ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of the people who made it possible, whose constant guidance and encouragement crowned the efforts with success.

We would like to thank the **Management** of **BNM Institute of Technology** for providing such a healthy environment for the successful completion of the Project work.

We would like to express our thanks to the Director **Prof. T. J. Rama Murthy** and the Principal **Dr. Krishnamurthy G N** for their encouragement that motivated us for the successful completion of Project work.

It gives us immense pleasure to thank **Dr. Sahana D Gowda,** Professor and Head of Department for her constant support and encouragement.

Also, we would like to express our deepest sense of gratitude to our Project guide **Dr. Divyashree B A,** Professor, Department of Computer Science & Engineering for her constant support and guidance throughout the Project work.

We would also like to thank our Project coordinator **Smt. Savitha G,** Associate Professor, Department of Computer Science & Engineering for her guidance throughout the Project work.

We also thank the BNMIT Library for helping us find research papers and related references.

We acknowledge the entire staff members of Computer Science and Engineering Department for their time and support. Their timely co-operation ensured a smooth learning for the project.

Sumit Kumar
Venkatesh Prasad S
Vinay B
Yoganand G K

ABSTRACT

In 802.11ad Infrastructure BSS, AP provides the data service to multiple Stations in DTI interval. In DTI, Data services are provided by three mechanism EDCA, SPCA and dynamic to provide the bandwidth allocation to the STA's. The main focus is on SPCA mechanism to provide the bandwidth allocation to the STA's in the Infrastructure BSS. Implementation of this project should contain an AP and three Stations to resemble the Infrastructure 802.11ad BSS. Three stations request the bandwidth allocation to AP through Service Period Request (SPR) frames. AP will respond back with admitted bandwidth through Grant frames to the Connected STA's. Effectiveness of this scheduling algorithm should be proved by three STA requesting more bandwidth than the available bandwidth in the AP.

In 802.11ad Infrastructure BSS, AP provides the data integrity through Robust Security Network Association (RSNA) using (Galois/Counter mode with GMAC Protocol (GCMP). The focus is on protocol implementation of four-way handshake frames exchange between AP and STA. By four-way handshake, AP provides the group key to the STA and authenticates the STA for further data transactions. It requires detailed understanding of the RSNA protocol along with the frames used to exchange between AP and STA. Implementation of this project should require an AP and three STA to resemble the Infrastructure BSS. Effectiveness of this project, could be the ability to demonstrate ANonce and SNonce negotiations and keys generation.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

Chapter 1

INTRODUCTION

1.1 Introduction to Wireless networks

Wireless networking is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.

A wireless local-area network (LAN) uses radio waves to connect devices such as laptops to the Internet and to a business network and its applications. When a laptop is connected to a Wi-Fi hotspot at a cafe, hotel, airport lounge, or other public place, it is connecting to that business's wireless network.

It is believed that wired networks were faster and more secure than wireless networks. But continual enhancements to wireless networking standards and technologies have eroded those speed and security differences. The figure 1.1 shows a Wireless Network system consisting of an Access Point (AP) enabling the clients to connect wirelessly to the network.

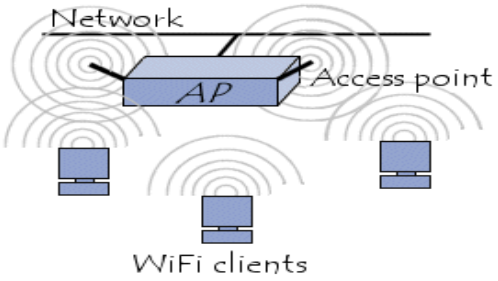

Figure 1.1: A Wireless Network System

1.1.1 How does Wireless Networks work?

Moving data through a wireless network involves three separate elements: the radio signals, the data format, and the network structure. Each of these elements is independent of the other two, so all three must be defined when a new network is laid. In terms of the OSI reference model, the radio signal operates at the physical layer, and the data format controls several of the higher layers. The network structure includes the wireless network interface adapters and base stations that send and receive the radio signals. In a wireless network, the network interface adapters in each computer and base station convert digital data to radio signals, which they transmit to other devices on the same network, and they receive and

convert incoming radio signals from other network elements back to digital data. Each of the broadband wireless data services use a different combination of radio signals, data formats, and network structure.

The pros of using wireless networks:

- **Convenience**: Network resources can be accessed from any location within the wireless network's coverage area or from any Wi-Fi hotspot.
- **Mobility**: Wireless networks eliminate the concept of stationary nodes. Since there is no real usage of wires or cables for communication, the nodes can be mobile and roam freely within the Wi-Fi range.
- **Productivity**: Wireless access to the Internet encourages collaboration.
- **Easy setup**: There is absolutely no need to string cables, so installation can be quick and cost-effective.
- **Expandable**: Wireless networks can easily be expanded with existing equipment, while a wired network might require additional wiring.
- **Security**: Advances in wireless networks provide robust security protections.
- **Cost**: Because wireless networks eliminate or reduce wiring costs, they can cost less to operate than wired networks.

1.1.2 Wireless Data Services

Since radio signals move through the air, a network connection from any place within the range of the network base station’s transmitter can be established. It is not necessary to use a telephone line, television cable, or some other dedicated wiring to connect a computer to the network. Therefore, a radio (or wireless) network connection is often a lot more convenient than a wired one.

This does not imply that wireless is always the best choice. A wired network is usually more secure than a wireless system because it is a lot more difficult for unauthorized eavesdroppers and other snoops to monitor data as it moves through the network, and a wired link does not require as many complex negotiations between the sender and receiver on protocols and so forth.

So now there are a bunch of radio transmitters and receivers that all operate on the same frequencies and all use the same kind of modulation (Modulation is the method a radio uses to add some kind of content, such as voice or digital data, to a radio wave). The next step

is to send some network data through those radios. Several different wireless data systems and services are available to connect computers and other devices to local networks and to the internet, including Wi-Fi, WiMAX, and a handful of services based on the latest generations of cellular mobile telephone technology.

1.2 Introduction to Wi-Fi

Wi-Fi was originally intended to be a wireless extension of a wired LAN, so the distances between Wi-Fi base stations and the computers that communicate through them are limited to about 100 feet (35 meters) indoors or up to 300 feet (100 meters) outdoors, assuming there are no obstructions between the access point and the computer.

Wi-Fi is a technology that allows electronic devices to connect to a wireless LAN (WLAN) network, mainly using the 2.4 gigahertz and 5 gigahertz radio bands. A WLAN is usually password protected, but may be open, which allows any device within its range to access the resources of the WLAN network.

The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network" (WLAN) product based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards. "Wi-Fi" is a trademark of the Wi-Fi Alliance. The "Wi-Fi Certified" trademark can only be used by Wi-Fi products that successfully complete Wi-Fi Alliance interoperability certification testing.

Devices which can use Wi-Fi technology include personal computers, video-game consoles, smartphones, digital cameras, tablet computers and digital audio players. Wi-Fi compatible devices can connect to the Internet via a WLAN network and a wireless access point.

Wi-Fi is less secure than wired connections, such as Ethernet, precisely because an intruder does not need a physical connection. Unencrypted Internet access can easily be detected by intruders. Because of this, Wi-Fi has adopted various encryption technologies. The first encryption technique WEP proved easy to break. Higher quality protocols (WPA, WPA2) were added later. An optional feature, called Wi-Fi Protected Setup (WPS), had a serious flaw that allowed an attacker to recover the router's password.

1.2.1 Wi-Fi Standards

The 802.11 standard is defined through several specifications of WLANs. It defines an over-the-air interface between a wireless client and a base station or wireless clients.

There are several standards/specifications in the 802.11 family: -

- **802.11**- This pertains to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS).
- **802.11a**- This is an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band. 802.11a employs the orthogonal frequency division multiplexing (OFDM) encoding scheme as opposed to either FHSS or DSSS.
- **802.11b**- The 802.11 high rate Wi-Fi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission (with a fallback to 5.5, 2, and 1 Mbps depending on strength of signal) in the 2.4-GHz band. The 802.11b specification uses only DSSS. 802.11b was actually an amendment to the original 802.11 standard to permit wireless functionality to be analogous to hard-wired Ethernet connections.
- **802.11g**- This pertains to wireless LANs and provides up to 54 Mbps in the 2.4-GHz band.
- **802.11n**- It's purpose is to significantly increase throughput in both the 2.4GHz and the 5GHz frequency range. It uses multiple antennas to increase data rates. The baseline goal of the standard was to reach speeds of 100Mbps. It is estimated that the speeds might reach a staggering 600Mbps (practically much slower). It uses Multiple Input Multiple output(MIMO), which is the key for the high speeds.
- **802.11ac**- This operates in the 5GHz spectrum. It provides data transmission speeds up to 1.3Gbps. It is backward compatible with 802.11n standard. This standard provides constant data transmission speed for a higher distance.
- **802.11ad**- The Wireless Gigabyte alliance (Wi-Gig) was formed to promote the 802.11ad standard. It operates in the 60GHz frequency spectrum. It provides a very high data throughput of up to 6Gbps.

