PACKET BASED AUTHENTICATION MECHANISM IN WIMAX

By

NC Moeen Ahmad

PC Jawad Zaheer

PC Ammar Ahmed

PC Muhammad Ahmed Bilal

Submitted to the Faculty of EE Dept. National University of Sciences and Technology, Rawalpindi in partial fulfillment of B.E. degree in Telecommunication Engineering.

March 2008

بسم الله الرحمن الرحيم

Dedication

We dedicate this project to our parents and teachers.

Abstract

WiMAX (World wide interoperability for Microwave Access) is a step towards 4th generation communication. Wireless communication is more vulnerable to attacks such as man in the middle attack, jamming, replay and DoS etc. The strength of CCMP algorithm used in WiMAX is prone to precomputation attack as the initial counter is predictable. Packet based challenge response mechanism uses separate encryption key for each packet thus strengthening the security of the connection against unauthorized access by immediately discarding the packet if packet authentication fails. Further, the Nonce and initial counter are not predictable anymore.

ACKNOWLEDGEMENT

In the name of Almighty Allah, The most Beneficent, The most Merciful. Completing the project was in the true sense a great learning opportunity which provided us a chance to experience and master new skills meet different people and collaborate with them. Though this project was the result of our own effort but we could not have reached this far, if it would not have been the guidance of various persons who helped us in different aspects.

We gratefully acknowledge the guidance and motivation provided to us by our project supervisor Asst. Prof. Zaka-ul-Mustafa. We are also grateful to Maj Saeed (Comsats, Wah) and David Corking (Motorola, UK). Their timely guidance helped us a lot in achieving our goals.

We are grateful to our beloved parents who provided their complete support, help and advice in every part of our lives.

Table of Contents

List of Figures

List of Tables

Introduction

The start of the new millennium has witnessed a telecommunication world that is very different from the previous millennium. The huge explosion of wireless and broadband technologies over the last few years has captured the imagination and innovativeness of technologists around the world. It has been a constant human endeavour to communicate more effectively and at the same time to be free of any bondage. A similar underlying trend can also be seen in the evolution of telecommunications. The need for mobility and higher speeds in an ever-changing environment has been of paramount importance. With the new-found power of mobility and broadband, the telecommunications industry has tapped into an explosive technology mix that can grow exponentially once creativity and innovativeness come into play.

1.1. Wireless Communication: -

The main reason behind the extreme growth and boom in the communication field especially in the wireless sector is due to the abilities of wireless communication i.e. information transfer anywhere, any time. The future of wireless communication lies in better data rates, high security and full mobility. The basic few reasons due to which the wireless communication is attractive to users are as follows:-

1.1.1. Mobility:-

The first thing that comes into mind after hearing the word "wireless communication" is the mobility this type of communication can provide to the users, the ability to use the technology beyond a fixed place and the ability to communicate with anyone from virtually anywhere.

1.1.2. Simplicity:-

Wireless communication is faster and easier to deploy than the wired systems.

1.1.3. Setup cost:-

The setup cost for implementing a wireless communications system is considerably less than the cost to setup the traditional wired systems. Other advantages of wireless systems include the feasibility of providing communication to areas where wired communications cannot be installed or are costly to implement.

1.1.4. Personal devices:-

Wireless communications systems provide real personal devices which are place independent whereas wired devices are place dependent. It is the direction in which telecommunications seem to be heading to provide all possible ways of keeping information place-independent to a greater or lesser extent.

