendmends 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band
- [8] IEEE Standard 802.11X-2004; IEEE Standard for Local and Metropolitan Area Networks Port Based Network Access Control, 2004
- [9] Borisov, N., Goldberg, I., Wagner, D.; Intercepting Mobile Communications: The Insecurity of 802.11; Seventh Annual International Conference on Mobile Computing and Networking; July 2001
- [10] Hao Yang, Ricciato, F., Songwu Lu, Lixia Zhang; Securing a wireless world Proceedings of the IEEE Volume 94; Feb. 2006
- [11] Lucent Technologies; Users Guide for the ORiNOCO Managers Suite; Nov. 2000
- [12] Wi-Fi Alliance; Wi-Fi Protected Access: Strong, Standard Based, Interoperable Security for todays Wi-Fi Network, [Online] Available at <http://www.wi-fi.org/>
- [13] Fathi, H., Kobara, K., Chakraborty, S.S., Imai, H., Prasad, R.; On the impact of security on latency in WLAN 802.11b; IEEE Global Telecommunications Conference, 2005.GLOBECOM '05. Dec. 2005
- [14] Aime, M.D., Calandriello, G., Lioy, A.;Dependability in Wireless Networks: Can We Rely on WiFi? IEEE Security & Privacy Magazine; Jan.-Feb. 2007
- [15] Sithirasenan, E.; Zafar, S.; Muthukkumarasamy, V.; Formal verification of the IEEE802.11i WLAN security protocol; Australian Software Engineering Conference, 2006.; April2006

- [16] Gurkas, G.Z., Zaim, A.H., Aydin, M.A.; Security Mechanisms And Their Performance Impacts On Wireless Local Area Networks; International Symposium on Computer Networks, 2006; June 2006
- [17] Jyh-Cheng Chen, Yu-Ping Wang; Extensible authentication protocol (EAP) and IEEE 802.11X: tutorial and empirical experience Communications Magazine, IEEE Volume 43; Dec. 2005
- [18] Changhua He, John Mitchell; Analysis of the 802.11i 4-way handshake; Proceedings of the 3rd ACM workshop on Wireless security; 2004 Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 2001.
- [19] Jyh-Cheng Chen; Ming-Chia Jiang; Yi-wen Liu; Wireless LAN security and IEEE 802.11i; Wireless Communications IEEE; Feb 2005
- [20] Wool, A.; A note on the fragility of the "Michael" message integrity code; IEEE Transactions on Wireless Communications; Sept. 2004
- [21] Tsakountakis, A., Kambourakis, G., Gritzalis, S.; Towards effective Wireless Intrusion Detection in IEEE 802.11i; Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2007. (SECPerU 2007); July 2007
- [22] KeunSoon Lee, HyoJin Kim, JooSeok Song; Lightweight packet authentication in IEEE 802.11; Wireless Telecommunications Symposium, 2005; April, 2005
- [23] Manivannan, N., Neelameham, P.; Alternative Pair-wise Key Exchange Protocols (IEEE 802.11i) in Wireless LANs; International Conference on Wireless and Mobile Communications, 2006. ICWMC '06; July 2006
- [24] Ju-A Lee, Jae-Hyun Kim, Jun-Hee Park, Kyung-Duk Moon; A Secure Wireless LAN Access Technique for Home Network; IEEE 63rd Vehicular Technology Conference, 2006;
- [25] 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
- [26] Xiao Liu, Fapojuwo, A.O.; Formal Evaluation of Major Authentication Methods for IEEE 802.11i WLAN Standard; IEEE 64th Vehicular Technology Conference, 2006; Sept. 2006
- [27] Aura, T., Roe, M.; Reducing Reauthentication Delay in Wireless Networks; First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005; Sept. 2005
- [28] Iacobucci, M.S.; Paris, G.; Simboli, D.; Zitti, G.; Analysis and Performance Evaluation of Wireless LAN Handover; 2nd International Symposium Wireless Communication Systems, 2005; Sept. 2005
- [29] Mukherjee, A., Joshi, T., Agrawal, D.P.; Minimizing re-authentication overheads in infrastructure IEEE 802.11 WLAN networks [re-authentication read pre-authentication];

2005 IEEE Wireless Communications and Networking Conference,
March 2005

- [30] 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
- [31] Matsunaka, T.; Izumikawa, H.; Sugiyama, K.; An Effective Authentication Procedure Considering User Expiry Time During Handover; IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications; Sept. 2006
- [32] Andrew S. Tanenbaum; Computer Networks; Fourth edition; Prentice Hall, 2003
- [33] Robert Moskowitz; Weakness in Passphrase Choice in WPA Interface; Online at: <http://www.wifinetnews.com/archive/002452.html>; 2003
- [34] Kassab, M., Belghith, A., Bonnin, J., Sassi, S.; Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks; Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling; 2005
- [35] Mishra, A., Shin, M., Arbaugh, W.; An empirical analysis of the IEEE 802.11 MAC layer handoff process; ACM SIGCOMM Computer Communication Review; 2003
- [36] Aboba, B.; Fast Handoff Issues; IEEE-03-155r0-1 IEEE 802.11 Working Group; March 2003
- [37] Chen, J., Tseng, Y., Lee, H.; A Seamless Handoff Mechanism for DHCP-Based IEEE 802.11 WLANs; IEEE Communication Letters; August 2007.
- [38] Barsocchi, P., Oligeri, G., Potorti, F.; Frame Error Rate in Rural Wi-Fi Networks; IEEE WinMee/WitMeMo Workshop; April 2007
- [39] 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;
- [40] J. WELCH, S. D. LATHROP, A Survey of 802.11a Wireless Security Threats and Security Mechanisms. United States Military Academy West Point, New York, (2003), [http://www.itoc.usma.edu/Documents/ITOCTR-2003-101\(G6\).pdf](http://www.itoc.usma.edu/Documents/ITOCTR-2003-101(G6).pdf).
- [42] J. C. CHEN, M. C. JIANG, Y. W. LIU, Wireless LAN security and IEEE 802.11i. IEEE Wireless Communications, (2005), vol. 12, no. 1, pp. 27—36.
- [43] R. PRODANOVIC, D. SIMIC, Holistic Approach to WEP Protocol in Securing Wireless Network Infrastructure. Com SIS, Vol. 3, No. 2, pp. 97—113, (2006)
- [44] C. HE, J. C. MITCHELL, Security Analysis and Improvements for IEEE 802.11i. Stanford, USA, (2004),
- [45] "Network Simulator 2", <http://www.linuxjournal.com/article/5929>, December 2015.