The figure 1.2 draws a comparison between the various Wi-Fi standards and shows the operating range of frequency and the maximum data transfer rates they offer. These standards operate in either of unlicensed frequency bands 2.4GHz and 5GHz. This results in interference between signals of various wireless devices like Bluetooth devices, microwave ovens etc. On the other hand, the standard 802.11ad operates in the unlicensed frequency band 60GHz. It provides

extremely high data transfer speeds up to 7Gbps in an interference free environment. This standard is applicable for short distance transmission about 20 feet.

Standard	Maximum Speed	Frequency
802.11 (legacy)	1.2 Mbps	2.4 GHz
802.11a	54 Mbps	5.8 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	150 Mbps	2.4 & 5 GHz
802.11ac	800 Mbps	5 GHz

Figure 1.2: Comparison of Wi-Fi standards

1.3 Security in Wireless Networks

Security is more of a concern in wireless networks because of the following reasons:

- **No inherent physical protection.** Physical connections between devices are replaced by logical associations. Sending and receiving messages do not need physical access to the network infrastructure such as cables, hubs and routers.
- **Broadcast Communication.** Wireless networks use radio waves which has a broadcast nature. i.e. Transmissions can be overheard by anyone within the range.
- Eavesdropping is easy.
- Injecting bogus messages into the network is easy.
- Replaying previously recorded messages is easy.
- Illegitimate access to the network and its resources is easy.
- Denial of Service is easily achieved by jamming

1.3.1 Wired Equivalent Privacy(WEP)

It was introduced as part of the original 802.11 standard. Standard 64-bit WEP uses a

40-bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 (Rivest Cipher 4) key. A 64-bit WEP key is usually entered as a string of 10 hexadecimals (base 16) characters (0–9 and A–F). Each character represents 4 bits, 10 digits of 4-bits each gives 40-bits; adding the 24-bit IV produces the complete 64-bit. The only advantage of WEP is that all Wi-Fi equipment supports it. The figure 1.3 shows the encryption and decryption of data in WEP.

The biggest problem with WEP is the static key which does not change during a session. The length of the key (64-bit, 128-bit and 256-bit WEP) only extends the time needed to crack the wireless network. It is really easy to crack WEP. It is no longer encouraged to use WEP for securing Wi-Fi.

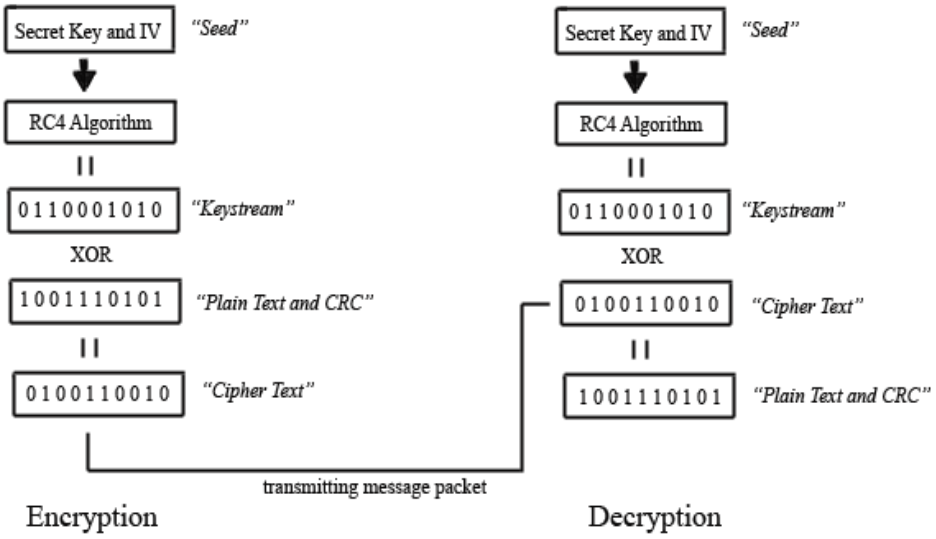

Figure 1.3: Encryption and Decryption of data in WEP

Limitations of WEP:

- **No mutual authentication** - Only clients can authenticate, not access points. This can lead to rogue APs.
- **No user-level authentication** - Static WEP key stored on device. This is a problem if the device is stolen or otherwise accessed without permission.
- **Re-use of static key** - The same key used for authentication and encryption.

1.3.2 Wi-Fi Protected Access(WPA)

A new standard from the Wi-Fi Alliance that uses the 40 or 104-bit WEP key, but it changes the key on each packet. The changing key functionality is called the Temporal

Key Integrity Protocol (TKIP). WPA provides strong user authentication based on 802.1x and the Extensible Authentication Protocol (EAP). Instead of authorizing computers based solely on their MAC address, WPA can use several other methods to verify each computer's identity. This makes it more difficult for unauthorized systems to gain access to the wireless network. Figure 1.4 illustrates the TKIP process to generate RC4 keys

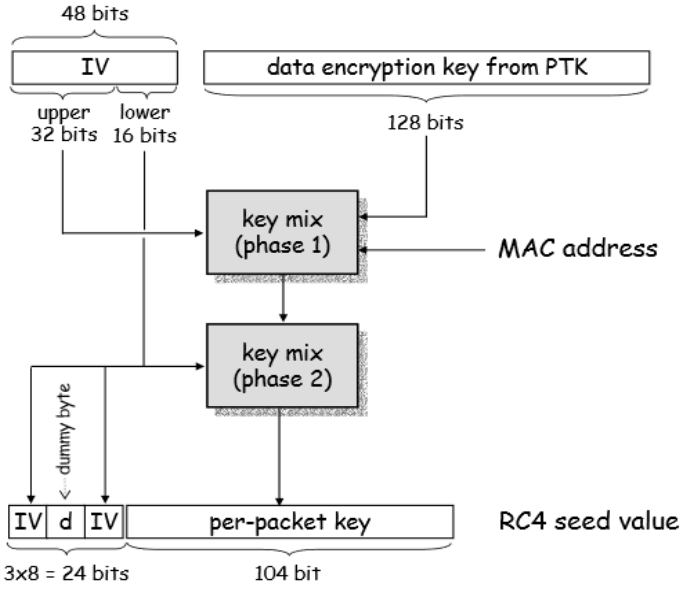

Figure 1.4: TKIP generating RC4 keys in WPA

Drawbacks of WPA:

- The biggest issue with WPA is its incompatibility with legacy hardware and older operating systems.
- WPA also has a larger performance overhead and increases data packet size leading to longer transmission.

1.3.3 WPA with Pre-Shared Key (WPA2-PSK)

The most significant enhancement to WPA2 over WPA is the use of the Advanced Encryption Standard (AES) for encryption. A Pre-Shared Key(PSK) is used to secure the network. Using TKIP (for Temporal Key Integrity Protocol), that pass phrase, along with the network SSID, is used to generate unique encryption keys for each wireless client. WPA2 also improves the security of Wi-Fi connections by requiring use of stronger wireless encryption than what WPA requires. WPA2 has replaced WPA. WPA2 requires more processing power than WPA. This is the only drawback of WPA2.

LITERATURE SURVEY

Chapter 2

LITERATURE SURVEY

WiMAX Technology is one of the emerging Wireless Technology that provides high speed data and telecommunication services. It provides several services such as data, voice and video including different classes of Quality of Services (QoS), which in turn were defined by IEEE 802.16 standards. Scheduling in WiMAX became one of the most challenging issues, since it was responsible for distributing available network resources among all users. This leaded to the demand of constructing and designing highly efficient scheduling algorithms in order to improve the network utilization, to increase the network throughput, and to minimize the end-to-end delay. A brief study to measure the performance of several scheduling algorithms in WiMAX, which were Strict Priority algorithm (SP), Round-Robin (RR), Weighted Round Robin (WRR), Weighted Fair Queuing (WFQ) and Self-Clocked Fair (SCF).

WiMAX is based on the standard IEEE 802.16, which consist of one Base Station (BS) and one or more Subscriber Stations(STAs). The BS is responsible for data transmission from STAs through two operational modes: Mesh and Point-to-multipoint (PMP). This transmission can be done through two independent channels: The Downlink Channel (from BS to STA) which is used only by the BS, and the Uplink Channel (from STA to BS) which is shared by all STAs. In Mesh mode, STA can communicate by either the BS or other STAs. In this mechanism the traffic can be routed not only by the BS but also by other STAs in the network. This means that the uplink and downlink channels are defined as traffic in both directions: to and from the BS. In the PMP mode, STAs can only communicate through the BS, which makes the provider capable of monitoring the network environment to guarantee the Quality of Service (QoS) to the customers. An essential principle of WiMAX technology is that it is connection oriented. Connection oriented means that before the STA can start to send or receive data, it must register itself to the BS in order to initialize QoS needs with the BS. Voice over IP is one of the most important applications for WiMAX, order to support bidirectional voice conversation. Since its introduction, VoIP has been building up more and more prevalence and some services have widened their coverage [5].