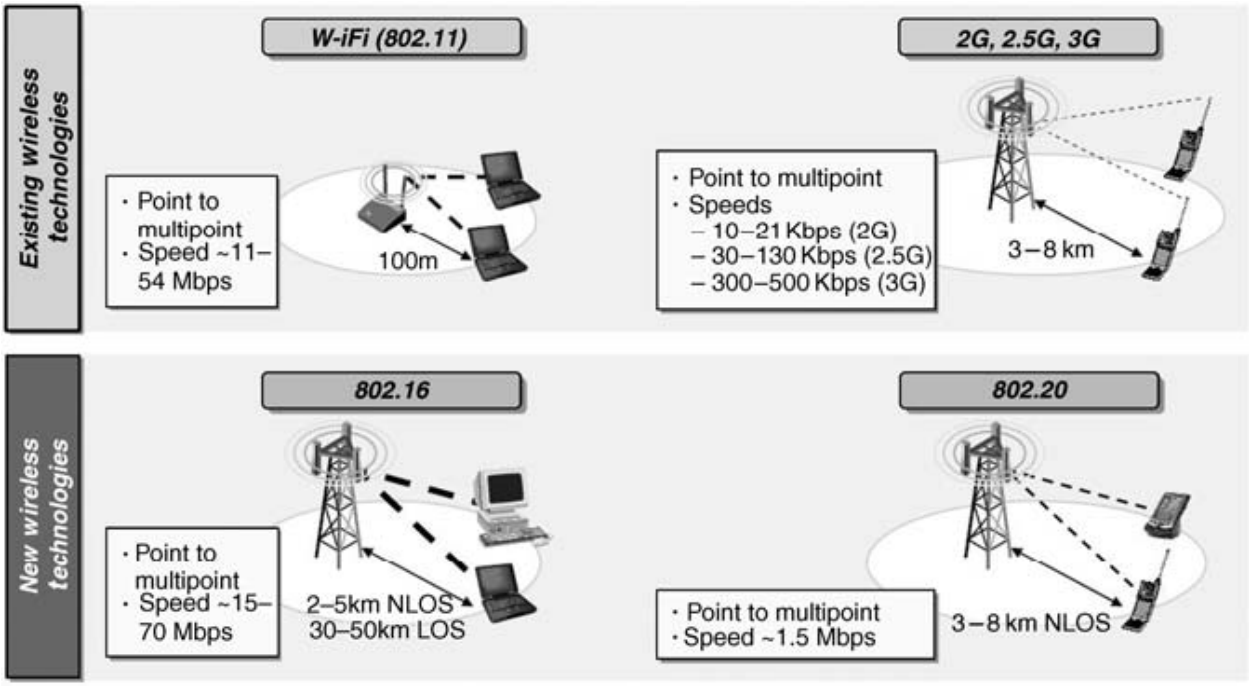


Figure 1:- Wireless Technologies [13]

1.2. Broadband Wireless:-

Broadband wireless sits at the convergence of two of the most remarkable growth stories of the telecommunications industry in recent years. Both wireless and broadband have enjoyed rapid mass-market adoption. Wireless mobile services grew from 11 million subscribers worldwide in 1990 to more than 2 billion in 2005 [14]. The same period, the Internet grew from being a curious academic tool to having about a billion users. This staggering growth of the Internet is driving demand for higher-speed Internet-access services, leading to a parallel growth in broadband adoption. In less than a decade, broadband subscription worldwide has grown from virtually zero to over 200 million [15].

Broadband users worldwide are finding that it dramatically changes how we share information, conduct business and seek entertainment. Broadband access not only provides faster web surfing and quicker file downloads but also enables several multimedia applications, such as real-time audio and video streaming, multimedia conferencing, and interactive gaming. Broadband connections are also being used for voice telephony using voice-over-Internet Protocol (VoIP) technology. More advanced broadband access systems, such as fiber-to-the-home (FTTH) and very high data rate digital subscriber loop (VDSL), enable such applications as entertainment-quality video, including high-definition TV (HDTV) and video on demand (VoD). As the broadband market continues to grow, several new

applications are likely to emerge and it is difficult to predict which of these will succeed in the future.

Broadband wireless is about bringing the broadband experience to a wireless context, which offers users certain unique benefits and convenience. There are two fundamentally different types of broadband wireless services. The first type provides broadband services much like the previous traditional broadband services (e-g DSL) but uses the wireless as the medium of transmission. This type, called fixed wireless broadband, can be thought of as a competitive alternative to DSL or cable modem. The second type of broadband wireless, called mobile broadband, offers the additional functionalities of portability and mobility. Mobile broadband attempts to bring broadband applications to new user experience scenarios. WiMAX (worldwide interoperability for microwave access) technology is designed to accommodate both fixed and mobile broadband applications.

WiMAX

2. WiMAX:-

The prospect of broadband Internet access anywhere, at any time, seemed a distant dream, far from reality for the vast majority of PC, laptop and handheld users. However, with WiMAX (worldwide interoperability for microwave access), it will soon become something users cannot live without. WiMAX is one of the hottest wireless technologies around today.

WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an economical way. After years of development and uncertainty, a standards-based interoperable solution has emerged for broadband wireless. A broad industry consortium, the Worldwide Interoperability for Microwave Access (WiMAX) Forum has started certifying broadband wireless products for interoperability and compliance with the standard. WiMAX is based on wireless metropolitan area networking (WMAN) standards developed by the IEEE 802.16 group and adopted by both IEEE and the ETSI HIPERMAN group.

WiMAX will be two different market technologies. The first is for fixed wireless and falls under the IEEE 802.16-2004 standard approved last year (2007). The second, for mobile applications, will be under the IEEE 802.16e specifications expected to be finalized this year (2008). As of now, fixed WiMAX is capable of becoming a replacement for DSL, cable modem or for network backhaul. In future, WiMAX will transform the world of mobile broadband by enabling the cost-effective deployment of metropolitan area networks based on the IEEE 802.16e standard to support notebook PC and mobile users on the move.

