



L OVELY
P ROFESSIONAL
U NIVERSITY

IMPROVING WIRELESS SECURITY WITH ENHANCEMENT IN WPA2 PROTOCOL

A Dissertation submitted

By SUMAN RAWAT

to

Department of Computer Science and Engineering

In partial fulfillment of the Requirement for the

Award of the Degree of

Master of Technology in Computer Science

Under the guidance of

Asst. Prof. Md. Ataulah

May 2015

ABSTRACT

Wireless local area networks have become quite popular and are widely deployed nowadays in universities, hospitals, airports, residential areas, cafes, public hotspots etc. with such a growth in wlans popularity, security is a keen concern. End users should be provided with full security so that their rights should not be at stake. CIA traits should remain intact i.e. confidentiality, integrity, availability should be there for the authentic and authorized user.

To provide security the users security mechanisms like Wired Equivalent Privacy (WEP), WI-FI Protected Access (WPA), and WI-FI Protected Access2 (WPA2) are used. These security protocols use strong and robust algorithms for the encryption purpose to protect our credentials. Some flaws or limitation were discovered in these protocols. So our main aim will be towards the removal of such flaws and enhance the security of these security mechanisms

DECLARATION

I hereby declare that the dissertation entitled, "Improving Wireless Security with Enhancement in WPA2 Protocol" submitted for the M.Tech degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: 4th May, 2015

Suman Rawat

Regn. No. 11008647

CERTIFICATE

This is to certify that Suman Rawat has completed M.Tech dissertation proposal titled **“Improving Wireless Security with Enhancement in WPA2 Protocol”** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech Computer Science and Engineering.

Date: 4th May, 2015

Signature of advisor

Name: Md. Ataulah

UID: 16915

ACKNOWLEDGEMENT

I am highly grateful to lovely professional university and also Md. Atullah Sir, for providing this opportunity to carry out the dissertation work. The constant guidance and encouragement received from Md. Atullah sir has been of great help in carrying out the project work and it's acknowledged with the reverential thanks He actually laid the ground for conceptual understanding of technologies used in project.

Without the wise counsel the able guidance, it would have been impossible to complete the dissertation report in this manner.

We express gratitude to other faculty member of CSE/IT department of Lovely Professional University for their intellectual support throughout the course of this work.

TABLE OF CONTENTS

CONTENTS	PAGE NUMBERS
1. Introduction	1
1.1 Network Security	1
1.2 Cryptography	2
1.3 WEP	3
1.4 WPA	5
1.5 WPA2	6
1.6 Organization of thesis	11
2. Literature review	13
2.1 An Efficient Password-based Three-party Authentication Multiple key Exchange protocol wireless mobile network.	13
2.2 Exploiting WPA2-Enterprise Vendor Implementation Weakness through challenge Response Oracles.	13
2.3 Evaluation of Enhanced Security Solutions in 802.11-Based Networks	14
2.4 A Modified RSA Encryption Technique Based on Multiple public key	14
2.5 Light Authentication and Key Management on 802.11 with Elliptic Curve Cryptography	15
2.6 An Investigation of Security Trends in Personal Wireless Network	15
2.7 Encryption using DES of ANounce in 4-Way Handshake Protocol for Authentication in WPA2	15
2.8 Multiple Packet System: a security approach for wireless network	16
2.9 Modeling and Analysis of IEEE802.11i WPA-PSK Authentication protocol.	16
2.10 Modeling and Analysis of IEEE802.11i WPA-PSK Authentication protocol.	17
2.11 DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis	17
2.12 Security Improvement of Wi-Fi Protected Access 2	18

2.13 Security Analysis and Authentication Improvements for IEEE 802.11i Specification.	19
2.14 A secure 4-Way Handshake in 802.11i uses cookies	19
3. Present Work	20
3.1 Problem Formulation	22
3.2 Objectives of problem	23
3.3 Research Methodology	24
4. Result and Discussions	28
5. Conclusion and Future Scope	33
6. References	34
7. Appendix	37

LIST OF TABLES

TABLES	PAGE NUMBER
1. Table 1.1: Comparison of security mechanism	11
2. Table 2.1: Algorithm setting	18

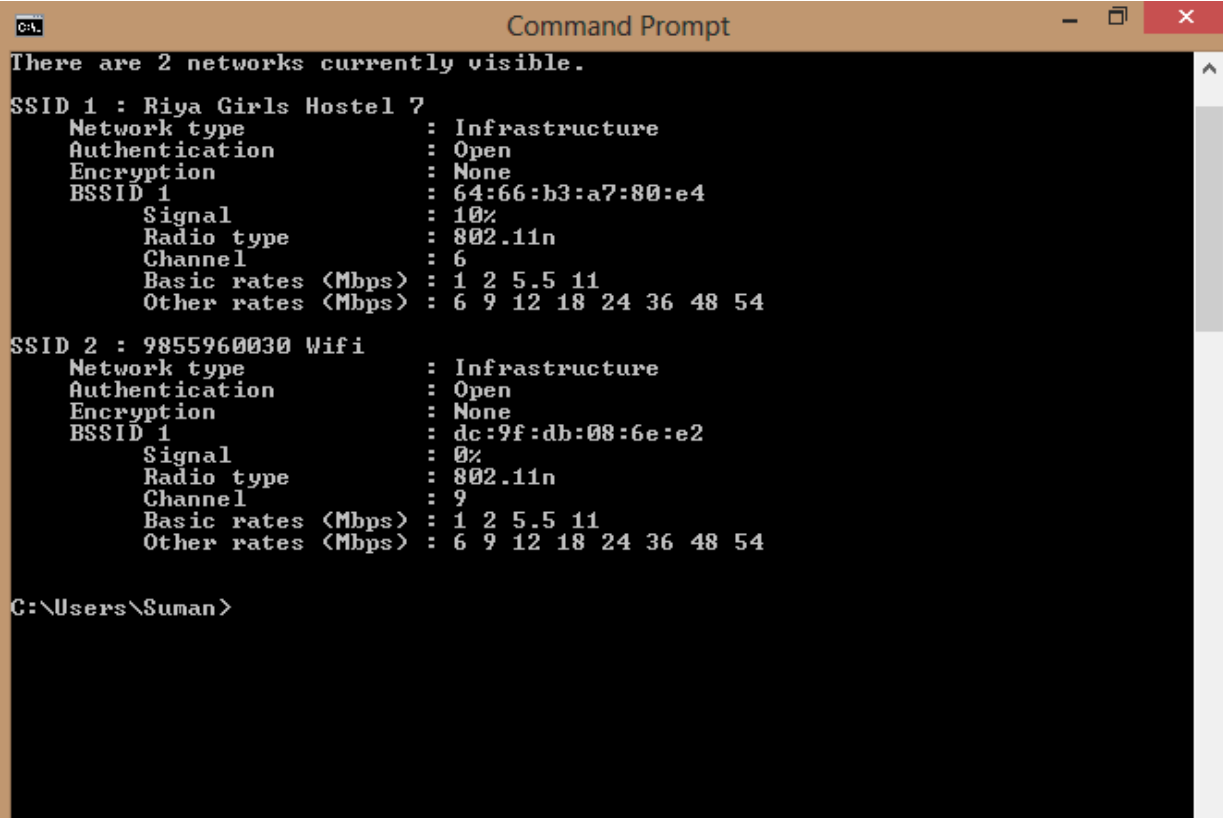
LIST OF FIGURES

FIGURES	PAGE NUMBER
1. Figure 1.1 : Monitoring Available networks	1
2. Figure 1.2 : WEP process	4
3. Figure 1.3: WPA-TKIP encryption/decryption process	5
4. Figure 1.4: GTK distribution	7
5. Figure 1.5: WPA2 Enterprise mode	8
6. Figure 1.6: WPA2 Personal mode	9
7. Figure 2.1: Execution results with CBC mode	18
8. Figure 3.1 Encryption procedure	25
9. Figure 3.2 Flow Chart	27
10. Figure 4.1 Probe request from client	29
11. Figure 4.2 Probe response	29
12. Figure 4.3 Client sending encrypted code	29
13. Figure 4.4 Message 1 generated by AP	30
14. Figure 4.5 Encrypted message 1 send to client	30
15. Figure 4.6 Message 1 received at client side	31
16. Figure 4.7 Sending message 2	31
17. Figure 4.8 Message 2 at AP	32
18. Figure 4.9 Key installed	32

CHAPTER 1

INTRODUCTION

Wireless local area network now a day is a typical term as we see numerous remote systems around us. With progression in innovation more remote gadget are accessible in the business sector. As WLAN cell system, Bluetooth have picked up notoriety as they give much solaces like adaptability, versatility, convenience the fundamental concern goes towards the security issues identified with the remote media. Remote framework engages people to grant an entrance applications and information without wires. Since bundles in remote system goes in an open media as radio waves and there comes an immense issue of its security as anybody can investigate your system catch parcels can decode them and utilization private information in any fancied way.



```
C:\> netsh wlan show networks

There are 2 networks currently visible.

SSID 1 : Riya Girls Hostel 7
Network type           : Infrastructure
Authentication         : Open
Encryption             : None
BSSID 1                : 64:66:b3:a7:80:e4
Signal                 : 10%
Radio type             : 802.11n
Channel                : 6
Basic rates (Mbps)    : 1 2 5.5 11
Other rates (Mbps)    : 6 9 12 18 24 36 48 54

SSID 2 : 9855960030 Wifi
Network type           : Infrastructure
Authentication         : Open
Encryption             : None
BSSID 1                : dc:9f:db:08:6e:e2
Signal                 : 0%
Radio type             : 802.11n
Channel                : 9
Basic rates (Mbps)    : 1 2 5.5 11
Other rates (Mbps)    : 6 9 12 18 24 36 48 54

C:\Users\Suman>
```

Figure 1.1: Monitoring available networks

1.1 Network security

The measures to be taken to protect data during their transmission to avert and screen unapproved access, abuse, adjustment, or refusal of a PC system and system open assets. System security includes the approval of access to information in a network. Network security is included in associations, endeavours, and different sorts of establishments. It does

as its title clarifies: It secures the system, and in addition securing and directing operations being finished. The most widely recognized and straightforward method for ensuring a system asset is by doling out it a one of a kind name and a comparing secret word.

1.2 Cryptography

The word is gotten from the Greek kryptos, importance covered up. The source of cryptography is typically dated from around 2000 BC, with the Egyptian practice of hieroglyphics. These comprised of complex pictograms, the full importance of which was just known to a world class few. The primary known utilization of an advanced figure was by Julius Caesar (100 BC to 44 BC), who did not believe his couriers when speaking with his governors and officers. Consequently, he made a framework in which every character in his messages was supplanted by a character three positions in front of it in the Roman letter set.

It is a process of converting the plain text in such a form which cannot be recognized by the intruder and only the legitimated person can read or process it. In cryptography the plain text is converted into the cipher text which is known as the process of encryption and then back again changing it into the plain text is known as the process of decryption.

The cryptography has four main objectives.

- **Confidentiality:** The data can't be seen by anybody for whom it was unintended.
- **Integrity:** The data can't be changed away or travel in the middle of sender and proposed collector without the adjustment being distinguished.
- **Non-repudiation:** The maker/sender of the data can't deny at a later stage his or her expectations in the creation or transmission of the data.
- **Authentication:** The sender and recipient can affirm every others personality and the source/destination of the data.

Security is the most important aspect of the wireless network and implementing security of the medium is very challenging task. To secure the data that it being transmitted in the medium many security measures were adopted.

To resolve wireless security issues IEEE developed 3 generations of wireless security protocols:

- Wired equivalent privacy (WEP)
- WI-FI Protected Access (WPA)
- WI-FI Protected Access, version 2 (WPA2/802.11i)

1.3 Wired Equivalent Privacy (WEP)

WEP was outlined in year 1999 alongside 802.11b standard to give remote security to the clients. It was meant to give secure correspondence between the end clients giving classifiedness when contrasted with the wired system. WEP was the first security calculation to give security to the remote medium. WEP encryption permits the gathering of gadgets in the system to trade the encoded messages with one another concealing the substance the messages to the outcasts. WEP conveys Rivest Cipher 4 (RC4) calculation otherwise called stream figure for encryption. Both sender and collector have the same key i.e. same key is utilized encryption and unscrambling. WEP utilize CRC-32 calculation for information trustworthiness.