Various scheduling algorithms such as Strict Priority scheduling, Round-Robin scheduling, Weighted Round-Robin scheduling, Weighted Fair Queueing and Self-Clocked Fair Queueing have

been reviewed and the working of their respective schedulers have been studied in case of data communication [5]. It has been analyzed that the Strict Priority scheduling algorithm does not perform as well as compared to other scheduling algorithms due to the reason of its bandwidth starvation.

Security is one of the most important challenge which is to be handled in the era of wireless technology these days. Current security standards have shown that security is not keeping up with the growing use of wireless technology. Every now and then, a new vulnerability comes into existence to the existing wireless standards. Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a network while being mobile has great benefits. However, wireless networking has many security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems are commonly used to enforce wireless security policies. The risks to users of wireless technology have increased as the service has become more popular. However, there are many security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless technology. Cracking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge [7].

The IEEE 802.11i wireless networking standard with respect to data confidentiality, integrity, mutual authentication and availability are the main concerns. Under the threat model, 802.11i appears to provide effective data confidentiality and integrity when CCMP is used. Furthermore, 802.11i may provide satisfactory mutual authentication and key management. Although there are some potential implementation oversights that may cause severe problems. Since the 802.11i does not emphasize availability, several Denial of Service attacks are possible. The review of the known DoS attacks on unprotected management frames and EAP frames, the ways of mitigating them in 802.11i. The practicality of a DoS attack against Michael MIC Failure countermeasure is discussed and improvements are proposed. Two new DoS attacks and possible repairs are identified: RSN IE Poisoning and 4-Way Handshake Blocking. Finally, some tradeoffs in failure-recovery strategies are

discussed and an improved variant of 802.11i is proposed to address all the discussed vulnerabilities.

802.11i appears to provide effective data confidentiality and integrity when CCMP is used. This requires a legacy WEP user to upgrade the hardware. Furthermore, 802.11i adopts a RSNA establishment procedure for mutual authentication and key management, which appears to be satisfactorily secure. However, several vulnerabilities might arise in a real implementation. If the mutual authentication mechanism is not implemented appropriately, there might be a Man-in-the-Middle attack that reveals the shared secret. If a passphrase is used to generate a 256-bit PSK, an adversary might be able to find the passphrase through dictionary attacks. An adversary is also able to discover the shared RADIUS secret through dictionary attacks. Furthermore, if Pre-RSNA and RSNA algorithms are implemented in a system simultaneously without careful considerations, an adversary is able to perform a Security Level Rollback Attack to force the communicating peers to use WEP, which is completely insecure. Moreover, if a wireless device is implemented to play the role of both the authenticator and the supplicant, an adversary can construct a reflection attack on the 4-Way Handshake. This scenario naturally appears in ad hoc networks. Availability is another important security property in wireless networks.

Since availability is not the primary design goal, 802.11i appears vulnerable to DoS attacks even if RSNA is implemented. The known DoS attacks and proposed solutions appropriate to 802.11i can be reviewed. It appears that a better way to eliminate management frame vulnerabilities is to authenticate them. First, analyze the practicality of the DoS attack on the Michael algorithm countermeasures. Here, eliminating re-keying and updating the TSC carefully appear to provide significant improvements. Second, describe a new DoS attack through RSN IE poisoning. Several repairs are discussed. Relaxing the condition for RSN IE verification seems the preferred approach because it only requires minor modifications to the algorithm. Third, a DoS attack on the unprotected Message 1 of the 4-Way Handshake is described and the corresponding defenses are proposed. The tradeoffs in the failure-recovery strategy are discussed and an efficient failure recovery for 802.11i is proposed, based on the characteristics of wireless networks. Finally, integrate all the improvements to construct a DoS resistant variant of the 802.11i protocols [4].

Wireless network, whether it’s ad-hoc or at enterprise level is vulnerable due to its features of open medium, and usually due to weak authentication, authorization, encryption, monitoring and accounting mechanisms. Various wireless vulnerability situations as well as the minimal features that

are required in order to protect, monitor, account, authenticate, and authorize nodes, users, computers into the network are examined. Also, aspects of several IEEE Security Standards, which were ratified and which are still in draft are described.

This combination of peripheral devices, encryption standards, authentication procedures and monitoring solutions will ensure extreme security for your network. After clients become part of the network, WIPS and WIDS should constantly monitor, and log activity. Even if clients are authorized to do some specific tasks within a network, it doesn't mean they will not try to harm or compromise other part of their boundaries. Wireless communication, data transmission is fully opened for attackers which could be located far away by using big antennas, thus strong encryption, privacy ensuring, integrity check must persist constantly. Different 802.11 security standards are consistently developing by introducing new features, schemas, possible additional hardware which adds security to wireless communication. Taking into account aforementioned the following strategy for establishing wireless secure environment is suggested. Before making a purchase of hardware or deciding which software should be used, prior assessment should be done, in order to avoid misconfiguration and additional money wastage. In perfect world the strongest authentication like 802.1Xwith AES should be used, 4-way handshake with CCMP/AES, other authentication mechanism based on EAP with tunneling or certificate based, in other word RSNA-capable devices must be used. In situations, where "legacy" devices could not be exchanged pre-RSNA authentication methods with appropriate encryption could be used, but with present processing power, you should purchase RSNA-capable devices; The 802.11-2012 security standard will consume all previously developed security solutions, including roaming, high-throughput, customization, data transmission speed, which is perfect situation could exceed 7Gbit/s, almost instant data transmission. Software- or hardware based monitoring solution, different WIDS/WIPS should constantly monitor your environment, by using different switches, methods, techniques you could even protect your network against zero-day attack, based on network behavioral solution. Even if one invests millions into security, the weakest link in any case will be human. In order to strengthen network security, all users without exceptions should be well trained, policies should be signed, questions answered [6].

To avoid these threats and to improve the security of the wireless networks various companies collaborated to make the Wi-Fi alliance to make the robust security protocol. Initially they came with the new security protocol for wireless networks known as Wi-Fi Protected Access (WPA). The WPA protocol implements the majority of the IEEE802.11i standard, and was intended as an intermediate measure to take the place of WEP. WPA uses the Temporal Key Integration

Protocol (TKIP) algorithm for encryption. TKIP is a security protocol used in the IEEE 802.11 wireless networking standard. TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as a solution to replace WEP without requiring the replacement of legacy hardware. This was because the breaking of WEP had left Wi-Fi networks without viable link-layer security, and a solution was required for already deployed hardware.

WPA has the following advantages:

- A cryptographic Message Integrity Code (MIC), to defeat forgeries. Message Integrity Code (MIC) is computed to detect errors in the data contents, either due to transfer errors or due to purposeful alterations. This prevents man in the middle attack, denial of service attack.
- A new Initialization Vector (IV) sequencing discipline, to remove replay attacks from the attacker's arsenal.
- A rekeying mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse. Thus provides security against eavesdropping attacks.

Although the WPA protocol has increased wireless security to a great extent, it also has some problems:

- Weakness in Passphrase Choice in WPA Interface: This weakness was based on the Pair Wise Master key (PMK) that is derived from the concatenation of the passphrase, Service Set Identifier(SSID), length of the SSID and nonce (a number or bit string used only once in each session).
- Possibility of the Brute Force Attack: Brute Force is considered to be a passive attack in which the intruder will generate every possible permutation in the key and try to decrypt the encrypted message with each generated permutation, and validate the output by means of cross comparison with words, file header and any other data.
- Placement of MIC: It is considered a problem because it can be used by any hacker in validating the contents of the decrypted message combined with the brute force attack. After WPA protocol, Wi-Fi Protected Access2 (WPA2) protocol was designed. The WPA2 uses the more robust encryption algorithm known as Advanced Encryption Standard (AES). There are various advantages of WPA2.

Advantages of WPA2 include:

- WPA2 supports IEEE 802.1X/EAP (Extensible Authentication Protocol) authentication or Pre Shared Key (PSK) technology. A pre-shared key or PSK is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. Such systems almost always use symmetric key cryptographic algorithms. Thus removing the passphrase choice problem of WPA.
- It also includes a new advanced encryption mechanism using the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) called the Advanced Encryption Standard (AES). Thus providing security against most of the attacks encountered due to weak encryption key. Although WPA2 uses more robust security algorithm i.e. AES [7].

SYSTEM REQUIREMENTS

Chapter 3

SYSTEM REQUIREMENTS

3.1 HARDWARE REQUIREMENTS

- GCMP supported Access Point.
- Service Stations like computers.

3.1.1 Access Points

A wireless access point (WAP) is a networking hardware device that allows a WiFi compliant device to connect to a wired network. The WAP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself. A WAP is differentiated from a hotspot, which is the physical location where Wi-Fi access to a WLAN is available.

A wireless access point allows network users to add devices that access the network with few or no cables. A WAP normally connects directly to a wired Ethernet connection and the WAP then provides wireless connections using radio frequency links for other devices to utilize that wired connection. Most WAPs support the connection of multiple wireless devices to one wired connection. Modern WAPs are built to support a standard for sending and receiving data using these radio frequencies. Those standards, and the frequencies they use are defined by the IEEE. Most APs use IEEE 802.11 standards.