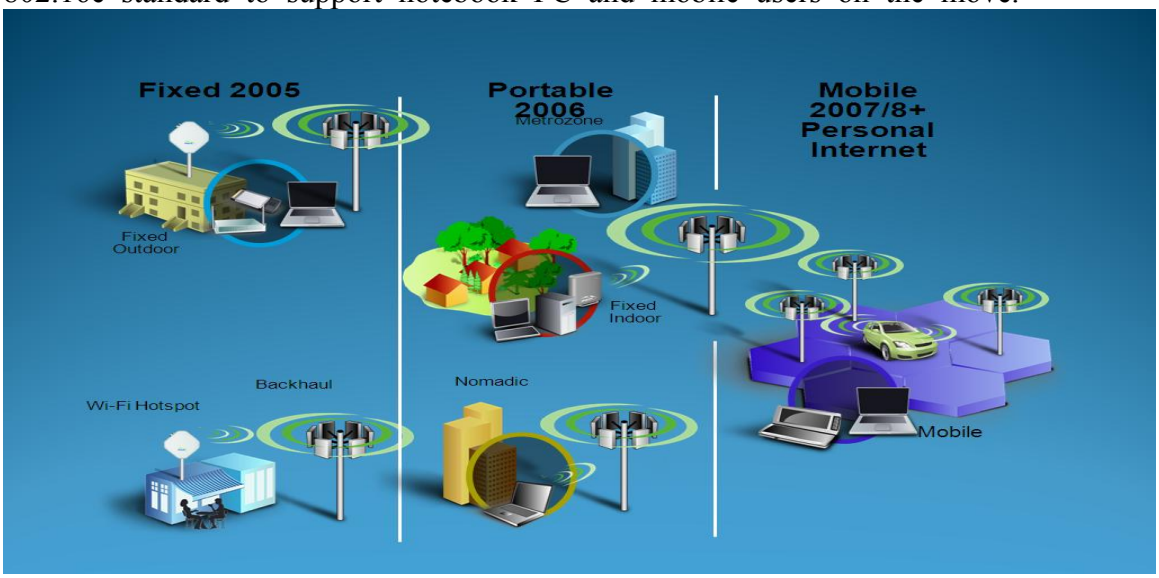


Figure 2:- WiMAX Scenarios

The advantages of systems implemented on the IEEE 802.16 include, the ability to provide service even in areas that are difficult for wired infrastructure to reach and the ability to overcome the physical limitations of traditional wired infrastructure. The standard will offer wireless connectivity of up to 30 miles. The

major capabilities of the standard are its widespread reach, which can be used to set up a metropolitan area network, and its data capacity of 75 Mbps.
This high-speed wireless broadband technology promises to open new, economically viable market opportunities for operators, wireless Internet service providers and equipment manufacturers. The flexibility of wireless technology, combined with high throughput, scalability and long-range features of the IEEE 802.16 standard helps to fill the broadband coverage gaps and reach millions of new residential and business customers worldwide.