The keys are generally a collection of hexadecimal digits and are referred to as WEP keys. These keys consists of numbers (0-9) and letters (A-F). Some of the examples of WEP keys are as follows:-

- 1A648C9FD2
- 99D767BAC48EA23B0C0176D152
- The length of a WEP key relies upon the kind of security used:
- 40- to 64-bit WEP: 10 digit key
- 104- or 128-bit WEP: 26 digit key
- 256-bit WEP: 58 digit key

Two techniques for validation can be utilized with WEP: Open System authentication and Shared Key authentication.

In Open System authentication, the WLAN customer need not give its accreditations to the Access Point amid verification. Any customer can confirm with the Access Point and after that endeavor to partner. In actuality, no verification happens. Along these lines WEP keys can be utilized for encoding information outlines. As of right now, the customer must have the right keys.

In Shared Key authentication, the WEP key is utilized for verification as a part of a four-stage challenge-reaction handshake:

- The customer sends a verification appeal to the Access Point.
- The Access Point answers with a reasonable content test.
- The customer scrambles the test content utilizing the designed WEP key and sends it back in another confirmation demand.

- The Access Point unscrambles the reaction. In the event that this matches the test content, the Access Point sends back a positive answer.

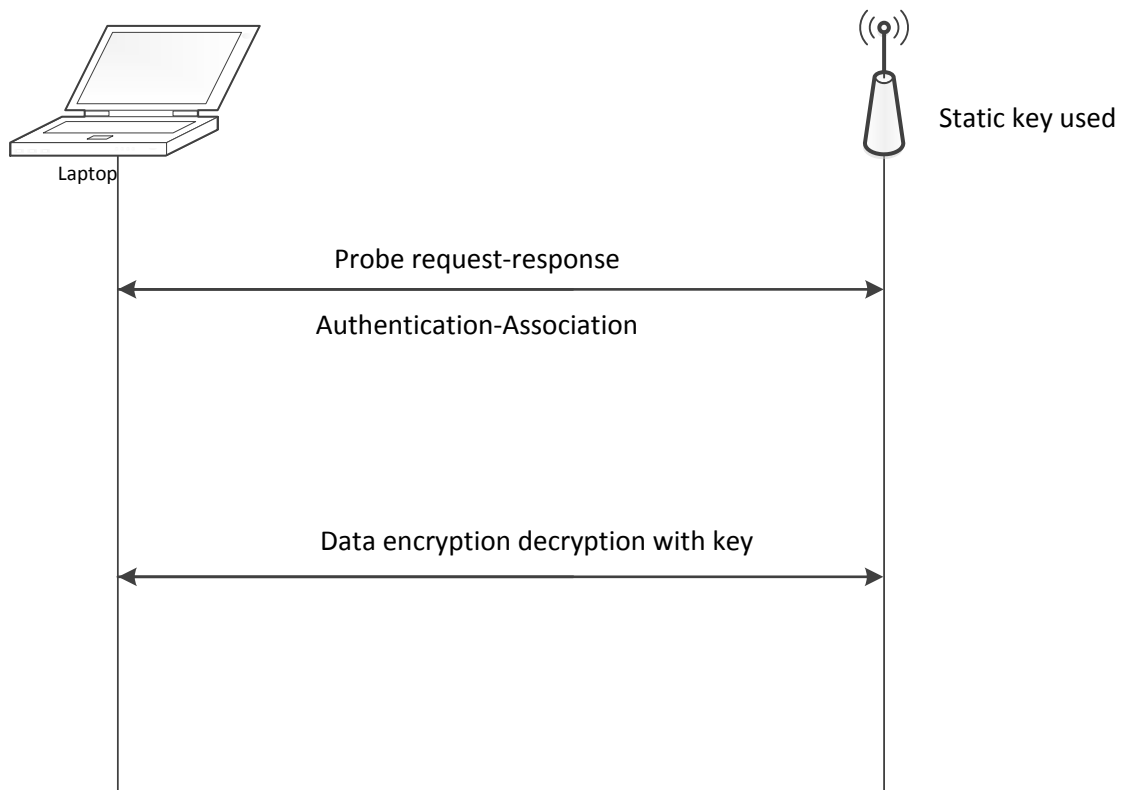


Figure 1.2: WEP process

It has been a decade since WEP cracked, since WEP security is based upon weak Michael algorithm which provides inadequate security and is easily crack able. Attacks done on WEP are Chop-chop attack, Korean attack etc.

1.3.1 Limitations of WEP protocol

- WEP does not forestall imitation of bundles.
- RC4 calculation is not legitimately utilized. The key utilized are exceptionally feeble and can be broken effortlessly by any online unreservedly accessible apparatuses couple of hours to minutes.
- It does not anticipate replay assault. Programming like wire shark can catch bundles and replay it n number of times and they will be acknowledged as genuine parcels by convention.
- Confidentiality is not gave as aggressor can change the parcel without the learning of the encryption key
- Same key is utilized for encryption and decryption.

1.4 WI-FI Protected Access

WPA was developed by IEEE 802.11 task force to resolve the security issues as a temporary solution so WPA was designed to run on existing hardware of WEP as a software upgrade. WAP introduced TKIP which is a per-packet key mixing 128-bit key and it is dynamically generated for each packet. 48 bit Initialization Vector, RC4 stream cipher along with 128 bit key are concatenated in WPA. Integrity check is implemented with MIC.

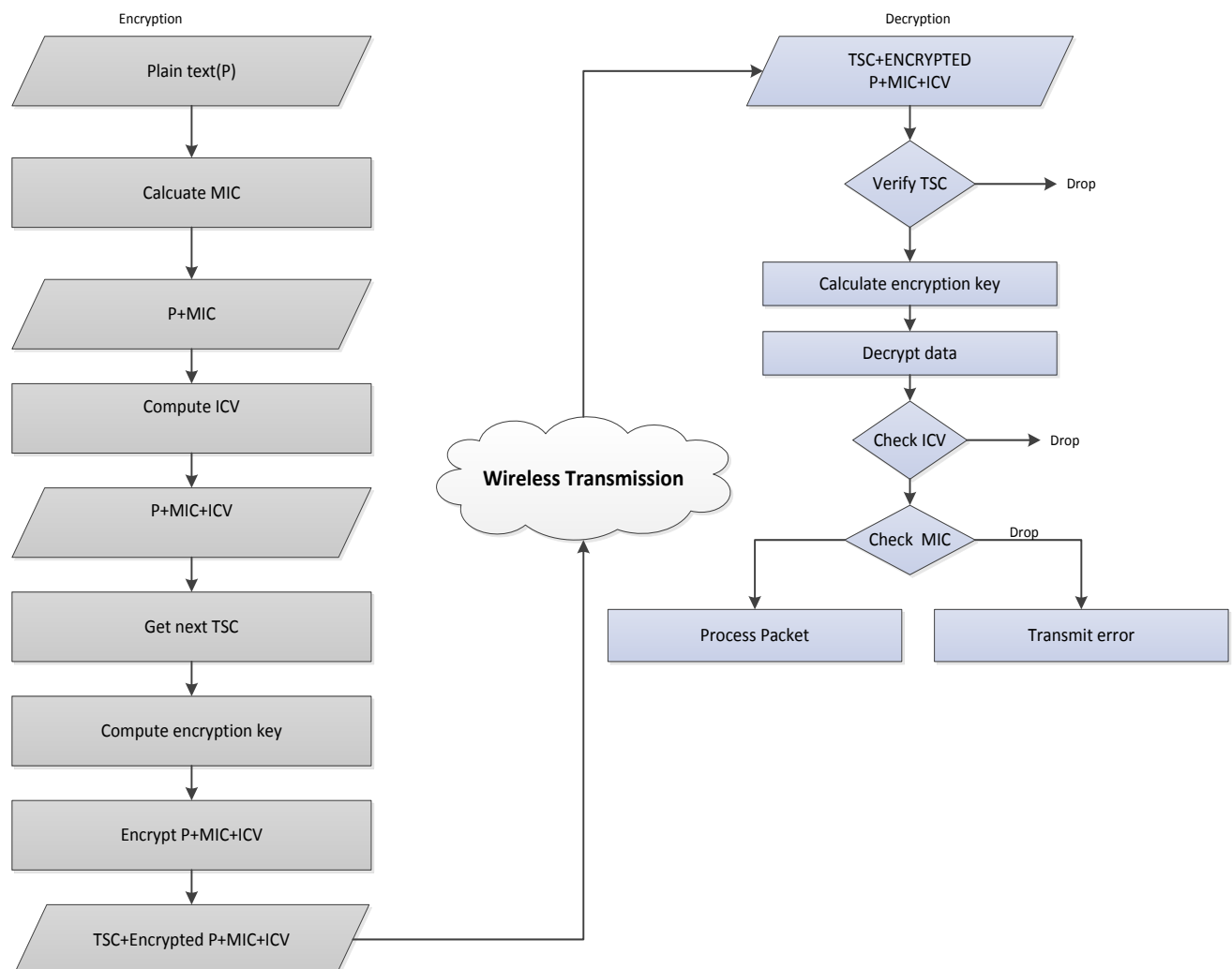


Figure 1.3: WPA-TKIP encryption/decryption process

1.4.1 WPA TKIP process

Sender: MAC Service Data unit (MSDU) is the data packet that is to be transmitted. MIC value is calculated for MSDU with the help of Michael algorithm. Michael algorithm is a keyed hash function which takes two inputs: input data and secret key. Different secret keys are used for calculating MIC for Client to AP and AP to client communication. However Michael algorithm is not the secure, one can easily retrieve MIC key with given data and

calculated MIC value. MSDU concatenated with MIC, if necessary fragmented into Mac protocol data units (MPDUs). At most 16 MPDUs are supported. To implement the TKIP on old WEP hardware each MPDU goes under WEP encapsulation which appends integrity check value (ICV) to MPDUs. This is later encrypted with RC4 algorithm; encryption key is called WEP seed which is calculated via mixing function which combined temporal key (TK), sender's MAC address and the TKIP Sequence Counter (TSC). In the end the frame is appended with appropriate 802.11 headers which include TSC which is a replay counter that increases each time a MPDU frame sent successfully.

Receiver: After receiving TKIP frame, AP checks if TSC is in order or not. If not, it is dropped. Proceed with checking ICV correct or not. If not, packet dropped. After receiving all the MPDUs they are assembled into one MSDU and its MIC value is verified. If it is correct the frame is accepted and TSC counter is updated otherwise TKIP countermeasure is activated.

1.4.2 TKIP counter measure

- When a MSDU is received at the client with an invalid MIC value it will send a MIC failure report to AP.
- An AP receiving an invalid MIC value does not broadcast MIC failure report but logs the failure.
- If AP detects two MIC failures within one minute and TKIP client to AP are deauthenticated and AP do not transmit or receive any request for one minute. After one minute all the clients reassociate with the AP new PTK.

1.4.3 Attacks on WPA

Beck and Tews discovered the flaw in TKIP. ARP reply packets are chosen for the attack. Attack allows attacker to decrypt data slowly and once the packet is decrypted, attacker can forge up to 7 packets of any content. It does not require any authentication for success. For this attack the QoS should be enabled.

1.5 WI-FI Protected Access 2

WI-FI Protected Access also known as robust security network 802.11i introduced in September 2004 by IEEE 802.11 authority. To implement WPA2 hardware changes are required. Two types of keys are used for data encryption in WPA2 and these keys are generated dynamically.

1.5.1 WPA2 Advantages

- Provides stronger information insurance and system access control.
- Uses better encryption – AES.
- It can utilize TKIP for interoperability with WPA.
- Impossible to break without access to the system.
- Older gear does no

Pairwise Temporal Key (PTK) : It is the value derived from PMK, AP MAC address, supplicant MAC address, ANonce , SNonce using a pseudo random function. It is split into five keys which are Temporal Encryption Key (TK), two MIC one for supplicant to AP communication and other for AP to client communication, EAPOL key encryption key (KEK), EAPOL – key confirmation key (KCK).

Group Master Key (GMK): It is an auxiliary key that is used to derive group temporal key (GTK).