3.1.2 Service Stations

In computer networking, a supplicant is an entity at one end of a point-to-point LAN segment that seeks to be authenticated by an authenticator attached to the other end of that link. The IEEE 802.1X standard uses the term "supplicant" to refer either to hardware or to software. In practice, a supplicant is a software application installed on an end-user's computer. The user invokes the supplicant and submits credentials to connect the computer to a secure network. If the authentication succeeds, the authenticator typically allows the computer to connect to the network. There can be an optional hub. The supplicant can connect straight to the authenticator itself. In a hub or an unmanaged switch, the uplink port (the port to which the hub is connected) should be

set in multi-session mode.

A supplicant, in some contexts, refers to a user or to a client in a network environment seeking to access network resources secured by the IEEE 802.1X authentication mechanism. in reality, the interaction takes place through a personal computer, an Internet protocol (IP) phone, or similar network device. Each of these must run supplicant software that initiates or reacts to IEEE 802.1X authentication requests for association.

3.2 SOFTWARE REQUIREMENTS

- Operating System: Linux / Windows
- GNU Compiler Collection (GCC) / Cygwin
- Connectify Hotspot 2016

SYSTEM ANALYSIS

Chapter 4

SYSTEM ANALYSIS

4.1 EXISTING SYSTEM

Authentication of service stations is a vital requirement in a wireless network. An access point needs to service only those stations which are authenticated to ensure proper confidentiality and integrity of data. The existing system for authentication is WPA and WPA2/PSK.

4.1.1 WPA

Wireless protected access (WPA) was the replacement for WEP protocol which was developed to overcome its disadvantages and yet it quickly became obsolete giving birth to WPA2 protocol. The only disadvantage of WPA is it incurs more processing power, resulting in delay in generation of keys.

4.1.2 WPA2/PSK

WPA2-PSK was designed to overcome the disadvantages of WPA. Security for the data that is being transferred from the access point to the station and from the station to access point is necessary for proper station-access point interaction. The existing security system is AES-CCMP.

4.1.3 AES-CCMP

AES-128 encryption method in counter mode is used to provide confidentiality and Cipher Block Chaining Message Authentication Code (CBC-MAC) is used for creating Message Integrity Code (MIC) as well, to provide integrity in wireless networks.

AES-CCMP encryption phase starts with creating Initial Counter (IC) by joining Nonce, Flag and Counter fields. Also, Nonce is created from Packet Number (PN), Priority and MAC Address. In encryption phase, MIC and original data contribute. In CTR mode, IC is encrypted and the result is XOR with plain text, then the value of counter in each block is increased one unit. So, IC value is updated for next block. This procedure is repeated until cipher text is completely generated.

Thus, security of counter mode is dependent to the Temporal Key (TK), and IC structure.

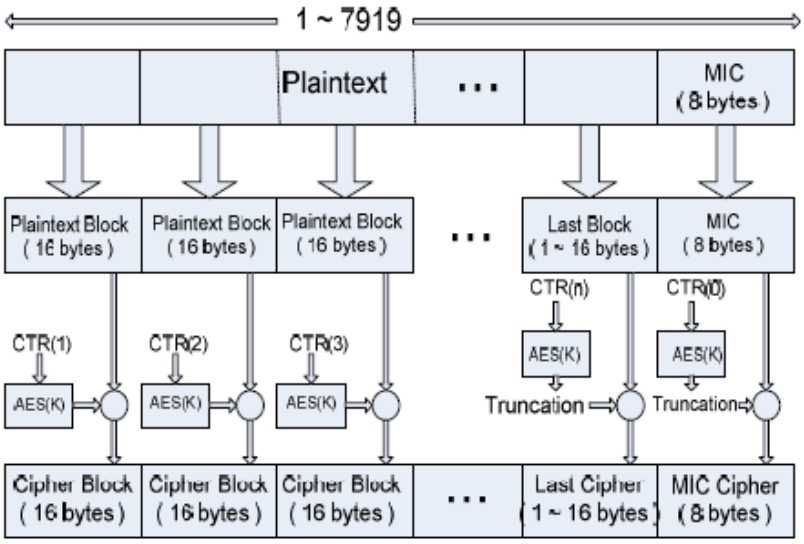

Figure 4.1: CCMP process

As depicted in Figure 4.1, the CTR algorithm ciphers a starting 128-bit counter (A0) with the AES-cipher, then XORs the result with final value of CBC-MAC process, increments the counter and ciphers the next 128-bit counter value with AES cipher. Then, it performs XOR between this result and the plain text of the first block to obtain first block of the ciphered MPDU. Again, counter is incremented and CTR repeats previous steps for the additional 128-bit blocks of data until the final block is processed. In order to parallelize the CTR and CBC-MAC modules, a structure is designed for CTR to start encryption before generation of the MIC T value. In this structure, CTR complete encryption just one clock cycle after MIC T value generation.

Service stations will request services from the access points. It is important for the access point to properly recognize the different services from the stations and provide service to the requests.

The access point uses bandwidth allocation algorithms for this purpose, which in turn implements a scheduling algorithm. The existing servicing process utilizes strict priority scheduling algorithm.

4.1.4 Strict Priority Scheduling

In Strict-Priority, packets are first classified by the scheduler according to the QoS class and then placed into different priority queues. It services the highest

universal hashing over a binary Galois field to provide authenticated encryption. It can be implemented in hardware to achieve high speeds with low cost and low latency. Software implementations can achieve excellent performance by using table-driven field operations. It uses mechanisms that are supported by a well-understood theoretical foundation, and its security follows from a single reasonable assumption about the security of the block cipher.

GCM has two operations, authenticated encryption and authenticated decryption. The authenticated encryption operation has four inputs, each of which is a bit string:

- A secret key K, whose length is appropriate for the underlying block cipher.
- An initialization vector IV, that can have any number of bits between1and 2 fixed value of the key, each IV value must be distinct, but need not have equal lengths. 96-bit IV values can be processed more efficiently, so that length is recommended for situations in which efficiency is critical.
- A plain text P, which can have any number of bits between 0 and 2
- Additional authenticated data (AAD), which is denoted as A. This data is authenticated, but not encrypted, and can have any number of bits between 0 and 2.

There are two outputs:

- A cipher text C whose length is exactly that of the plain text P.
- An authentication tag T, whose length can be any value between 0 and 128. The length of the tag is denoted as t.

Figure 4.3 shows the process of GCMP. A count value will be generated in each round using a pseudo random number generator which will be encrypted using encryption algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple DES etc. After the counter is encrypted, the encrypted data is XORed with the plain text and the result of the XOR operation will be XORed with the previous encrypted data. This chain will continue until there the end of plain text is reached. The counter 0 value is encrypted and XORed with the additional authentication data. The result of this XOR operation is then passed to the next cycle. At the end of the process, an Authentication Tag will be generated. The generated authentication tag will be used to check the integrity of the data over the network.

Thus, GCMP provides a stronger level of encryption when compared to CCMP. One of the main advantage of GCMP over CCMP is that it requires relatively less computation and

SYSTEM DESIGN

Chapter 5

SYSTEM DESIGN

DATA FLOW DIAGRAMS

The design of the proposed system including all the required components can be represented by Data Flow Diagrams (DFD) as explained in the subsections. Data Flow Diagrams illustrates the flow of data within the system, and also the input and output of each components

5.1 DFD for Bandwidth Allocation module

The data flow diagram for Service Period Bandwidth Allocation is as shown in the Figure 5.1. The input to the module will be the priority and the bandwidth which the service station requires. The input is provided to the access point. The service station makes the input through a frame known as Service Period Request. The priority input in the Service Period Request (SPR) frame indicates the type of data that it requires.

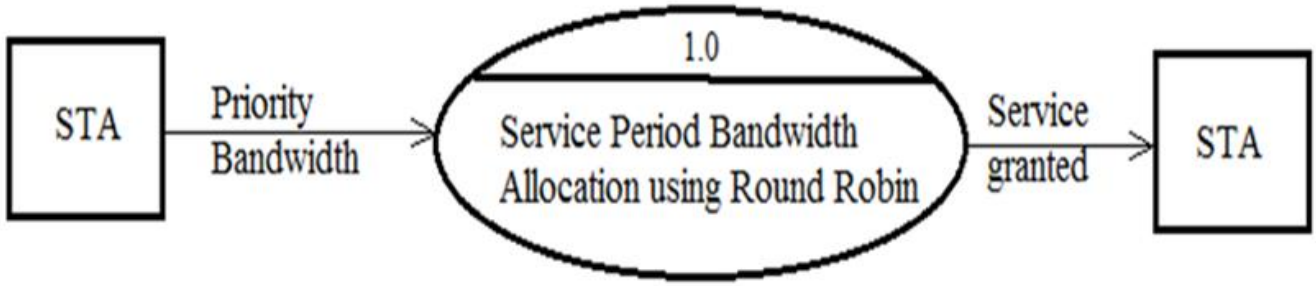

Figure 5.1: Level 0 DFD for Bandwidth Allocation

The priority and bandwidth inputs are taken and used in an algorithm which instructs the access point how much bandwidth to allocate to a particular service station. The priority is decided by the type of service requested by the station indicated by the Service Period Request Frame (SPR). Various types of services include Voice over IP, Video, Best Effort and Background. VoIP is the highest priority service and the background service has the least priority. The algorithm implements a modified form of Round Robin allocation. The algorithm analyses the type of data being requested by the service station using the priority. The access point responds to the Service Period Request Frame (SPR) from the service station with a Grant Frame indicating if its request will be served or not. The Grant frame will specify the service order of a particular service station for its request and the amount of bandwidth allocated for that particular request of corresponding stations in that cycle of service period bandwidth allocation.