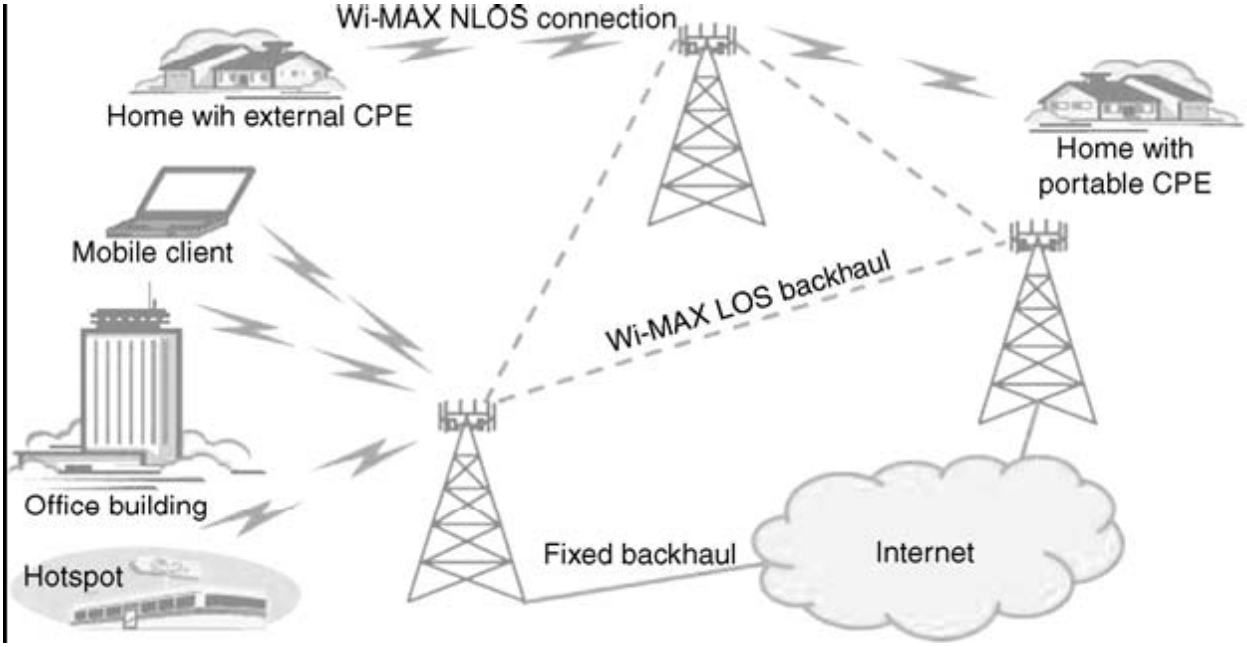


Figure 3:- LOS vs NLOS

2.1. Background on IEEE 802.16 and WiMAX:-

The IEEE 802.16 group was formed in 1998 to develop an air-interface standard for wireless broadband. The group's initial focus was the development of a LOS-based point-to-multipoint wireless broadband system for operation in the 10GHz–66GHz band. The resulting standard—the original IEEE 802.16 standard, completed in December 2001—was based on a single-carrier physical (PHY) layer with a burst time division multiplexed (TDM) MAC layer. Many of the concepts related to the MAC layer were adapted for wireless from the popular cable modem DOCSIS (data over cable service interface specification) standard.
The IEEE 802.16 group subsequently produced IEEE 802.16a, an amendment to the standard, to include NLOS applications in the 2 GHz – 11 GHz band, with orthogonal frequency division multiplexing (OFDM)-based physical layer. Additions to the MAC layer, such as support for orthogonal frequency division multiple access (OFDMA), were also included. Further revisions resulted in a new standard in 2004, called IEEE 802.16-2004, which replaced all prior versions and formed the basis for the first WiMAX solution. These early WiMAX solutions based on IEEE 802.16-2004 targeted fixed applications and are referred as fixed WiMAX

[4]. In December 2005, the IEEE group completed and approved IFEEE 802.16e-2005, an amendment to the IEEE 802.16-2004 standard that added mobility support. The IEEE 802.16e-2005 forms the basis for the WiMAX solution for nomadic and mobile applications and is often referred to as mobile WiMAX [17]. The basic characteristics of the various IEEE 802.16 standards are summarized in the following table:

	802.16	802.16-2004	802.16e-2005
Status	Completed December 2001	Completed June 2004	Completed December 2005
Frequency band	10GHz–66GHz	2GHz–11GHz	2GHz–11GHz for fixed; 2GHz–6GHz for mobile applications
Application	Fixed LOS	Fixed NLOS	Fixed and mobile NLOS
MAC architec-ture	Point-to-multipoint, mesh	Point-to-multipoint, mesh	Point-to-multipoint, mesh
Transmission scheme	Single carrier only	Single carrier, 256 OFDM or 2,048 OFDM	Single carrier, 256 OFDM or scalable OFDM with 128, 512, 1,024, or 2,048 subcarriers
Modulation	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM
Gross data rate	32Mbps–134.4Mbps	1Mbps–75Mbps	1Mbps–75Mbps
Multiplexing	Burst TDM/TDMA	Burst TDM/TDMA/ OFDMA	Burst TDM/TDMA/ OFDMA
Duplexing	TDD and FDD	TDD and FDD	TDD and FDD
Channel band-widths	20MHz, 25MHz, 28MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz
Air-interface designation	WirelessMAN-SC	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA WirelessHUMAN[a]	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA WirelessHUMAN[a]
WiMAX implementation	None	256 - OFDM as Fixed WiMAX	Scalable OFDMA as Mobile WiMAX

Table 1:- Various IEEE 802.16 standards

For practical reasons of interoperability, the scope of the standard needs to be reduced, and a smaller set of design choices for implementation needs to be defined. The WiMAX Forum does this by defining a limited number of system profiles and certification profiles. A system profile defines the subset of mandatory and optional physical-layer and MAC-layer features selected by the WiMAX Forum from the IEEE 802.16-2004 or IEEE 802.16e-2005 standard. It should be noted that the mandatory and optional status of a particular feature within a WiMAX system profile may be different from what it is in the original IEEE standard. Currently, the WiMAX Forum has two different system profiles: one based on IEEE 802.16-2004, OFDM PHY, called the fixed system profile; the other one based on IEEE 802.16e-2005 scalable OFDMA PHY, called the mobility system profile. A certification profile is defined as a particular instantiation of a system profile where the operating frequency, channel bandwidth, and duplexing mode are also specified. WiMAX equipment are certified for interoperability against a particular certification profile.

WiMAX Forum is the Worldwide Microwave Interoperability Forum, a non-profit industrial body, dedicated to promoting the adoption of this technology and ensuring that different vendors' products will interoperate. WiMAX Forum will do this through developing conformance and interoperability test plans, selecting certification laboratories and hosting interoperability events for IEEE 802.16 equipment vendors.

The WiMAX Forum has thus far defined five fixed certification profiles and fourteen mobility certification profiles. To date, there are two fixed WiMAX profiles against which equipment have been certified. These are 3.5GHz systems operating over a 3.5MHz channel, using the fixed system profile based on the IEEE 802.16-2004 OFDM physical layer with a point-to-multipoint. MAC uses time division duplexing (TDD).