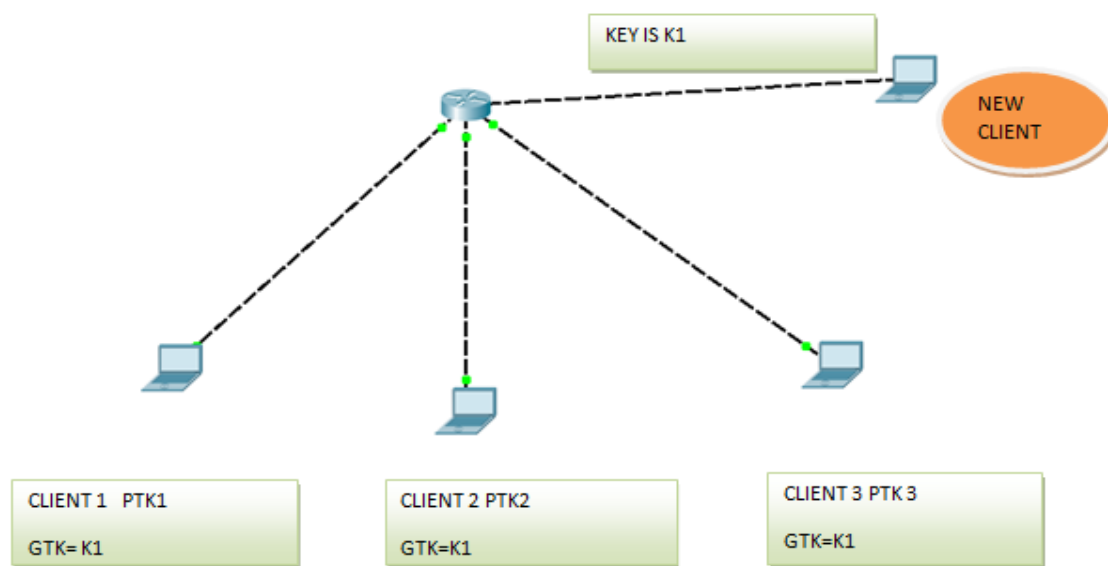


Figure 1.4: GTK distribution

WPA2 also has two versions

- **Enterprise mode**
- **Personal mode**

Enterprise mode: Authentication relies on IEEE 802.1 X standards. It includes three major components which are supplicant (client), authentication server RADIUS and the Authenticator (AP), the authentication server. The enterprise mode of the WPA2 is more secure than the personal mode. In big multinational companies, government agencies, universities the enterprise mode is used.

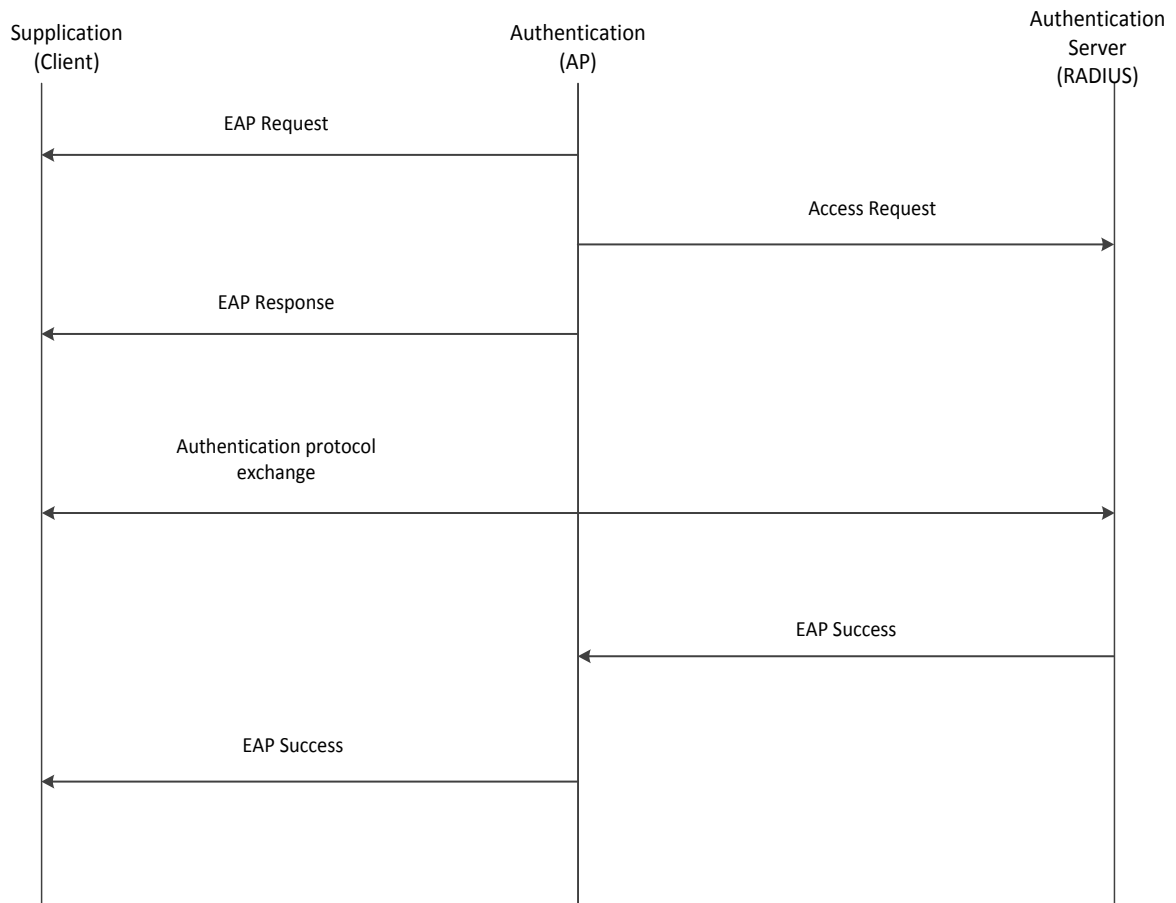


Figure 1.5: WPA2 enterprise mode

Personal mode: In personal mode the authentication does not require an authentication server; it is performed between the supplicant and the AP generating a 256-bit PSK from passphrase (8 to 63 characters). PSK along with SSID length and Service Set Identifier is used to calculate PMK which is used in later stages for key generation.

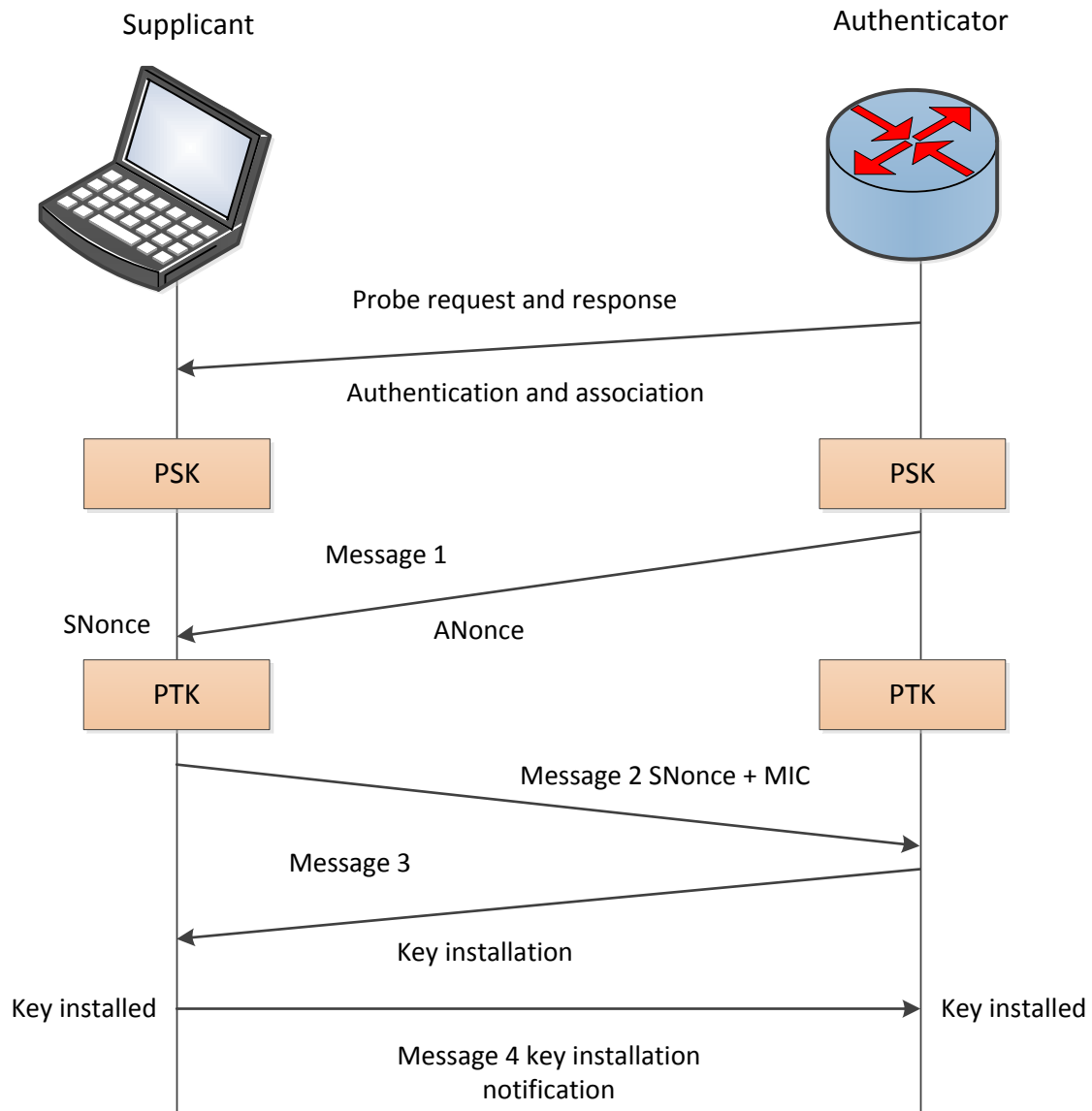


Figure 1.6: WPA2 Personal mode

WPA2 uses 802.1x to authenticate users and AES-based CCMP to encrypt messages. In WPA2 hardware change is required.

When confirmation done, customer sends affiliation appeal to AP. This appeal incorporates secure validation and encryption conventions it needs to utilize; if AP bolsters the asked for conventions affiliation is made and AP advises customer that affiliation is finished. After verification and affiliation, 4-way handshake performed when utilizing CCMP, a 512-bit PTK is created from PSK which 256-bit which is derived from the passphrase and is imparted in the middle of customer and AP.

PBKDF2 is a password based key derivation function which maps the variable length passphrase into fixed key size which is to be used.

4096 is number of times the passphrase is hashed.

256 is a number of bits output by passphrase mapping.

From PTK Temporal Encryption Key (TK) 128-bit long key and two 32-bit long Message Integrity Check (MIC) keys: one for AP to client and one for client to AP communication; are derived.

1.5.2 Attacks on WPA2

- **Deauthentication assault:** To catch the 4-way handshake the gatecrasher send disassociation parcels to customer associated with AP because of this the customer will be disassociated from the AP. This assault is mostly sent to catch the 4-Way Handshake.
- **Dictionary assault:** Gatecrasher utilizes word reference of words; creates PSK with the assistance of caught 4-way handshake and determine PTK confirms in the event that it is right or not with MIC.
- **Denial of Service (Dos) assault:** This makes assets occupied to the true blue client. This assault can be performed by infusion administration parcel or control outlines.
- **Evil Twin assault:** Gatecrasher will imagine like server to customer and imagine like cline to server. interloper will disassociate the authentic customer association with the server and when customer tries to reconnect it will divert its activity towards itself and sends confirmation page to customer o enter qualifications as customer enters watchword, the gatecrasher knows

	WEP	WPA	WPA2
AIM	Provide security to wireless medium	Overcome shortcoming of WEP	Provide robust and strong security mechanism. Enhancement of WPA.
KEY SIZE	Small key 40 bits	128 bits	256 bits
ENCRYPTION SCHEME	Rivest cipher 4(RC4)	Temporal key integrity protocol(TKIP)	Counter Mode with Cipher block Chaining Message Authentication Code protocol(CCMP) using AES
DATA INTEGRITY	CRC-32	MIC	CBC-MAC
CIPHER MODE	Stream cipher	Stream cipher	Block cipher
KEY MANAGEMENT	None and static keys used always	Strong and robust	Strong , robust and dynamic
AUTHENTICATION	WEP-shared and WEP-open.	WPA-PSK and WPA-enterprise.	WPA2-Personal and WPA2-Enterprise.
HARDWARE COMPATIBILITY	Works on existing hardware.	Works on existing hardware with software updates.	New hardware configuration required.