5.2 DFD for Authentication of Service Station module

5.2.1 DFD Level 0

Figure 5.2 shows the data flow diagram for the Authentication of the STA module. The authentication is done using the RSNA protocol. The input to the module will be the username and password. The access point uses the username and password of the service station to obtain the Pairwise Master Key(PMK) which will be used for the authentication process. The Pairwise Master Key will be already available with both the access point and the service station. The PMK will be generated and provided to the AP and STA by a third party authentication server like Kerberos or RADIUS. The access point will generate a Pairwise Temporal Key using which the KCK, KEK and TK can be obtained.

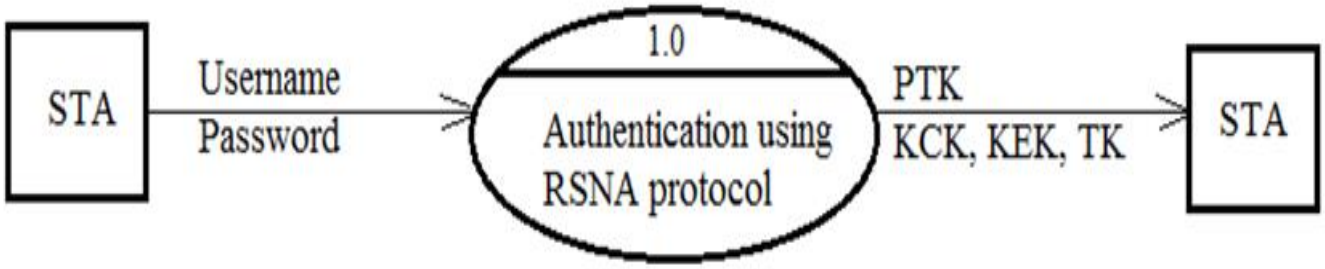

Figure 5.2: DFD for Level 0 for Authentication of STA

The authentication of the STA happens using the 4-way Handshake protocol and a unique Pairwise Temporal Key(PTK) is generated for each STA using which the STA can be authorized.

5.2.2 DFD Level 1

Figure 5.3 shows the DFD for Authentication of STA. The Pairwise Master Key, which is identified using the inputs sent from the service station, is used in the 4-way Handshake process to authenticate the service station by the access point. In the 4-way Handshake process the Nonces are exchanged between the service station and the access point. The Nonce sent by access point is termed ANonce and the Nonce sent by service station is termed SNonce. The Nonces are usually generated using a pseudo random number generator.

PTK is derived as:

PTK = EAPOL-PRF (PMK, ANonce, SNonce, AP Mac addr, STA Mac addr)

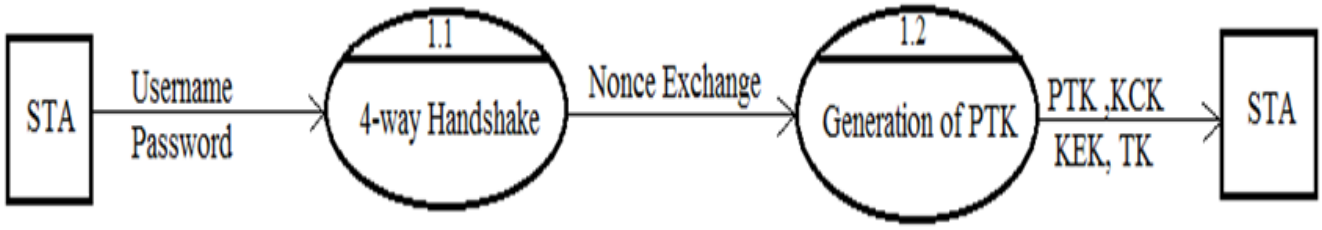

Figure 5.3: Level 1 DFD for Authentication of STA

The Nonce along with the MAC addresses of the access point and the service station is used by the access point to generate the Pairwise Temporal Key. The Pairwise Temporal Key will be unique for each service station. The Pairwise Temporal Key can be divided to obtain the KCK, KEK and TK. The service station and the access point can further use the PTK to generate a GroupWise Transient Key (GTK). The GTK can be used for further data transfer between the access point and service station. A unique GroupWise Transient Key will be generated for each session using the Pairwise Temporal Key.

IMPLEMENTATION

Chapter 6

IMPLEMENTATION

The implementation can be done as a seven step process as follows:

1. Authenticate the STAs
2. Generate the required keys
3. Poll the authenticated STAs
4. Accept service request frames from the STAs
5. Send Grant frames to the requesting STAs
6. Allocate bandwidth to the STAs
7. AP services the requests from STAs

6.1 Authenticate the STAs

The authentication of the STAs (Service Stations) is achieved using RSNA protocol. RSNA protocol uses a process called 4-way Handshake to achieve authentication of stations. The following are the operations done to authenticate a service station.

6.1.1 Identify STA

The service station first logs into the network using his username and password. The access point uses the credentials of the station to identify the unique Pairwise Master Key(PMK) for that station and access point. This unique PMK is used further in the 4-way Handshake process.

6.1.2 4-Way Handshake

The handshake completes the IEEE 802.1X authentication process. It involves exchange of messages between the service station(STA) and access point(AP). The messages are exchanged in frames. The frame used in 4-way Handshake is EAPOL frame.

Figure 6.1, shows the general structure of the EAPOL key frame. All the fields are appropriately populated and sent as a message at each step. Once a message is received, it is deframed and the required particular fields are used for the authentication process.

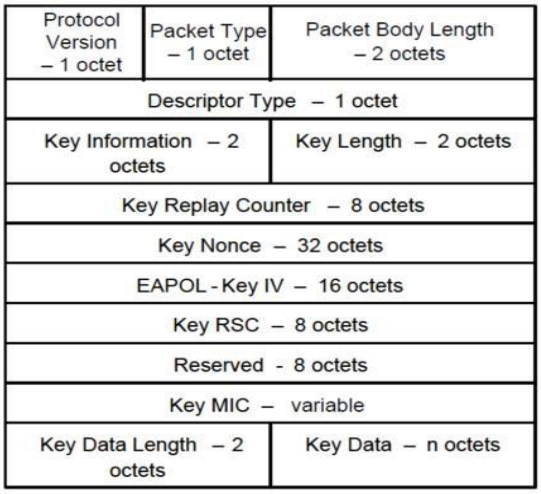

Figure 6.1: EAPOL key frame format

The key frame is encoded and sent in the sender side and it is decoded in the receiver side. The algorithm shows the encoding and decoding.

The encoded key frames are exchanged between the access point(AP) and service station(STA).

EAPOL frame structure:

```
struct EAPOL {
        uint8_t ProtocolVersion;
        uint8_t PacketType;
        uint16_t PacketBodyLength;
        uint8_t DescriptorType;
        uint8_t KeyDescriptorVersion;
        uint8_t KeyType;
        uint8_t Reserved1;
        uint8_t install;
        uint8_t KeyAck;
        uint8_t IKeyMic;
        uint8_t Secure;
        uint8_t Error;
        uint8_t Request;
        uint8_t EncryptedKeyData;
        uint8_t SMKMessage;
        uint8_t Reserved2;
        uint16_t KeyLength;
        uint64_t KeyReplayCounter;
        uint64_t KeyNounce[4];
        uint64_t EapolKeyIV[2];
        uint64_t KeyRsc;
        //uint8_t *KeyMic;
        uint16_t KeyDataLength;
        //uint8_t *KeyData;
};
```