Band Index	Frequency Band	Channel Bandwidth	OFDM FFT Size	Duplexing	Notes
Fixed WiMAX Profiles					
1	3.5 GHz	3.5MHz	256	FDD	Products already certified
		3.5MHz	256	TDD	
		7MHz	256	FDD	
		7MHz	256	TDD	
2	5.8GHz	10MHz	256	TDD	
Mobile WiMAX Profiles					
1	2.3GHz–2.4GHz	5MHz	512	TDD	Both bandwidths must be supported by mobile station (MS)
		10MHz	1,024	TDD	
		8.75MHz	1,024	TDD	
2	2.305GHz–2.320GHz, 2.345GHz–2.360GHz	3.5MHz	512	TDD	
		5MHz	512	TDD	
		10MHz	1,024	TDD	
3	2.496GHz–2.69GHz	5MHz	512	TDD	Both bandwidths must be supported by mobile station (MS)
		10MHz	1,024	TDD	
4	3.3GHz–3.4GHz	5MHz	512	TDD	
		7MHz	1,024	TDD	
		10MHz	1,024	TDD	
5	3.4GHz–3.8GHz, 3.4GHz–3.6GHz, 3.6GHz–3.8GHz	5MHz	512	TDD	
		7MHz	1,024	TDD	
		10MHz	1,024	TDD	

Table 2:- Fixed and Mobile Initial Certification Profiles

2.2. Basic IEEE 802.16:-

Unlike other wireless standards, which address transmissions over a single frequency range, WiMAX allows data transport over multiple broad frequency ranges. Being able to work in multiple ranges maximizes the technology's ability

to transmit over the frequencies that will avoid interfering with other wireless applications.
The initial 802.16 standard operates in the 10 to 66 GHz range. At these higher frequencies, IEEE 802.16 requires a direct line of sight between senders and receivers. This reduces Multi-path distortion, which occurs when broadcast signals not following a line of sight bounce off large objects and end up out of synch, thereby scrambling the received transmission. IEEE 802.16 can provide single-channel data rates up to 75 Mbps on both the uplink and downlink.

2.3. IEEE 802.16 Extensions:-

IEEE 802.16 has adopted several extensions to the technology's basic standard. Some of the extensions have been reviewed as follows:-

2.3.1. IEEE 802.16a:-

The IEEE developed IEEE 802.16a for use in licensed and license-exempt frequencies from 2 to 11 GHz. At the lower ranges, the signals can penetrate barriers and thus do not require a line of sight between transceiver and antenna. This enables more flexible WiMAX implementations while maintaining the technology's data rate and transmission range.
IEEE 802.16a supports mesh deployment, in which transceivers can pass a single communication on to other transceivers, thereby extending basic 802.16's transmission range.

2.3.2. IEEE 802.16b:-

This extension increases the spectrum and the technology can be used in the 5 and 6 GHz frequency bands and provides quality of service. WiMAX provides QoS to ensure priority transmission for real-time voice and video and to offer differentiated service levels for different traffic types.

2.3.3. IEEE 802.16c:-

IEEE 802.16c represents a 10 to 66 GHz system profile that standardizes more details of the technology. This encourages more consistent implementation and, therefore, interoperability.

2.3.4. IEEE 802.16d:-

IEEE 802.16d includes minor improvements and fixes to IEEE 802.16a. This extension creates system profiles for compliance testing of IEEE 802.16a devices.

2.3.5. IEEE 802.16e:-

IEEE 802.16e will standardize networking between carrier's fixed base stations and mobile devices, rather than just between base stations and fixed recipients.

IEEE 802.16e would enable the high-speed signal handoffs necessary for communications with users moving at vehicular speeds.

2.4. Salient features of WiMAX:-

WiMAX is a very flexible wireless broad band technology that has a lot to offer, some of which are described below:-

2.4.1. High data rates:-

WiMAX offers very high data rates. In fact, the highest data rate that WiMAX can offer at its physical layer is around 74 Mbps (when using the 20MHZ spectrum). This peak data rate is achieved by using 64 QAM. The data rate can exceed this value if multiple high efficiency antennas are used.

2.4.2. OFDM based physical layer:-

To ensure the capability to work in NLOS (Non Line Of Sight) conditions and to resist against multipath and shadowing effects the WiMAX physical layer (PHY) has been designed on the concepts of Orthogonal Frequency Division Multiplexing (OFDM).

2.4.3. Adaptive modulation and coding (AMC):-

A number of adaptive modulation and forward error correction schemes are supported by WiMAX. WiMAX allows the scheme to be changed on a per user and per frame basis, based on channel conditions. This increases the throughput in the system. In the algorithm each user is provided the highest modulation and coding scheme as dictated by the signal to noise and interference ratio for the particular user.

2.4.4. Scalable bandwidth and data rate support:-

WiMAX has a scalable physical-layer architecture that allows for the data rate to scale easily with available channel bandwidth. This scalability is supported in the OFDMA mode, where the FFT (fast fourier transform) size may be scaled based on the available channel bandwidth. For example, a WiMAX system may use 128, 512, or 1,024-bit FFTs based on whether the channel bandwidth is 1.25MHz, 5MHz, or 10MHz, respectively. This

scaling may be done dynamically to support user roaming across different networks that may have different bandwidth allocations.

2.4.5. Link-layer retransmissions:-

For connections that require enhanced reliability, WiMAX supports automatic retransmission requests (ARQ) at the link layer. ARQ-enabled connections require each transmitted packet to be acknowledged by the receiver; unacknowledged packets are assumed to be lost and are retransmitted. WiMAX also optionally supports hybrid-ARQ, which is an effective hybrid between FEC and ARQ.