Table 1.1: Comparison of security mechanisms

1.6 Organization of thesis

Our thesis work is organized as follows.

Chapter 2 is dedicated to the literature review that has helped a lot in deciding the objectives of our research. We analyzed the security of the WPA2 in depth with the intense literature survey by analyzing the previous research done by the researchers. Mitigated on how to improve its security; to avoid the intruder from getting access to the confidential data of the users by making modifications in the current mechanism. We will to make the security mechanism more secure and efficient by critically reviewing the exiting security mechanisms.

We will consider several existing solutions to solve the present problems and adding more procedure to mitigate the issues and the limitations.

Chapter 3 explains the current or present work which we are doing in the wpa2 protocol. It includes the problem formulation, objective of the research and the research methodology. In problem formulation we have discussed the problems which describe the issues which we are currently facing. In this section the problems and the shortcomings of the WPA2 protocol are discussed in detail. It is followed by the objective of the problem in which we have discussed our goals to be achieved in our research. It is followed by the research methodology in which we have discussed the detail procedure of our implementation which we have adopted to accomplish our research. It includes the algorithm of the proposed solution; how the modification is done on the current version of the WPA2 protocol.

Chapter 4 contains the results and implementation of the proposed methodology where the snapshots of each step are shown.

In Chapter 5 we will sum up our thesis by the conclusion and future scope of the performed work.

CHAPTER 2

REVIEW OF LITERATURE

2.1 An Efficient Password-based Three-party Authentication Multiple key Exchange protocol wireless mobile network

Hang Tu et al. [1] proposed improved three-party authenticated multiple key exchange (3PAMKE) protocol for wireless mobile network. Proposed protocol consists of two phases; initialization phase and the authenticated key exchange phase. In initialization phase server generates system parameters and both end users get their private keys by registering into the server. End users generate their session keys with the aid of server. In authentication and key exchange phase server generates two random numbers send to end users separately along with identity keys. Upon receiving the messages both end users generates three random numbers both calculates e_a and e_b values for them separately and send to server. Server after receiving the message calculates K_a and K_b and checks whether e_a and e_b values are same it has calculated, if not session is ended. Then both end users compute their keys. This proposed protocol provides mutual authentication and perfect forward secrecy. This protocol also prevents off-line password-guessing attacks, replay attacks and man in the middle attack.

2.2 Exploiting WPA2-Enterprise Vendor Implementation Weakness through challenge Response Oracles

Pieter Robyns et al. [2] demonstrated the attack of stealing the user's credentials and gained the unauthorized access to the network. This paper explains how the devices like MSCHAPv2 challenge response oracles, Lightweight EAP (LEAP) MSCHAPv1 credentials can be captured by the fake or rouge AP. The vulnerability was also found in all the current versions of the Apple's iOS and OS X operating systems and other devices as well. The attack that is executed is the combination of the two vulnerabilities. First is that some devices accepts olders LEAP method for authentication which is not secure. LEAP does not establish the tunnel from the supplicant to the Authentication server before exchanging credentials. This vulnerability leads to the fake authentication server MITM attack. The second vulnerability is that when user joins or configures a PEAP network, some of the devices use the supplied assets for all supported EAP methods. The attacker will try to capture these LEAP assets using the fake AS and crack them by applying dictionary attack and may freely available tools. From the conducted experiment they proved that the Apple devices are currently vulnerable to the discussed attacks.

2.3 Evaluation of Enhanced Security Solutions in 802.11-Based Networks

Ajah Ifeyinwa Angela [4], evaluated major wireless protocols WEP, WPA/WPA2, 802.1X focusing on their mode of operation, performance, limitations, possible attacks and recommended biometric integration as a best solution for addressing threats to wlan. RC4 and AES were evaluated on the basis of time, power and memory in different devices with different key sizes, the result showed that RC4 works better in data transmission, time and memory utilisation but the AES provides better protection. WPA and 802.11i was evaluated and it was proposed that dynamic 4-way handshake avoids many of the attacks. WPA2 is better than past protocols but weakness in nonce construction and transmission in 2 steps of 4-way handshake of CCMP is vulnerable to pre-computed time trade off attack. Biometric approach to WLAN security in which user iris is scanning used by network server for authentication each time a new connection is maintained.

2.4 A Modified RSA Encryption Technique Based on Multiple public key

Amare Anagaw Ayele and Dr. Vuda Sreenivasarao [5] did an effective usage of RSA calculation utilizing two open key combines and utilizing some numerical rationale instead of sending the e esteem specifically as an open key. Because if an aggressor has chance of getting the e esteem they can specifically discover d esteem and unscramble the message. RSA is a piece figure in which the plaintext and figure content are whole numbers somewhere around 0 and $n-1$ for some n . Encryption and unscrambling are of the accompanying structure, for some plaintext piece M and figure content square C :

$$C = Mb/a \text{ mod } n$$

$$M = Cd \text{ mod } n = (Mb/a)d \text{ mod } n = Mb/ad \text{ mod } n$$

Both sender and recipient must know the estimations of n , b and a just the beneficiary knows the estimation of d . This is a public key encryption calculation with an open key of $KU = \{b,n\}, \{a\}$ and a private key of $KR = \{d,n\}$. For this calculation to be palatable for open key encryption, the accompanying prerequisites must be met:

1. It is conceivable to discover estimations of b , a , d , n such that $Mb/ad = M \text{ mod } n$ for all $M < n$.
2. It is generally simple to ascertain Mb/a and Cd for all estimations of $M < n$.
3. b is a different of a and e (which people in general key in the ordinary RSA calculation)

In this paper a calculation is proposed for RSA a system for actualizing an open key cryptosystem (RSA) utilizing two open key and some numerical relation. These two open keys are sent independently, this makes the aggressor not to get much information about the

key and not able to unscramble the message. The proposed RSA is utilized for framework that needs high security. Be that as it may, with less speed.

2.5 Light Authentication and Key Management on 802.11 with Elliptic Curve Cryptography

Suneth Namal et al. [7] proposed a novel approach called HIP-WPA of fast initial authentication (FIA) which is a combination of Host identity protocol diet Exchange (HIP-DEX) with features of WPA. Proposal provides ip layer security and provides fast authentication. HIP-DEX authenticates host by the use of elliptic curve cryptography (ECC) with two message exchange between them and therefore it improves the authentication mechanism delay by 300% compared to WPA2 protocol. Proposed mechanism can be used with any real-time application for BSS transitions and ESS handovers. HIP-WPA provides end-to-end authentication and key establishment. HIP-DEX does not provide greater forward secrecy.

2.6 An Investigation of Security Trends in Personal Wireless Network

Lu Liu et al. [8] investigated on the various freely available online tools like AIRCRACK, MDK3, KISMET, NETGEAR, WIRESHARK, RIVER etc. used for cracking wpa/wpa2 protocols and showed how easily through simple tools wpa2 can be cracked and discussed the vulnerability of wpa2 protocol. Analysis also being done about the awareness of people about the security issues related to WEP,WPA,WPA2 and their deployment of protocols in network.

2.7 Encryption using DES of ANonce in 4-Way Handshake Protocol for Authentication in WPA2

Pawan Kumar et al. [9] Presented a proposal to prevent DOS attack against 4-way handshake protocol and improve its security. There are various dos attacks such as radio frequency jamming ,disassociation, flooding, deauthentication attacks that could be implemented.WPA2 4-way handshake is vulnerable to such attacks that could result in failure or incompleteness of 4-way handshake, due to which the client's authentication process cannot complete at the access point or authenticator. To execute DOS attack the attacker can take the advantage of lack of confidentiality and integrity of message1; the AP sends the ANonce to the client which is in plaintext, the attacker can again send the fake ANonce to client before the client could send the message 2 which results in generation of SNonce again and again even sending the credentials to the fake AP .Proposed mechanism consists of the use of DES

cipher block chaining (DES-CBC) is used to encrypt the ANonce value before sending it to the client. Before the authentication process the PMK should be known to both the side i.e. AP and the supplicant. PMK is used a key in the encryption/decryption process. After obtaining ANonce value it is used for computing PTK value for proceeding steps. Brute force attack or dictionary attack could be done on the captured packet to and PMK can be obtained. Strength of the passphrase should be kept high.

2.8 Multiple Packet System: a security approach for wireless network

Richa Jain et al. [10] proposed a mechanism called Multiple Packet System (MPS).MPS operates at the application layer. This system uses five different algorithms AES, RSA, IDEA, BLOWFISH, RC4 for encryption/decryption. This technique uses 256 packets in which one combination of five algorithms is inserted, there are 4-bit to distinguish between the combinations of algorithms in place of actual names. MPS stores key list for each algorithm. MPS header consists of key selector, packet selector, and MIC shuffle selector. MPS encrypts messages with different algorithms as well as different keys. In this mechanism shuffled tables are used to shuffle MIC bits with original message. Access point (AP) will contain all the configuration files and handle the encryption/decryption process. Different MPS files are maintained for each user. This proposed mechanism handles the MIC problem with its shuffle mechanism. The entire configuration is maintained at the AP; DOS attack could create a problem. If server crashes the entire configuration will be lost since for all users it is stores at AP. More computation time will be required at AP.

2.9 Enhancement of ZigBee AND WI-FI security by a robust and fast chaotic algorithm

Bassem Bakhache et al. [12] proposed a new chaotic encryption algorithm for data encryption recommended for in use in area where security is a major concern. The proposed algorithm is composed of two perturbed piece wise linear chaotic map (PWLCM) chaotic maps. The security level increases as the sequence produced by the chaos function are very random and complex. The proposed algorithm can also implemented in security protocols like WPA2 as the security and the robust nature of the AES algorithm is maintained and the proposed algorithm provides high encryption speed.

2.10 Modeling and Analysis of IEEE802.11i WPA-PSK Authentication Protocol

K.V. Krishnam Raju et al. [13] verified the WPA-PSK authentication protocol using casperFDR tool for verification of security protocols using the SPL language. WPA-PSK is considered to less secure, so the protocol was modeled and analyzed with tool CasperFDR

then CasperFDR used to show the new security level to be achieved by the WPA-PSK. The attacks that were conceived by the tool and the message sequence are reported.

2.11 DES,AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis

Jawahar Thakur and Nagesh Kumar [14] made the comparison between the three most common symmetric key algorithms i.e. DES, AES and Blowfish. Execution of calculations under distinctive settings is demonstrated, the correlation mulls over the conduct and the execution of the calculation when diverse information burdens are utilized. The correlation is made on the premise of these parameters: rate, piece size, and key size. Reenactment project is actualized utilizing Java programming. The introduced recreation results demonstrated that Blowfish has a superior execution than other normal encryption calculations utilized. Since Blowfish has not any known security feeble focuses as such, this makes it a fantastic contender to be considered as a standard encryption calculation. AES indicated poor execution results contrasted with different calculations since it obliges all the more transforming force. Utilizing CBC mode has included additional preparing time, however general it was moderately unimportant particularly for certain application that obliges more secure encryption to generally extensive information squares.