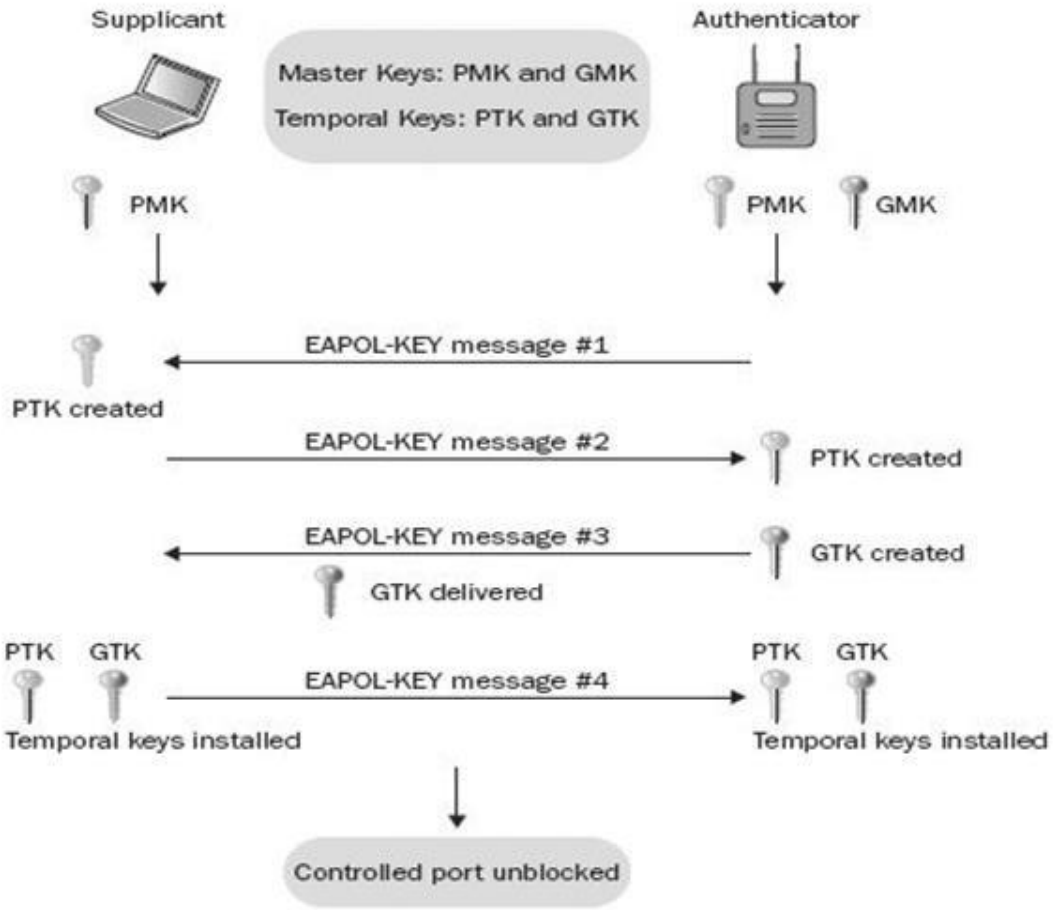

Figure 6.2: 4-way Handshake

Figure 6.2 depicts the information flow of the 4-Way Handshake. The 4-way Handshake process is as follows:

a) **Message 1**: Authenticator → Supplicant

The message 1 of the 4-way Handshake includes the ANonce sent from the access point to the station. The station uses the ANonce and SNonce, which it has, to generate the PTK.

EAPOL-Key(0,0,1,0,P,0,0,ANonce,0,DataKD_M1)

where DataKD_M1 = 0 or PMKID for PTK generation, ANonce is used in PTK generation.

b) **Message 2**: Supplicant → Authenticator

The message 2 of the 4-way Handshake includes the SNonce sent by the station. The station uses the SNonce and ANonce, which it obtained from AP, uses it to generate the PTK.

EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,DataKD_M2)

where DataKD_M2 = RSNE for creating PTK generation or peer RSNE,

SNonce is used for PTK generation

c) **Message 3**: Authenticator → Supplicant

EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,DataKD_M3)

where DataKD_M3 = RSNE,GTK[N] for creating PTK generation or initiator RSNE,

Lifetime KDE for STK generation

d) **Message 4**: Supplicant → Authenticator

EAPOL-Key(1,1,0,0,P,0,0,0,MIC,DataKD_M4)

where DataKD_M4 = 0.

The messages are exchanged between the client and server in the form of EAPOL frames that are sent using TCP socket as a wireless communication channel.

The Nonces that are generated during the initial phase of the 4-way handshake are encrypted using Advanced Encryption Standards (AES) before sending it through the wireless network. Figure 6.3 illustrates how a connection is established between a client and the server using TCP socket.

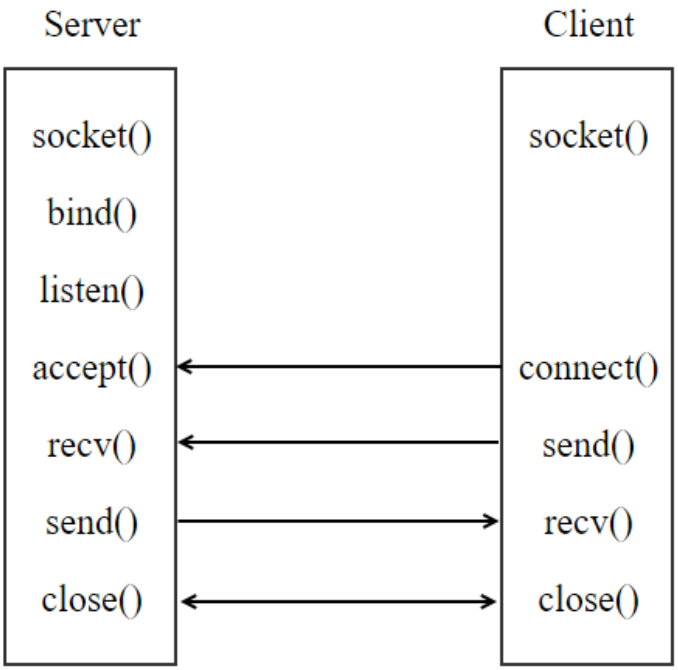

Figure 6.3: Connection establishment between Client and Server

Algorithm for encoding the EAPOL frames

```
//Encoding Eapol-Key Frame

//Encode-Eapol(struct EAPOL *frame)
//input: Eapol-key frame
//output: Encoded buffer

char *Buffer = NULL
Buffer = (char*)malloc(len*sizeof(char));

for each field of 8bits
            *Buffer = (char)frame->data;
             Buffer++;
end for

for each field of 16bits
            uint16_t val = frame->data;
            unsigned char lo = val >> 8;
            unsigned char hi = val;
            *Buffer = lo;Buffer++;
            *Buffer = hi;Buffer++;
end for

for each field of 64bits
            uint64_t val = frame->data;
            unsigned char arr[8];
            arr[0] = data >> 56;
            arr[1] = data >> 48;
            arr[2] = data >> 40;
            arr[3] = data >> 32;
            arr[4] = data >> 24;
            arr[5] = data >> 16;
            arr[6] = data >> 8;
            arr[7] = data;
            *Buffer = arr[0];Buffer++;
            *Buffer = arr[1];Buffer++;
            *Buffer = arr[2];Buffer++;
            *Buffer = arr[3];Buffer++;
            *Buffer = arr[4];Buffer++;
            *Buffer = arr[5];Buffer++;
            *Buffer = arr[6];Buffer++;
            *Buffer = arr[7];Buffer++;
end for
```

Algorithm for Decoding the EAPOL frames:

```
//Decoding Eapol-key frame

//Decode-Eapol(struct EAPOL *frame)
//Input: EAPOL-key frame
//Output: decoded buffer



char *Buffer = NULL
Buffer = (char*)malloc(len*sizeof(char));
recv buffer over socket

for each field of 8bits
            frame->data = (uint8_t)*Buffer;
             Buffer++;
end for

for each field of 16bits
            unsigned char lo = *Buffer;Buffer++;
            unsigned char hi = *Buffer;Buffer++;
            uint16_val val = ((uint16_t)lo << 8) | hi;
            frame->data = val;
end for

for each field of 64bits
            unsigned char arr[8];
            arr[0] = (*Buffer);Buffer++;
            arr[1] = (*Buffer);Buffer++;
            arr[2] = (*Buffer);Buffer++;
            arr[3] = (*Buffer);Buffer++;
            arr[4] = (*Buffer);Buffer++;
            arr[5] = (*Buffer);Buffer++;
            arr[6] = (*Buffer);Buffer++;
            arr[7] = (*Buffer);Buffer++;
            uint64_t val= ((uint64_t)arr[0] << 56) |
                                    ((uint64_t)arr[1] << 48) |
                                    ((uint64_t)arr[2] << 40) |
                                    ((uint64_t)arr[3] << 32) |
                                    ((uint64_t)arr[4] << 24) |
                                    ((uint64_t)arr[5] << 16) |
                                    ((uint64_t)arr[6] << 8) |
                                    (arr[7]);
            frame->data = val;

end for
```

Algorithm for PTK generation:

```
//Algorithm: PRF(K,A,B,X)
//Input: K is a key, A is a unique label for different purpose , B is varient length string , len is the length
//output: random phrase of length len

PRF(K,A,B,len)
        for i<=0 to (len+159)/160 do
                Result = "";
                Result <= Result||H-SHA-1(K,A,B,i)
        end for
return Truncate-to-len(Result,0,len)

//Function For Secure Hash .

function HMAC-SHA1(unsigned char *key,char *data)

   unsigned char* digest;
   digest = HMAC(EVP_sha1(), key, strlen(key), (unsigned char*)data, strlen(data), NULL, NULL);

   char mdString[20];
   for(int i = 0; i < 20; i++)
      sprintf(&mdString[i*2], "%02x", (unsigned int)digest[i]);
   end for
return mdstring
end function

PTK <= PRF-X(PMK,"Pairwise Key expansion", Min(AA,SPA)||MAx(AA,SPA)||Min(Anounce,SNounce)||Max(Anounce,Snounce))

X = 256 + TK_bits
TK_bits is cipher suit dependent.

KCK is computed as the first bits(0-127) of th ptk
KCK <= L(PTK,0,128)

KEK is Computed using 128-255 of the PTK.
KEK <= L(PTK,128,128)

TK is computed using 256 to (255+TK_bits) of the PTK.
TK <= L(PTK,256,TK_bits)
```

6.3 Accept service requests from the STAs

The STAs after being authenticated can make requests for services to the AP. The service requests from the STAs are accepted by the AP through a 3-way Handshake.