2.4.6. Support for TDD and FDD:-

IEEE 802.16-2004 and IEEE 802.16e-2005 supports both time division duplexing and frequency division duplexing, as well as a half-duplex FDD, which allows for a low-cost system implementation. TDD is favored by a majority of implementations because of its advantages: (1) flexibility in choosing uplink-to-downlink data rate ratios, (2) ability to exploit channel reciprocity, (3) ability to implement in non-paired spectrum, and (4) less complex transceiver design. All the initial WiMAX profiles are based on TDD, except for two fixed WiMAX profiles in 3.5GHz.

2.4.7. Orthogonal frequency division multiple access (OFDMA):-

Mobile WiMAX uses OFDMA as a multiple-access technique, whereby different users can be allocated different subsets of the OFDM tones. OFDMA facilitates the exploitation of frequency diversity and multi-user diversity to significantly improve the system capacity.

2.4.8. Flexible and dynamic per user resource allocation:-

Both uplink and downlink resource allocation are controlled by a scheduler in the base station. Capacity is shared among multiple users on a demand basis, using a burst TDM scheme.

2.4.9. Support for advanced antenna techniques:-

The WiMAX solution has a number of hooks built into the physical-layer design, which allows for the use of multiple-antenna techniques, such as beam forming, space-time coding, and spatial multiplexing. These schemes can be used to improve the overall system capacity and spectral efficiency by deploying multiple antennas at the transmitter and/or the receiver.

2.4.10. Quality-of-service support:-

The WiMAX MAC layer has a connection-oriented architecture that is designed to support a variety of applications, including voice and multimedia services. The system offers support for constant bit rate, variable bit rate, real-time, and non-real-time traffic flows, in addition to best-effort data traffic. WiMAX MAC is designed to support a large number of users, with multiple connections per terminal, each with its own QoS requirement.

2.4.11. Support for mobility:-

The mobile WiMAX variant of the system has mechanisms to support secure seamless handovers for delay-tolerant full-mobility applications, such as VoIP. The system also has built-in support for power-saving mechanisms that extend the battery life of handheld subscriber devices. Physical-layer enhancements, such as more frequent channel estimation, uplink sub channelization, and power control, are also specified in support of mobile applications.

2.4.12. IP-based architecture:-

The WiMAX Forum has defined a reference network architecture that is based on an all-IP platform. All end-to-end services are delivered over an IP architecture relying on IP-based protocols for end-to-end transport, QoS, session management, security and mobility. Reliance on IP allows WiMAX to ride the declining cost curves of IP processing, facilitate easy convergence with other networks, and exploit the rich ecosystem for application development that exists for IP.

Medium Access Control layer (MAC)

3. THE MEDIUM ACCESS CONTROL (MAC):-

The WiMAX MAC protocol is connection oriented and designed for point-to-multipoint broadband wireless access applications. It addresses the need for very high bit rates, both UL (to the BS) and DL (from the BS). The medium access algorithm and bandwidth allocation algorithm must accommodate hundreds of terminals per channel and terminals may be shared by multiple end users. The users require the services according to their nature and include legacy time-division multiplex (TDM) voice and data, IP connectivity, and packetized VoIP. To support various services, the WiMAX MAC must accommodate both continuous and bursty traffic. Furthermore, QoS may be assigned for these services to keep with the traffic types. The WiMAX MAC provides a lot of service types similar to the classic asynchronous transfer mode (ATM) service.
The WiMAX MAC also supports a variety of backhaul requirements, such as asynchronous transfer mode (ATM) and packet-based protocols. Convergence sublayers map the transport-layer-specific traffic to a MAC that is flexible enough to efficiently carry any traffic type. The convergence sublayers and MAC work together with such features as payload header suppression, packing, and fragmentation to carry traffic in a form that is often more efficient than the original transport mechanism[18].

3.1. MAC Protocol Data Unit:-

Each protocol data unit (PDU) is comprised of a generic MAC header (GMH), a payload, and an optional cyclic redundancy check (CRC). The GMH defines the contents of the payload and starts at the most significant bit (MSB). The payload consists of zero or more subheaders and MAC service data units (SDUs). The length of the payload may vary [16].