Algorithm	Key Size(Bits)	Block Size(Bits)
DES	64	64
AES	128	128
Blowfish	128	64

Table 2: Algorithm setting

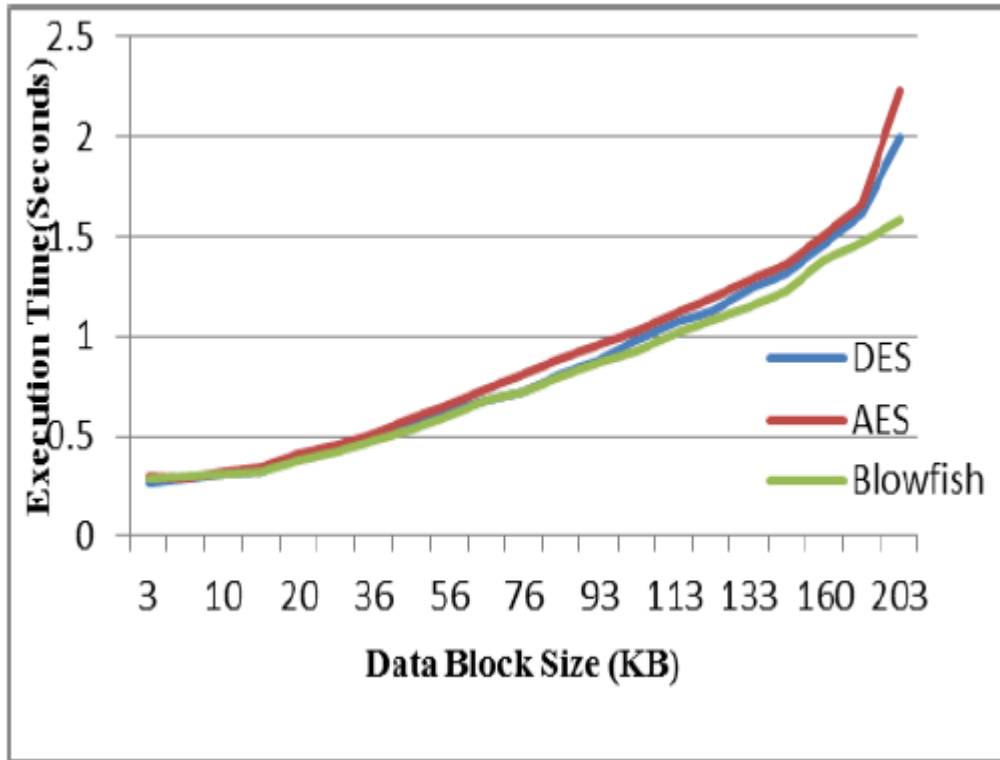


Figure 2.1: Execution results with CBC mode

The displayed diversion results exhibited that Blowfish has a predominant execution than other essential encryption estimations used. Since Blowfish has not any known security slight concentrates thusly, this makes it an extraordinary contender to be considered as a standard encryption count. AES showed poor execution results appeared differently in relation to diverse figurings since it obliges moreover taking care of power. Using CBC mode has included extra changing time, yet broad it was reasonably insignificant especially for certain application that obliges more secure encryption to a by and large immense data piece.

2.12 Security Improvement of Wi-Fi Protected Access 2

A.K.M Nazmus Sakib et al. [16] discussed the benefits and weakness of WPA2 protocol and proposed solutions and suggestions for the improvement in security of wpa2 protocol. Solution like hash based authentication protocols can be implemented. Symmetric key generation using Diffie Hellman algorithm and also shared key generation process by use of hash function provided.

2.13 Security Analysis and Authentication Improvements for IEEE 802.11i Specification

Xinyu Xing et al. [18] proposed an enhanced verification component which utilizes lopsided cryptography and achieves connection layer edge assurance. The proposed component introduces pair or open private keys, which are gotten by the utilization of Authentication-marked endorsement or a self-marked declaration. In revelation stage customer sends appeal edge to AP to perform lopsided cryptography confirmation. Next AP sends reaction outline if MAC address in the appeal casing is in the rundown of enrolled stations of AP. Reaction edge epitomizes declaration of AP and ticket. Ticket contains MAC location of AP, timestamp and MIC. Taking into account these components customer checks the character of access point and produces a precession key scrambled with open key of AP. Customer sends outline which epitomizes scrambled session key and ticket to AP. AP confirms ticket with the timestamp esteem and the MIC. On the off chance that right AP registers symmetric session key and sends an edge containing Authentication State Code. In the event that wrong MIC or terminated timestamp triggers a reaction outline with disappointment validation.

2.14 A secure 4-Way Handshake in 802.11i uses cookies

Cookie-based mechanism to derive key. Two solutions for key derivation are hash cookie and encryption cookie. The proposed mechanism resolves the problem of DOS attack. In the proposed mechanism focuses on the fact that the message 1 and message 2 are not secure in the 4 way-handshake. In the discussed mechanism the Client does not store the ANonce and PTK values instead it makes these parameters into cookie by applying the encryption procedure and sends it to AP, the client uses the secret key that is known by it only . After receiving message 2 AP derives PTK and verifies it with MIC value. Cookie is again sent to client and it decrypts it with its secret key also verifies the MIC. Since ANonce and PTK is not stores at client the intruder may not cause Dos attack via memory depletion. The problems with the proposed solution is that it is time consuming, more processing as encryption, decryption takes more time and power required is also more. Additional symmetric key is required in the procedure. In second solution is somewhat same as first; when client derives PTK it generates the hash value of PTK and the hash value of the PTK is transmitted as cookie to AP. AP receives the cookies and sends it back to the client. After getting it back the client compares the values of the cookies if its same or not. In this the client does not store SNonce and PTK.

CHAPTER 3 PRESENT WORK

In this section we will discuss the issues and the limitations that we are facing in the WPA2 protocol that motivated us to improve and enhance its security and lead to the development of the problem definition for our research work.

PBKDF2

PBKDF2 uses a pseudorandom limit, for instance, a hash, figure, or HMAC for data mystery word or passphrase nearby a salt regard and iterates the philosophy generally to convey a decided key, which can be used as a cryptographic key as a piece of coming about operations. [1] The included computational work makes mystery key part significantly more troublesome, and is known as key expanding. Exactly when the standard was formed in 2000, the proposed minimum number of cycles was 1000, yet the parameter is proposed to be extended as time goes on as CPU rates increase. Having a salt added to the watchword lessens the ability to use recomputed hashes for ambushes, and suggests that diverse passwords must be attempted independently, not in the meantime. The standard endorses a salt length of no under 64 bits. [4]

The PBKDF2 key incitement limit has five data parameters:

$PSK = PBKDF2(PRF, Password, Salt, c, skLen)$

Where:

PRF is a pseudorandom limit of two parameters with yield hLen length.

Mystery word is the master watchword from which a decided key is made.

Salt is cryptographic salt.

c is the amount of accentuations needed.

skLen is the needed length of the surmised key.

DK is the made decided key.

RSA

RSA was initially depicted in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. Open key cryptography, otherwise called uneven cryptography, utilizes two distinctive yet scientifically connected keys, one open and one private. The general population key can be imparted to everybody, though the private key must be kept mystery. [5] In RSA cryptography, both the general population and the private keys can scramble a message; the inverse key from the one used to encode a message is

utilized to decode it. This quality is one motivation behind why RSA has turned into the most broadly utilized lopsided calculation: It gives a strategy for guaranteeing the classifiedness, trustworthiness, validness and non-reputability of electronic interchanges and information stockpiling.

SHA 256

SHA-2 is an arranged of cryptographic hash limits sketched out by the NSA. SHA stays for Secure Hash Algorithm. The hash limits are investigative operations run on mechanized data; by differentiating the figured "hash" to know and expected hash regard, an individual can center the data's respectability. For ex. , enlisting the hash of a downloaded record and standing out the result from an officially circulated hash result can show whether the download has been balanced or changed with. [4] A key piece of cryptographic hash limits is their effect resistance: nobody should have the ability to find two unmistakable data values that result in the same hash yield.

SHA-2 joins gigantic changes from its predecessor, SHA-1. The SHA-2 family involves six hash limits with audits that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256. SHA-256 and SHA-512 are novel hash limits figured with 32-bit and 64-bit words, independently. They use differing development wholes and included substance constants, however their structures are for the most part in every practical sense vague, changing just in the amount of rounds.

Blowfish

Blowfish (Bruce Schneier, 1993) is a symmetric-key piece figure i.e. the same key is used for encryption as well as decryption process, composed in 1993 by Bruce Schneider and included in an extensive number of figure suites and encryption items. [7] Blowfish has a 64-bit Block size and a variable key length from 32 bits up to 448 bits. It is a 16-round Feistel cipher and uses vast key-subordinate S-boxes. In structure it looks like CAST-128, which uses settled S-boxes. Blowfish gives a decent encryption rate in programming and no powerful cryptanalysis of it has been found to date. Blowfish as a broadly useful calculation proposed as a different option for the maturing DES and free of the issues and imperatives connected with different calculations. At the time Blowfish was discharged, numerous different outlines were restrictive, hampered by licenses or were business or government mysteries. Striking highlights of the configuration incorporate key-subordinate S-boxes and an exceedingly complex key timetable.

Key features of Blowfish algorithm

- **Quick:** It encodes information on huge 32-bit microchips at a rate of 26 clock cycles every byte.
- **Reduced:** It can run in under 5K of memory.
- **Basic:** It utilizes expansion, XOR, lookup table with 32-bit operands.
- **Secure:** The key length is variable, it can be in the scope of 32~448 bits: default 128 bits key length.

It is suitable for applications where the key does not change regularly, similar to correspondence join or a programmed document encryptor. Unpatented and sans royalty. BLOWFISH is the popular encryption algorithm and very fast with high performance rate. No attack has been detected yet on this algorithm.

In later part of the section, we will discuss the objectives and the proposed methodology for the improvement in the wpa2.

3.1 Problem Formulation

Wireless technology growth has provided us with flexibility, mobility and comfort but with increased use, main issue arises of its security. Since all the data in wireless scenario travels in open medium in which any one can misuse our data and utilize the resources being provided to the authorized and authenticated user. The requirement of today is to have security of the data that is being sent into the wireless network. To provide high level of wireless security, IEEE 802.11 standard developed wlan security protocols. Security protocols are used to encrypt our confidential data and make it accessible to only the legitimate user. Such security protocols are WEP, WPA, and WPA2.

Many attacks were discovered against WEP so now a days no one deploys it as WEP can be cracked easily and any one can hack network. WPA and WPA2 are mainly in wlans to provide security. WPA is susceptible to attacks like Beck and Twes attack, Replay attack etc. Beck and Twes found flaws in TKIP which is used in WPA. So as per security concern WPA cannot be considered safe.

Till now WPA2 is the safest protocol as it uses robust AES algorithm for encryption. Still WPA2 does provide full security. The problem comes when the intruder or the attacker deploys dictionary attack and is able to derive the PTK by capturing the 4-way handshake used by WPA2 in key creation process.

Handshake consists of exchange of 4 Messages between the client and the AP. In first message AP sends its Nonce, counter and MAC address to the client. Client after receiving AP's MAC and Nonce; and with its own nonce, its MAC, PSK calculates the PTK. In second

message the client sends its MAC and its nonce value along with MIC to the AP. After receiving message 2 the AP calculates its own PTK value and verifies it with the MIC sent by the client in message 2. Message 3 is the acknowledgement from the AP side that the MIC is verified. Message 4 is that both client and AP are agreeing for key installation.

In **WPA2** main risk is the capture of the 4-way handshake. The intruder captures this handshake between the client and the AP and uses it for the purpose to calculate the PTK and can misuse the client's critical information.

In WPA2 intruder captures the 4 way handshake and derives the PSK

- PSK generates PTK and verifies PTK with MIC.
- If generated PTK is correct intruder knows the passphrase.
- Can decrypt any message which is been passed in the network.
- The security of the client is compromised.
- If MIC is not correct the failure report is sent to the AP. By which intruder comes to know that the PSK selected was not correct. AP is not susceptible to this attack as it does not generate failure reports.

So improvements need to be done to remove the flaws of WPA2 protocol enhance its strength and security of the handshake.

3.2 Objectives of Problem

The main objective is to provide security to the end users so that they could connect to the internet safely, send their confidential information, and do online transaction without any fear of losing their privacy and confidentiality. The standard of the security provided should of that level in which the security is not compromised at any cost and authentic client surf a secure net.

The main objective of this study is to:

- Analyze different kind of attacks that can be done WPA/WPA2 protocols.
- Analyze the major security flaws of WPA/WPA2 protocol. What are their weaknesses or limitations where more work needs to be done.
- Mechanism implemented in such a way that the key or passphrase should be protected from the intruder and intruder would not be able to gain possession of it at any cost.
- Provide countermeasure solutions or suggestions so that the weaknesses in the security mechanisms could be improved with their implementation.
- Reduce the handshake from 4 to 2 so the overhead of sending more messages could be reduced.