Figure 6.3a depicts the interaction between the access point and the service stations.

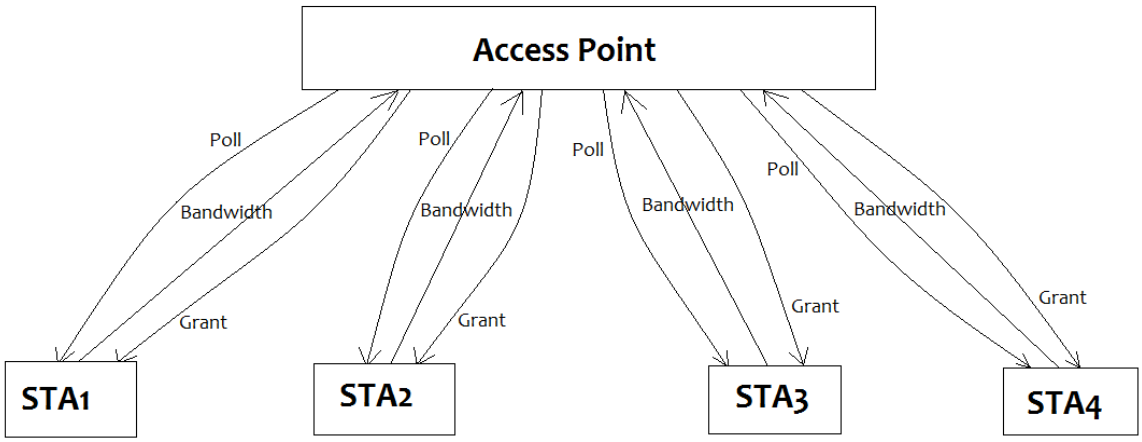

Figure 6.5: AP - STA Interaction (3-way handshake)

The 3-way Handshake process starts with the AP polling all the authenticated STAs. The AP sends a Poll frame. The STA which requires a service will respond to the poll frame by registering a request. The request is sent using the SPR (Service Period Request) frame. The AP accepts request frames from all stations for a particular poll duration after which the polling stops and the servicing starts. The AP processes all the request and responds to them with the amount of bandwidth allocated and the service order based on the priorities of the service. It is sent to the STA using a Grant frame.

a) Poll frame:

The access point sends the poll frame to all the stations stating its maximum bandwidth in the frame. Figure 6.5 shows the poll frame.

	Frame Control	Duration	RA	TA	Response Offset	FCS
Octets:	2	2	6	6	2	4

Figure 6.6: Poll Frame

b) SPR frame:

The service station responds to the poll from the access point by sending an SPR, service period request, to the access point. The SPR frame includes the type of data which the station requires and the amount of bandwidth it requires. Figure 6.6 depicts the frame structure of SPR frame sent by the STA.

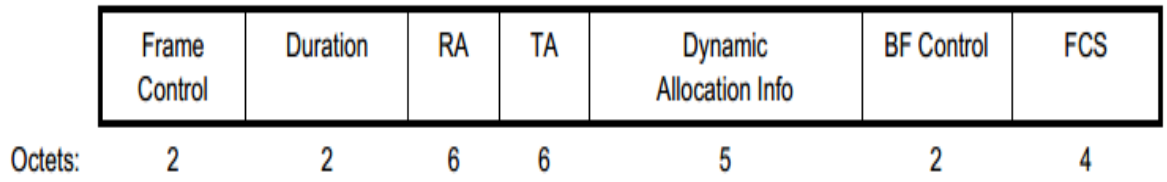

Figure 6.7: SPR Frame Format

The Dynamic Allocation Info field in the SPR frame contains the information about the bandwidth it requires and the type of service requested. It is a separate frame as shown in figure 6.7

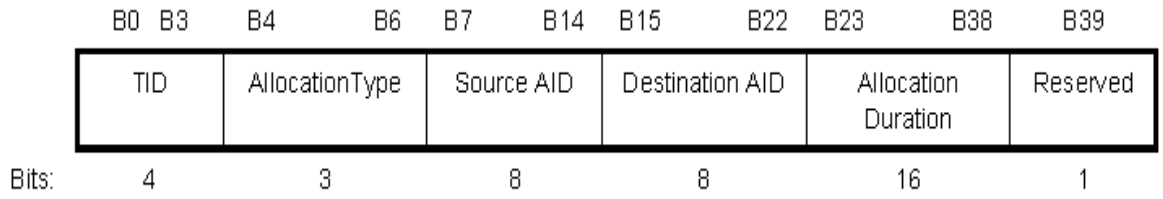

Figure 6.8: Dynamic Allocation Info Frame

c) Grant frame:

Figure 6.8 shows the format of a Grant Frame. The access point extracts the request from the SPR frame. It processes the request and responds to the station with a Grant frame. The Grant frame is similar to the SPR frame with same fields. The Dynamic Allocation Info field will contain the amount of bandwidth allocated each servicing cycle and the order of servicing for a particular STA.

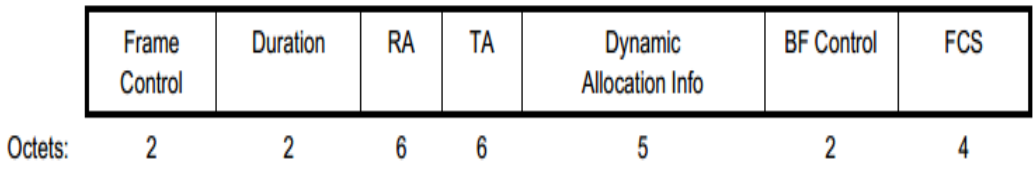

Figure 6.9: Grant Frame Format

6.4 Allocate bandwidth to the STAs

The access point obtains the requests from the service stations through the SPR frame. It analyses the requests and provides appropriate bandwidth to the stations to service its requests. The analysis is done using the algorithm. The algorithm revolves around the Round Robin fashion of servicing the requests.

After accepting all the request frames during a poll interval, the algorithm computes the sum of all the requested bandwidth.

Then it computes a factor known as the "Allocation Factor" which is given by:

Allocation Factor = (Sum of Requests / Maximum available Bandwidth) ..... (1)

If the Allocation factor is less than 1, then the total requests made is well within the maximum available bandwidth, and hence complete allocation is done to all the stations.

On the other hand, if the Allocation factor is greater than 1, then the sum of requests exceeds the maximum available bandwidth. In this case the individual requests are reduced by dividing with the Allocation factor, and the fraction of the bandwidth is allocated. This process continues for multiple cycles in Round Robin fashion until the entire requested bandwidth of each station has been allocated.

If the requested bandwidth is less than 1, then available bandwidth is allocated to each client and is processed in round robin fashion based on the algorithm. It can be completed in a single cycle if the sum of the requested bandwidth is less than the maximum available bandwidth. After allocating the bandwidth if bandwidth is still available then some amount of bandwidth is allocated to the highest priority queue to the lowest priority queue. Which ensures that the bandwidth is utilized completely which takes lower time to complete the process.

If the requested bandwidth is equal to 1 then the entire available bandwidth is allocated to the requested client. And the client is served in round robin fashion. In this case the bandwidth is completely utilized. If single client is requesting the bandwidth then, the bandwidth is allocated completely to the client. As the client dynamically requests the bandwidth the allocation factor is changed by the algorithms and multiple client are served in round robin fashion.