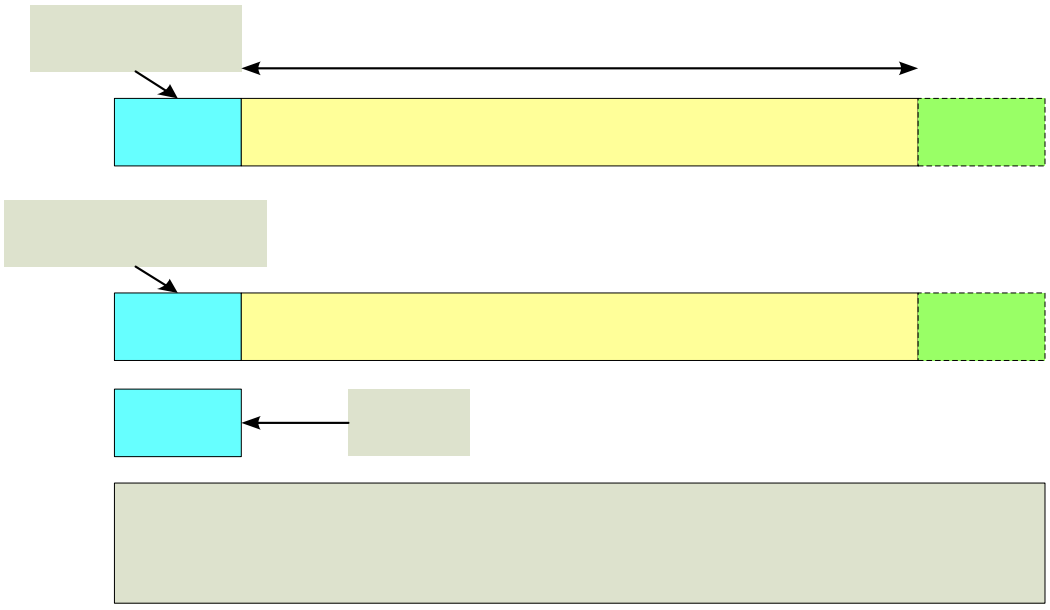


Figure 4:- IEEE 802.16 MAC protocol data units.

There are two formats defined for the MAC header. The GMH is used for MAC PDUs that contain MAC management messages or convergence sublayer data. The bandwidth request header is used when requesting additional bandwidth. The two headers are distinguished by the single-bit header type (HT) field, which is zero for the generic header and one for the bandwidth request header[16].

3.2. Generic MAC Header:-

The GMH, shown below, is encoded from the HT field on. It is 6 bytes in length and consists of 12 fields. Two of these fields, which are 1 bit in length each, are reserved for future use. The remaining fields are defined in table as follows:-
The type field of the GMH is used to indicate what type of subheader or special payload is included in the message.

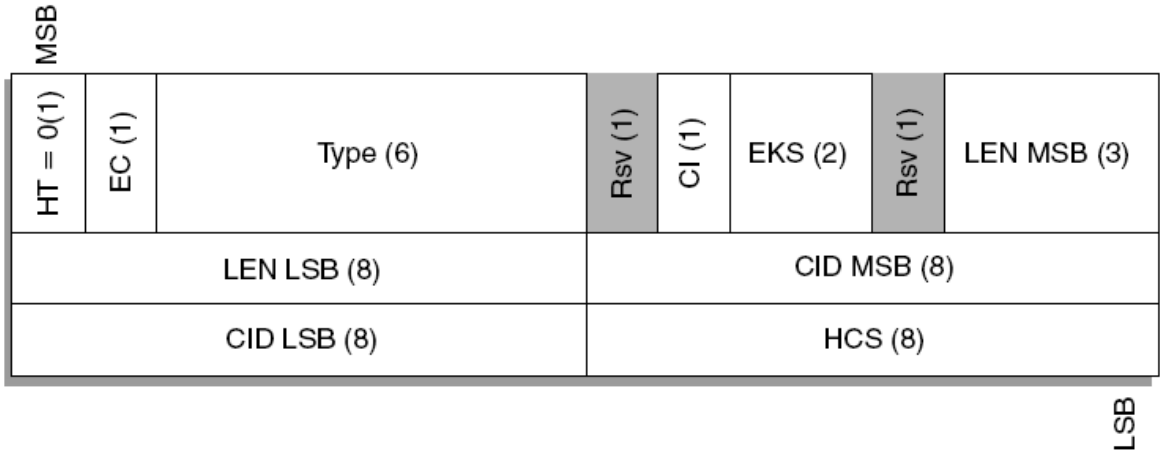


Figure 5: - Generic MAC Header[4]

The Generic MAC Header fields are described by the following table:-

Generic MAC Header Fields

Name	Length (Bits)	Description
CI	1	CRC indicator 1 = CRC is included in the PDU by appending it to the payload after encryption if any 0 = No CRC is included
CID	16	Connection identifier
EC	1	Encryption control 0 = Payload is not encrypted 1 = Payload is encrypted
EKS	2	Encryption key sequence The index of the traffic encryption key (TEK) and initialization vector used to encrypt the payload. This field is only meaningful if the EC field is set to 1
HCS	8	Header check sequence An 8-bit field used to detect errors in the header
HT	1	Header type Shall be set to zero
LEN	11	Length The length in bytes of the MAC PDU including the MAC header and the CRC if present
Type	6	This field indicates the subheaders and special payload types present in the message payload

Table 3:- Generic MAC Header Fields[4]

3.3. Bandwidth Request Header:-

The bandwidth request header, shown below, has no payload and consists of only the header. It is 6 bytes in length and consists of 8 fields in the following table. Like the GMH, the bandwidth request header is encoded from the HT field on.