- Increase the complexity of the 4 way handshake.

3.3 Research Methodology

The improvement done in the procedure of WPA2 protocol is demonstrated in the following steps:

- Instead of 4 way handshake we will use 2 way handshakes.
- Since message 1 and message 2 both are unencrypted and the attacker can easily capture the handshake and get to know about the MAC addresses and nonce values of both AP and client.
- Public key of AP is used to encrypt the code. The public key and the private key of the AP are generated using RSA encryption technique
- Code is decrypted with the private key of AP. This ensures that it is only the possible for the AP to decrypt the code using the private key which is available with the AP alone.
- So to remove this causality of easily accessible credentials we will first create the hash (H1) of the message 1 with SHA256 and then the message is encrypted with the Blowfish algorithm; the key used is the one which is generated by the RSA. BLOWFISH encryption process will be used in encryption and decryption process.
- Decrypting the message at the client side with key generated by the RSA.
- Calculate the Hash(H2)of the message and compare it with the H1.If both the hash values same then the client derives PTK by using SNonce, its own MAC address ,AP MAC address ,ANonce and PSK.
- MIC is calculated over the message. Again encrypt it with the Blowfish and send the message2 to AP.
- Decrypt the message 2 at the AP with the code generated by the RSA.
- Calculate the PTK.
- Compare new calculated MIC with the one sent by the client.
- If both MIC are same then; PTK is used by both the parties for that session.
- If not and wrong MIC for more than 2 times in 60 sec then the connection is terminated

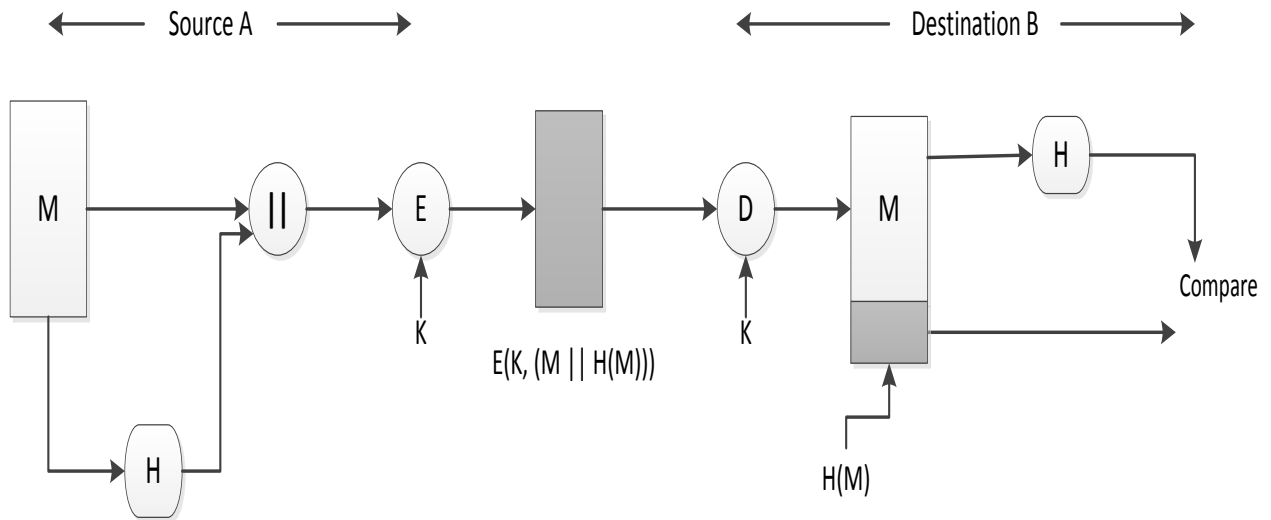


Figure 3.1: Encryption procedure

Even if the handshake will be captured and the intruder tries to calculate the PTK by sending the Wrong MIC to the client by implementing the dictionary attack with the usage of PSK values and the capturing the credentials like ANonce, AP Mac address, SNonce and client MAC address. Since the client is susceptible to MIC attacks as the AP do not generate the MIC failure reports. Same like the AP our client will not generate the MIC failure reports but will keep log maintained in its database. If the intruder tries to send wrong AP more than 2 times in 60 seconds the connection will be terminated and that user will be blocked by both the client and the AP.

Algorithm

BEGIN:

- 1) Probe request from client.
 - 2) Response from AP.
 - 3) Authentication and Association.
 - 4) Generate secret code with RSA.
 - 5) Send to AP.
 - 6) A message will be send from AP to client.
 - 7) Calculate hash1.
 - 3) Blowfish encryption technique will be used for encryption of message1.
 - 4) Code encrypted by RSA keys used as an encryption key.
- // At client side
- 5) Decrypt the message using secret key.
 - 6) Calculate hash2 of message.
 - 7) *if* (hash1=hash2), then

Calculate PTK1 and MIC1 from message1.

8) *Else* goto 14

//From Client to AP.

// for encryption of message 2 start again with same procedure.

9) Repeat Step 3 to 5

10) Calculate MIC and set count=0

if (MIC1=MIC2), then

Connection established.

11) *else if* (MIC1! =MIC2)

Count++

12) *if* (count<2), then

Connect.

13) *Else* goto 14.

14) *Else* Discard and Disconnect

END:

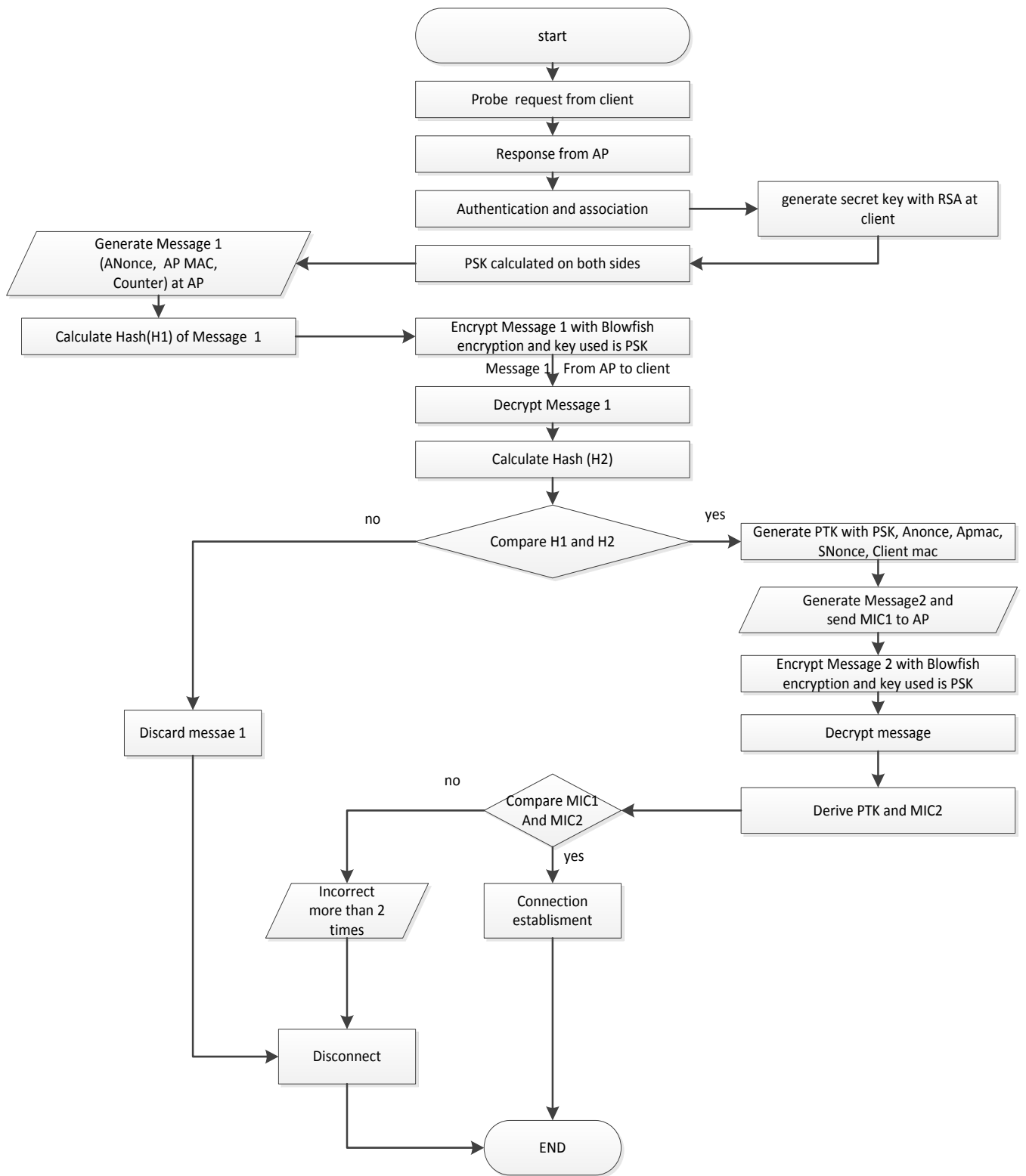


Figure 3.2: Flowchart for the steps to be followed

CHAPTER 4

RESULT AND DISCUSSION

In this section we proposed the solution that will improve and enhance the security of WPA2 security mechanism. With this proposed solution the steps in 4-handshake will be reduced in number hence the overhead will be decrease. In our implementation the security of the handshake is provided for the step one; hence the handshake will be secured from the starting step only and the new handshake will be complex, robust and more secure in nature. The computation time will increased as the encryption is applied to from the step 1 and hash is also used to define the uniqueness of the message; By applying the proposed solutions it will be difficult for the intruder to know that whether his generated key is correct or not.

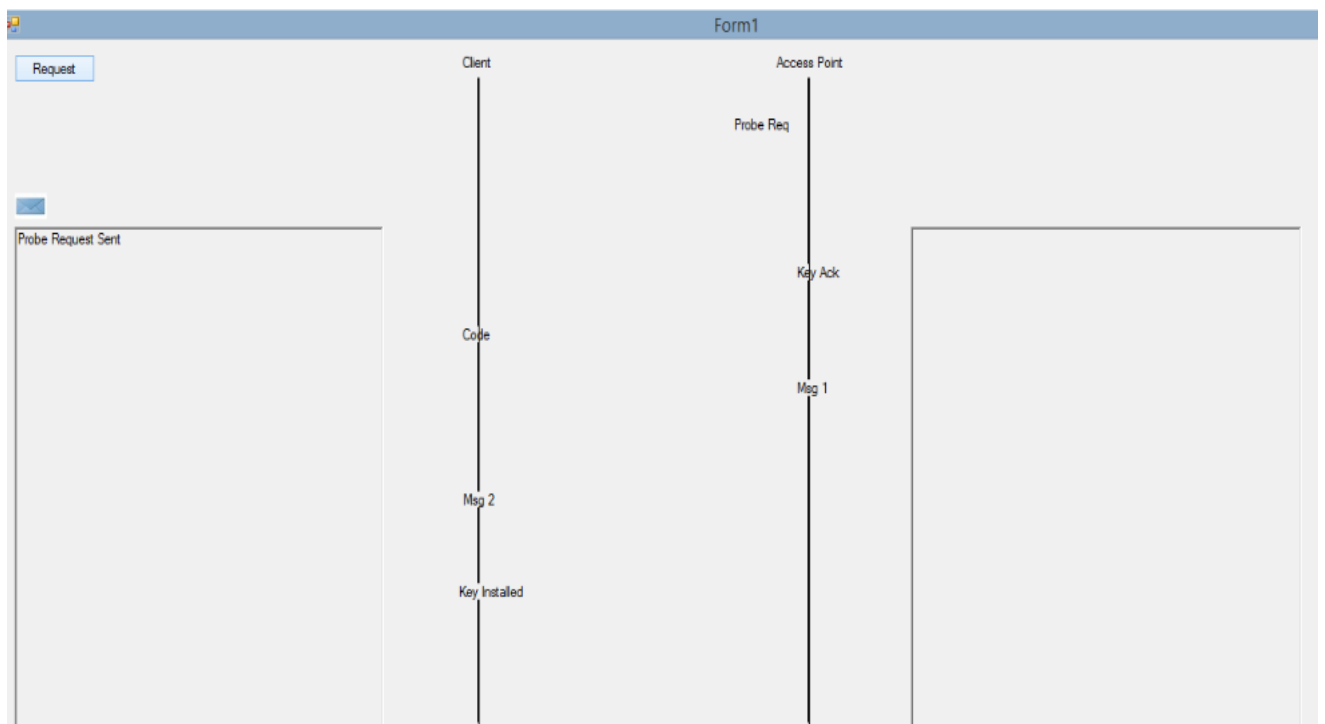


Figure 4.1 : probe request from client

To establish the connection the clients sends the probe request to the AP.