The following pseudo code captures the essence of bandwidth allocation:

```
Initialize MAX_BANDWIDTH to 100 (or whatever be the max)

Initialize four arrays Q1, Q2, Q3, Q4 of equal size to 0

Initialize the schedule array "out" to 0


Initialize i1, i2, i3, i4 to 0

Initialize Req_Sum to 0

Initialize Allocation_Factor to 0

while the polling does not stop

                        obtain the requests from the client

                        if requested service type = 1 (VoIP)
                                put the request in  Q1[i1++]

                        if requested service type = 2 (Video)
                                put the request in  Q2[i2++]

                        if requested service type = 3 (Best Effort)
                                put the request in  Q3[i3++]

                        if requested service type = 4 (Background)
                                put the request in  Q4[i4++]

Polling ends after the poll duration ends


for i = 0 to i1
        Req_Sum = Req_Sum + Q1[i]

for i = 0 to i2
        Req_Sum = Req_Sum + Q2[i]

for i = 0 to i3
        Req_Sum = Req_Sum + Q3[i]

for i = 0 to i4
        Req_Sum = Req_Sum + Q4[i]

Allocation_Factor = Req_Sum / MAX_BANDWIDTH
i = 0
Initialize Rem_Sum to Req_Sum
```

```
while Rem_Sum > 0
        if Allocation_Factor > 1.0

                for j = 0 to i1
                        if Q1[j] > 0
                                out[i++] = Q1[j] / Allocation_Factor;
                                Q1[j] = Q1[j] - (Q1[j] / Allocation_Factor)
                                Rem_Sum - = Q1[j]

                for j = 0 to i2
                        if Q2[j] > 0
                                out[i++] = Q2[j] / Allocation_Factor;
                                Q2[j] = Q2[j] - (Q2[j] / Allocation_Factor)
                                Rem_Sum - = Q2[j]

                for j = 0 to i3
                        if Q3[j] > 0
                                out[i++] = Q3[j] / Allocation_Factor;
                                Q3[j] = Q3[j] - (Q3[j] / Allocation_Factor)
                                Rem_Sum - = Q3[j]

                for j = 0 to i4
                        if Q4[j] > 0
                                out[i++] = Q4[j] / Allocation_Factor;
                                Q4[j] = Q4[j] - (Q4[j] / Allocation_Factor)
                                Rem_Sum - = Q4[j]


        else


                for j = 0 to i1
                        out[i++] = Q1[j]
                        Rem_Sum = Rem_Sum - Q1[j]
                        Q1[j] = 0
                        i1 = i1 - 1

                for j = 0 to i2
                        out[i++] = Q2[j]
                        Rem_Sum = Rem_Sum - Q2[j]
                        Q2[j] = 0
                        i2 = i2 - 1


                for j = 0 to i3
                        out[i++] = Q3[j]
                        Rem_Sum = Rem_Sum - Q3[j]
                        Q3[j] = 0
                        i3 = i3 - 1

                for j = 0 to i4
                        out[i++] = Q4[j]
                        Rem_Sum = Rem_Sum - Q4[j]
                        Q4[j] = 0
                        i4 = i4 - 1
```

end while

The array "out" contains the servicing order and the scheduled bandwidth for each station

The server sends back the grant frames that contain the service order and the amount of bandwidth allocated, to the stations.

TESTING

Chapter 7

TESTING

Software Testing is the process of executing a program or system with the intent of finding errors. It involves any activity aimed at evaluating an attribute or capability of a program or system and determining that it meets its required results.

7.1 Unit Testing

Unit testing is the process of testing individual components of program. It is a procedure used to validate that a particular module of a source code is working properly. The objective of unit testing is to test not only the functionality of the code, but also to ensure that code is structurally sound and robust, and able to respond appropriately in all conditions. A unit testing is also called component testing, as it requires the knowledge of the internal design of the code. It is typically used to verify control flow.

The whole application is made up of different modules. Unit testing focuses on each sub modules independent of one another, to locate errors, enabling the programmer to detect errors. During module testing the concept of trace and breakpoints are applied at different stages of testing. During the unit testing of this project, each and every module was tested with certain test data to ensure that the program works accurately.

The following unit test cases were performed:

Test case ID	**U-1**
Name	Exchange of Nonces
Purpose	To verify if all the messages are being exchanged in correct process.
Sample input	Username, Password
Expected output	Nonce Exchange
Actual output	AP receives SNonce and STA receives ANonce.
Remark	Messages are properly received by the AP and STA and sent to the appropriate device

Table 7.1: Test case for Nonce Exchange

Test case ID	**U-2**
Name	Generation of PTK
Purpose	To generate Pairwise Transient Key
Sample input	Nonces, AP Mac address, STA Mac address
Expected output	Pairwise Transient Key generated
Actual output	PTK generated which comprises of KCK, KEK and TK
Remark	PTK is generated.

Table 7.2: Test case for Generation of PTK

Test case ID	**U-3**
Name	Request generation
Purpose	To generate requests based on the maximum available bandwidth.
Expected output	Requests properly generated.
Actual output	STA generates service requests comprising of the type of data and the bandwidth it requires.
Remark	Requests are precisely generated.

Table 7.3: Test case for Request Generation

Test case ID	**U-4**
Name	Request Acceptance
Purpose	AP needs to accept requests from the STAs correctly..
Sample input	Service Period Requests from STAs
Expected output	AP accepts SPRs
Actual output	AP receives the SPRs from STAs and extracts the bandwidth and the type of data.
Remark	AP accepts all the requests from the STAs accurately.

Table 7.4: Test case for Request Acceptance

Test case ID	**U-5**
Name	Bandwidth Allocation Algorithm
Purpose	To properly process all the input service requests and allocate bandwidth accordingly.
Sample input	Service Period Requests from STAs
Expected output	Bandwidth allocated to STAs based on their request
Actual output	AP assigns Bandwidth to all STAs depending on the priority of the requests made by the STAs.
Remark	AP assigns bandwidth to all the STAs depending on the type of data it requests.

Table 7.5: Test case for Bandwidth Allocation Algorithm

7.2 Integration Testing

Upon completion of unit testing, the units or modules are to be integrated which gives raise to integration testing. It occurs after unit testing and before validation testing. Integration testing takes as its input modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing. It is done to ensure that all the modules, which works correctly when independent, works without any discrepancies when integrated. The purpose of integration testing is to verify the functional, performance, and reliability between the modules that are integrated.

Test case ID	**I-1**
Name	4-way Handshake
Purpose	To verify proper exchange of Nonces and generation of PTK
Sample input	Username, Password
Expected output	PTK generated
Actual output	PTK generated which comprises of KCK, KEK and TK
Remark	AP assigns a PTK to STA thus authenticating the STA. The PTK can be used by the AP and STA for further interaction between AP and STA

Table 7.6: Test case for 4-way Handshake

Test case ID	**I-2**
Name	3-way Handshake
Purpose	To verify if the AP accepts and receives the requests properly and responds with the bandwidth allocated.
Sample input	Service Period Requests from STAs
Expected output	Bandwidth allocated to STAs based on their request
Actual output	AP assigns Bandwidth to all STAs depending on the priority of the requests made by the STAs.
Remark	AP accepts SPRs from STAs, allocates the requested bandwidth to each STA based on the type of data it requested.

Table 7.7: Test case for 3-way Handshake

RESULTS

CONCLUSION

Chapter 9

CONCLUSION

Considering a wireless network system conforming to IEEE 802.11ad standard, consisting of an Access Point and a few stations, the system aims at providing an efficient fool proof authentication process to authenticate the clients and an efficient mechanism to service the so authenticated clients, by allocating the required bandwidth for the requested service.

The system proves to be efficient as it makes use of the 4-way Handshake process which involves multi-step client authentication and continuous key generation for each cycles which makes it practically impossible for attackers to crack the keys through various attacks like Brute Force, Hash attack etc.

The bandwidth allocation mechanism proves to be efficient as it follows the round robin principle. Irrespective of the number of clients requesting various services, the system allocates at least some amount of bandwidth to each of the requested client. This eliminates the problem of indefinite waiting or starving. The system also aims at allocating bandwidth based on certain weights assigned to each type of service. More weight is given to the higher priority services which means the fraction of bandwidth allocated to higher priority services will be relatively higher than that allocated for lower priority services. This brings more fairness to the process.

LIMITATIONS AND FUTURE ENHANCEMENTS

Chapter 10

LIMITATIONS AND FUTURE ENHANCEMENTS

The system uses 4-way Handshake for authentication. Since the process involves creation of various keys, there might be chances of rogue clients hogging the Authenticator, resulting in a Denial of Service (DoS) attack. As an improvisation of the 4-way handshake, 2-way handshake can be implemented along with the 4-way handshake.

The bandwidth allocation algorithm focuses on the fairness in bandwidth allocation. In the process, it fails to service a tiny amount of bandwidth entirely. As an example, if there are many requests of various services and the total requested bandwidth well exceeds the maximum available bandwidth, and along with those, there is a request for a service which requires very less amount of bandwidth. If this algorithm were to be more fair, it has to service the shorter requests immediately and based on the priority of the service requested. The algorithm can be tweaked in such a way that the shorter requests are considered first before moving on to other requests.

BIBILOGRAPHY

[1] IEEE 802.11 specification.

[2] IEEE 802.11ad specification.

[3] IEEE 802.11i Overview, Nancy Cam-Winget, Cisco Systems, Tim Moore, Microsoft, Dorothy Stanley, Agere Systems, Jesse Walker, Intel Corporation.

[4] Security Analysis and Improvements for IEEE 802.11i Changhua, John C Mitchell Electrical Engineering and Computer Science Departments Stanford University, Stanford CA 2008.

[5] Comparison of Various Scheduling Algorithms in WiMAX: A Brief Review. International Conference on Advances in Management and Technology (iCAMT - 2013).

[6] IEEE paper on "Robust Security Network Association Adjusted Hybrid Authentication Schema", Viktors gopejenko, Sergejs Bobrovskis 2014.

[7] "A Literature Review of Security Threats to Wireless Networks", YMCA University of Science and Technology 2014