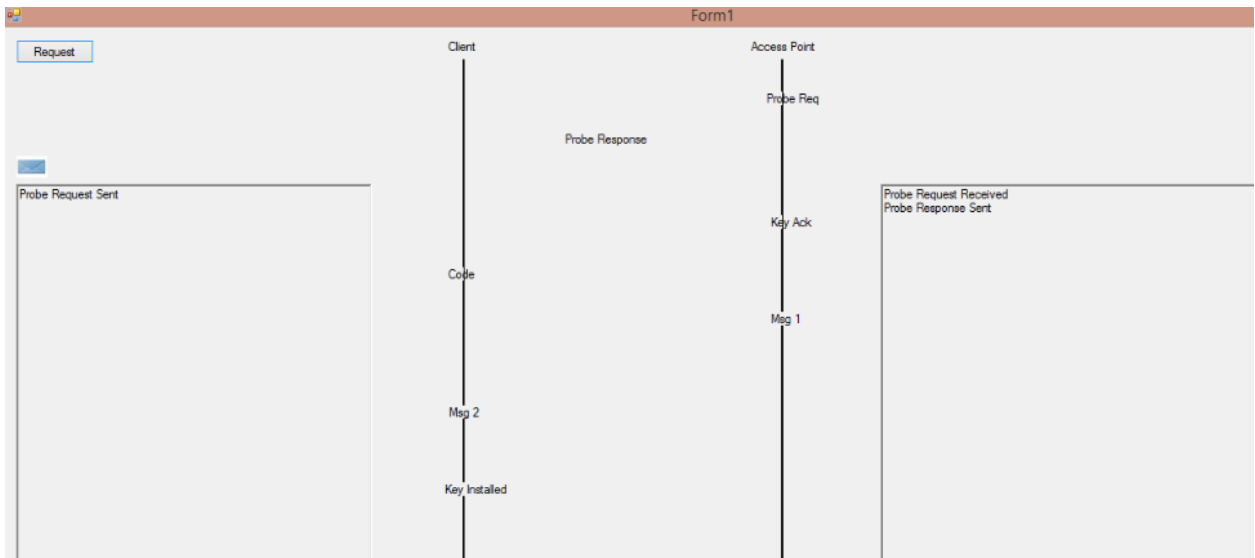


Figure 4.2: Probe response

The probe response is sent to the client by the AP.

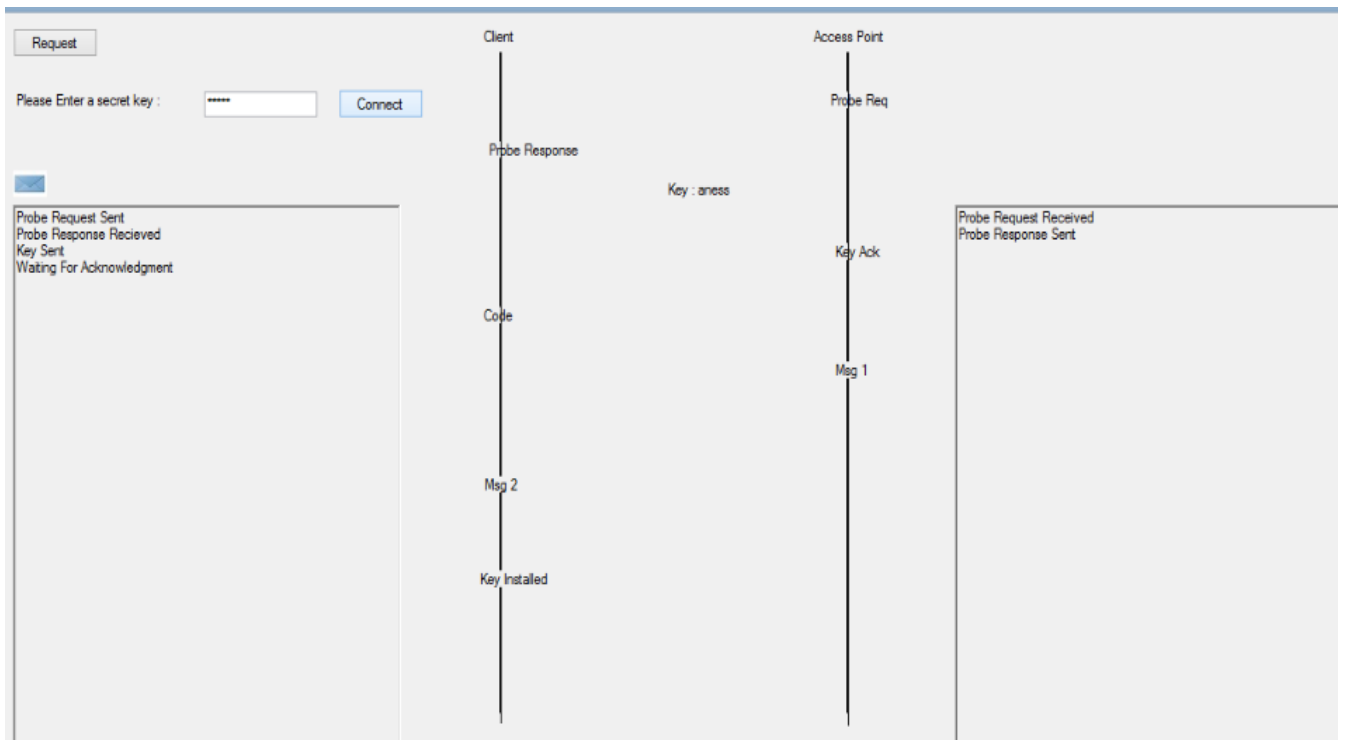


Figure 4.3: client sending code encrypted with public key of AP

The public key and the private keys are generated at the client side with RSA and are sent to the AP along with the code which is encrypted with the public key of the AP. When the code is received at the AP an acknowledgement is sent to the client.

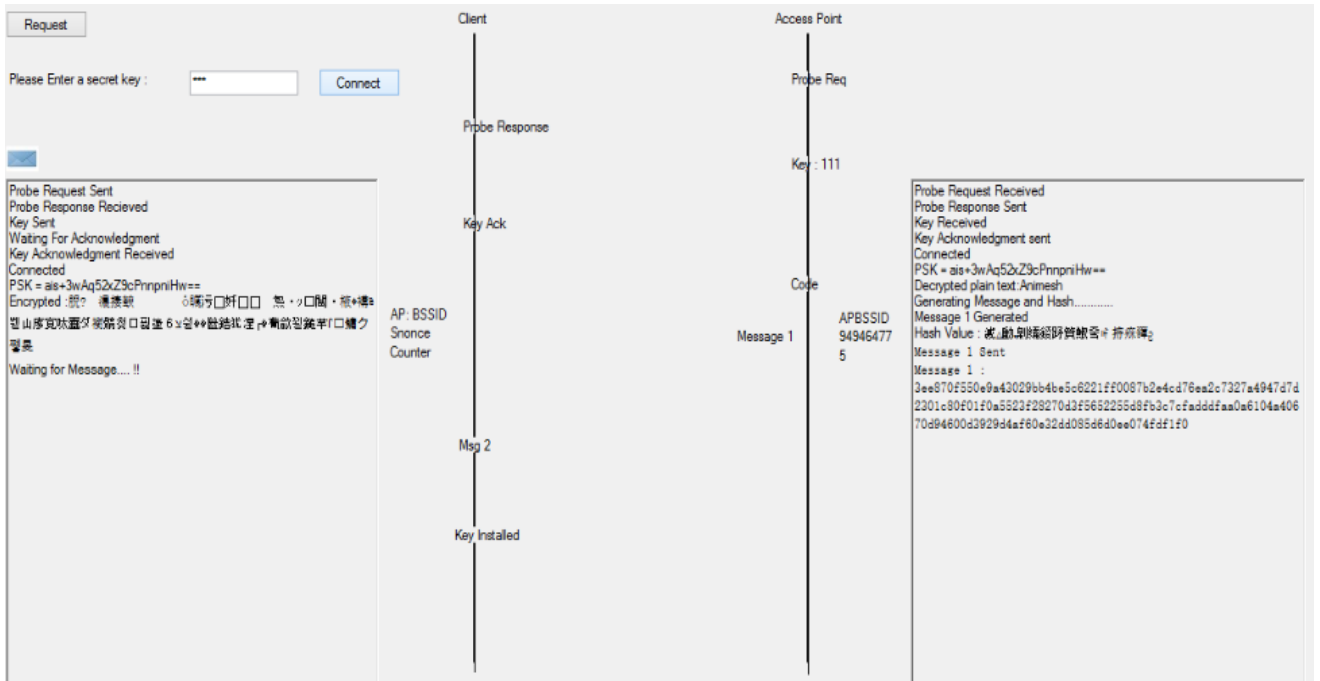


Figure 4.4: Message 1 generated at AP

After the code is received at the AP side ;the PSK is calculated on both the side with the use of PBKDF2.

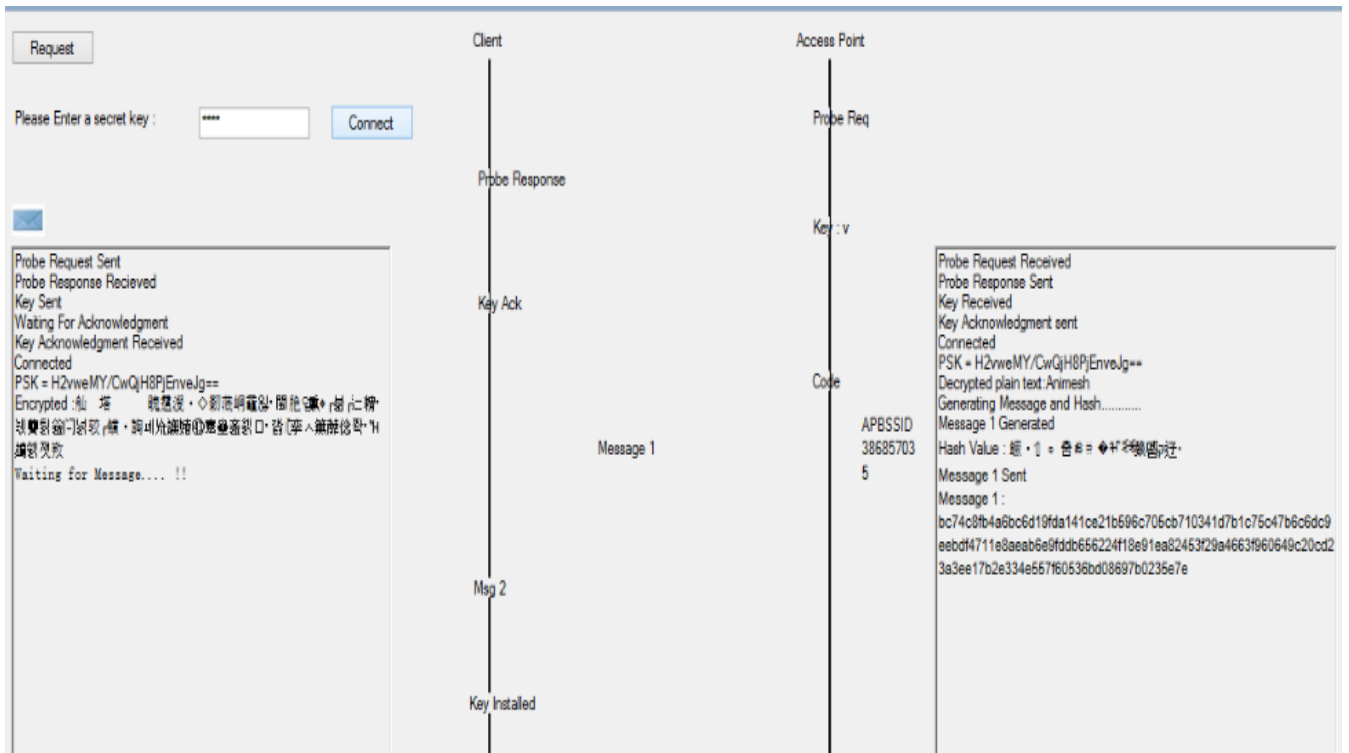


Figure 4.5: Encrypted Message 1 sent to client

The Message 1 is sent from the AP to the client client. Message 1 contains the ANonce, APMac and the counter value. To ensure the security of the Message 1 we will hash the

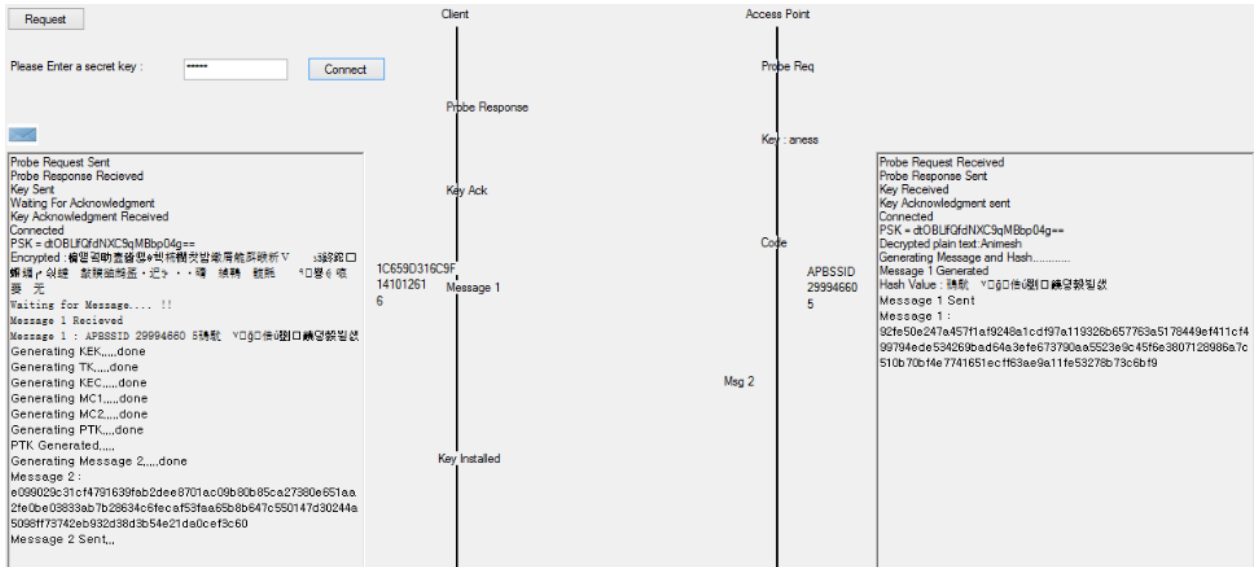


Figure 4.8: Message 2 is received at AP

When the message 2 is received at the AP, it is decrypted. PTK is derived, the MIC values are checked, if it is same as that sent from the client side; the connection is established as terminated and the key i.e. PTK is used for as the session key.

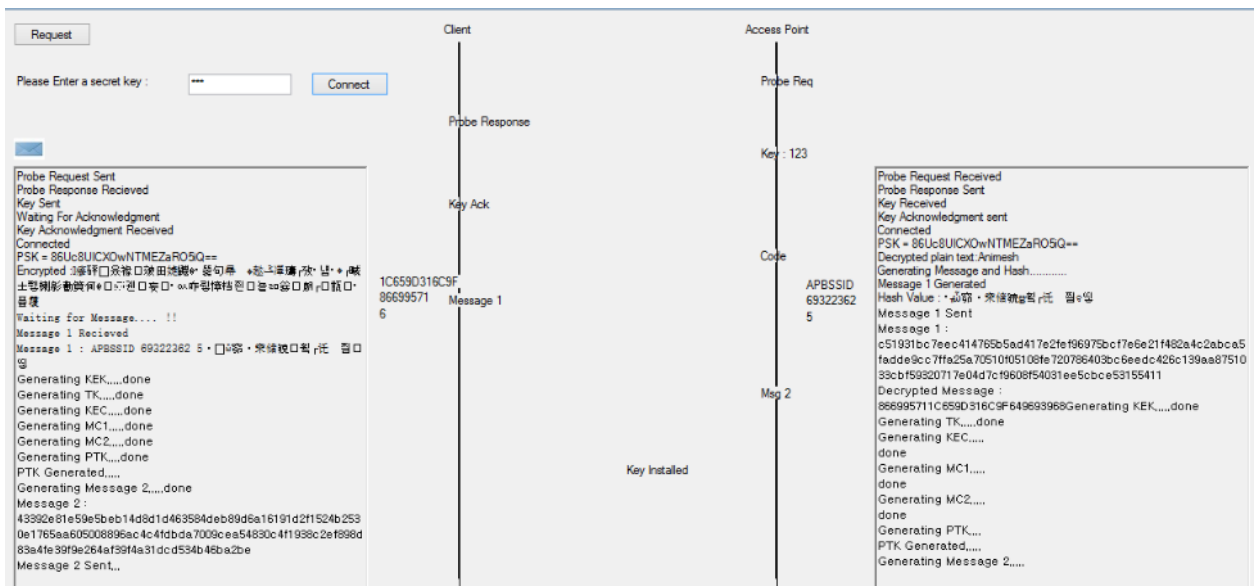


Figure 4.9: Key installed

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

Wireless medium is never secure and risk of data exposure to intruder is always there. To mitigate these security issues security mechanisms like WEP, WPA and WPA2 were developed out of which 802.11i or WPA2 protocol is best security mechanisms as it very secure and robust in nature. It uses AES-CCMP for the encryption purpose before which 4-way handshake mechanism is used to generate the session keys. People should move towards the use of WPA2 to secure their network.

Solutions provided increases the security and efficiency of the WPA/WPA2 protocol. In our research computation time of MIC will increase. The security is provided from the beginning of the handshake and the security is provided to initial steps which were not secure earlier.

This research can be used in future for further enhancement and improvement can be made to like decrease the processing time and reduce the power consumption.

REFERENCES

References of Research papers

- [1] Hang Tu, Neeraj Kumar, Debiao He, Jongsung Kim (2014), Changhoon Lee “An efficient password-based three-party authentication multiple key exchange protocol wireless mobile network”, *Published online: 10 May 2014, Springer Science*.
- [2] Pieter Robyns, Bram Bonné, Peter Quax, Wim Lamotte (2014), “ Exploiting WPA2-Enterprise Vendor Implementation Weakness through challenge Response Oracles”, *WiSec'14, July 23–25, Oxford, UK*.
- [3] Kenneth G. Paterson, Bertram Poettering, and Jacob C. N. Schuldt (2014), “Plaintext Recovery Attacks Against WPA/TKIP”, *Information Security Group Royal Holloway, University of London*.
- [4] Ajah Ifeyinwa Angela (2014), “Evaluation of Enhanced Security Solutions in 802.11-Based Networks”, *International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July*.
- [5] Amare Anagaw Ayele and Dr. Vuda Sreenivasarao (2013), “A Modified RSA Encryption Technique Based on Multiple public key”, *International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 4*.
- [6] Jean-Marc Seigneur, Carlos Ballester Lafuente, Alfredo Matos (2013), “Secure User-Friendly Wi-Fi Access Point Joining”, *IEEE*.
- [7] Suneth Namal, Konstantinos Georgantasy and Andrei Gurtov (2013), “Light Authentication and Key Management on 802.11 with Elliptic Curve Cryptography”, *IEEE*.
- [8] Lu Liu Thomas Stimpson, Nick Antonopoulos, Zhijun Ding · Yongzhao Zhan (2013) “An Investigation of Security Trends in Personal Wireless Network”, *Published online: 31 August 2013 Springer Science+Business Media New York*.
- [9] Pawan Kumar , Gopal Prasad, Atul Kumar Singh (2013) “Encryption using DES of ANounce in 4-Way Handshake Protocol for Authentication in WPA2”, *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October*.
- [10] Richa Jain, Shuchi Jani, Madhuri agrawal (2013) “Multiple Packet System: a security approach for wireless network”, *International Journal of Advanced Research in Computer Science, Volume 4, No. 3*.

- [11] Rui A. C. Ferreira (2012), “A Probability Problem Arising from the Security of the Temporal Key Hash of WPA”, *Published online: 5 July 2012, Springer, LLC*.
- [12] Bassem Bakhache, Joseph Ghazal, Safwan El Assad (2011) “Enhancement of ZigBee AND WI-FI security by a robust and fast chaotic algorithm”, *IEEE*.
- [13] V. Krishnam Raju, Dr. V. Vallikumari (2011), Dr. KVSVN Raju “Modeling and Analysis of IEEE802.11i WPA-PSK Authentication Protocol”, *IEEE*.
- [14] Jawahar Thakur, Nagesh Kumar (2011), “DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performane Analysis”, *International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com, ISSN 2250-2459, Volume 1, Issue 2*.
- [15] A.S.Rumale and Dr. D.N. Chaudhari (2011) “IEEE 802.11x, and WEP, EAP, WPA/WPA2”.
- [16] A.K.M Nazmus Sakib , Fariha Tasmin Jaigirdar , Muntasim Munim , Armin Akter (2010)“Security Improvement of Wi-Fi Protected Access 2”, *International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462 Vol. 3 No. 1*.
- [17] Martin Beck, TU-Dresden,” Enhanced TKIP Michael Attacks.
- [18] Xinyu Xing, Elhadi Shakshuki, Darcy Benoit ,Tarek Sheltami (2008), “Security Analysis and Authentication Improvements for IEEE 802.11i Specification”, *in proceedings IEEE "GLOBECOM"*.
- [19] Sung-Hyun Eum, Yae-Hoe Kim, and Hyoung-Kee Choi (2008),“A secure 4-Way Handshake in 802.11i using cookies”, *International Journal of Principles and Applications of Information Science and Technology, , Vol.2, No.1*.
- [20] Toshihiro Ohigashi and Masakatu Morii, “A Practical Message Falsification Attack on WPA”.

Reference to webpages

- [1] <http://anandam.name/pbkdf2/>
- [2] http://compnetworking.about.com/od/wirelessfaqs/f/wep_keys.htm
- [3] www.cwnp.com
- [4] <http://en.wikipedia.org/wiki/PBKDF2>
- [5] <http://iitd.vlab.co.in/?sub=66&brch=184&sim=1147&cnt=1>
- [6] <http://searchsoftwarequality.techtarget.com/definition/cryptography>
- [7] <http://www.splashdata.com/splashid/blowfish.htm>
- [8] <http://science.opposingviews.com/wpa2-encryption-2469.html>
- [9] <http://thebestwirelessinternet.com/wep-vs-wpa.html>

[10] www.og150.com

Reference to Books

- [1] William Stallings, "Cryptography And Network Security Principles And Practice" ,Fifth Edition;2011

List of Abbreviations

A

- AES Advance Encryption Standard
- AP Access Point
- AS Authenticated Server

C

- CCMP Counter Cipher Mode with Block Chaining Messages

D

- DES Data Encryption Standard
- DOS Denial of Services

E

- EAP Extensive Authentication Protocol

I

- ICV Integrity Check Value

K

- KCK Key Conformation Key
- KEK Key Encryption Key

M

- MAC Media Access Control
- MIC Message Integrity Check
- MPDU MAC Protocol Data Unit
- MSDU MAC Service Data Unit

P

- PBKDF2 Password Based Key Derivation Function 2
- PSK Pair-Wise Shared Key
- PTK Pairwise Transient Key

Q

- QOS Quality of Service

R

- RADIUS Remote Authentication Dial In User Service

T

TK Temporary Key

TKIP Temporal Key Integrity Protocol

W

WPA WI-FI Protected Access

WPA2 WI-FI Protected Access 2

WEP Wired Equivalent Privacy