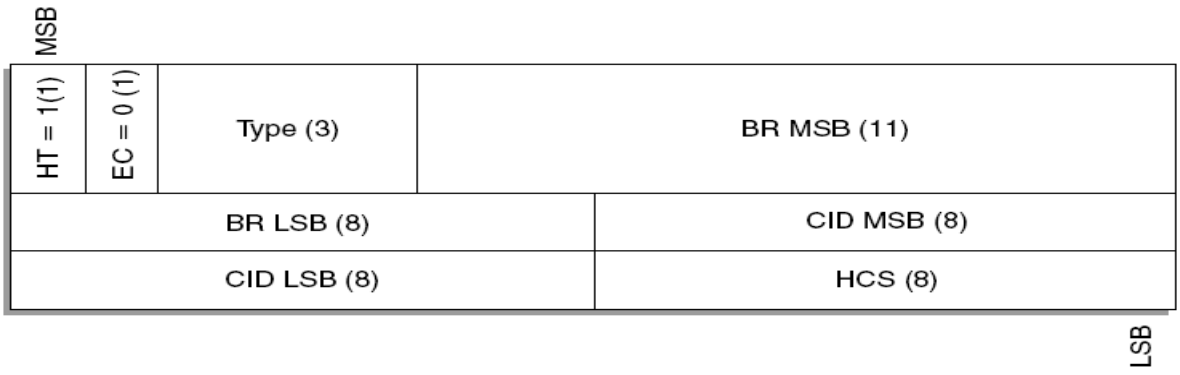


Figure 6:- Bandwidth Request Header

Name	Length (Bits)	Description
BR	19	Bandwidth request The number of bytes of uplink bandwidth requested by the subscriber station. The bandwidth request is for the CID. The request shall not include any PHY overhead
CID	16	Connection identifier
EC	1	Always set to zero
HCS	8	Header check sequence An 8-bit field used to detect errors in the header
HT	1	Header type = 1
Type	3	Indicates the type of bandwidth request header

Table 4: - Bandwidth Request Header Fields

3.4. Medium Access Control Details:-

The WiMAX MAC layer consists of three sublayers, Service Specific Convergence Sublayer (CS), the Common Part Sublayer (CPS) and the Security Sublayer (SS). The Convergence Sublayer transforms the data transferring between higher layers and the CS layer. CS has two types: ATM convergence sublayer for ATM networks and services, and packet convergence sublayer for packet data services like Ethernet, PPP, IP and VLAN. The CS layer receives data from higher layers, classifies data as ATM cell or packet and forwards frames to CPS layer.

The CPS layer is the core of the WiMAX MAC. It defines all methods for connection management, bandwidth distribution, request & grant, system access procedure, uplink scheduling, connection control and automatic repeat request (ARQ). MAC Service Access Point (MAC SAP) maintains the communications between the CS and the CPS. The basic functions of communication processes include creation, modification, deletion of connection and transportation of data over the channel.

The Security Sublayer is responsible for the encryption and decryption of data that is coming and leaving the PHY layer. Authentication and secure key exchange are also used. It carries 56-bit DES encryption for traffic and 3-DES encryption for key exchanges. In WiMAX network, the BS has 48-bit base station ID, which is not a MAC address while SS has 48-bit IEEE 802.3 MAC address [19].

3.4.1. Service-Specific Convergence Sublayers:-

There are two general service-specific convergence sublayers in IEEE 802.16 Standard that map services to and from IEEE 802.16 MAC connections. The ATM convergence sublayer for ATM services and the packet convergence sublayer

for packet-based services such as IP, Ethernet and VLAN. The main purpose of this sublayer is to classify service data units (SDUs) to the proper MAC connection, preserve or enable QoS, and enable bandwidth allocation. The mapping forms may vary due to the type of service. Furthermore, more complicated functions are also provided by the convergence sublayers such as payload header suppression and reconstruction to enhance airlink efficiency. [18]

3.4.2. Common Part Sublayer:-

The IEEE 802.16 MAC supports point-to-multipoint architecture with a central BS handling multiple independent sectors simultaneously. The downlinks (to SSs) are multiplexed in TDM fashion. The uplink (to BS) is shared between SSs in TDMA fashion.
The IEEE 802.16 MAC is connection-oriented. All services are mapped to a connection even if it is a connectionless service inherently. It enables service to have the abilities such as requesting bandwidth, associating QoS and traffic parameters, transporting and routing data to the appropriate convergence sublayer, and all other actions associated. Connections are identified by 16-bit connection identifiers (CIDs) and may require continuously granted bandwidth or bandwidth on demand.
There is a standard 48-bit MAC address in each SS, but this serves mainly as an equipment identifier, since the primary addresses used during operation are the CIDs. While entering the network, the SS is assigned three management connections per direction. Three different QoS requirements are needed due to these three connections which may have different management levels. The first one is the basic connection, which is used for the transfer of short, time-critical MAC and radio link control (RLC) messages. The primary management connection is used to transfer longer, more delay-tolerant messages such as authentication and connection setup. The secondary management connection is used for the transfer of standards-based management messages such as Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), and Simple Network Management Protocol (SNMP). Except these management connections, transport connections are allocated for the contracted services by SSs. Transport connections are unidirectional for accommodating different uplink and downlink QoS and traffic parameters; they are usually assigned to services in pairs.

3.4.3. Security Sublayer:-

The stated purpose of the Security Sublayer is to prevent eavesdropping on user data as it traverses the wireless link. With the exception of MAC management messages, all data traffic between the BS and SS is encrypted. However, the main focus of the Security Sublayer is on protecting service providers against theft of service, rather than protecting network users. Encrypting user data is simply a very desirable means to the end of preventing theft of service. It is also important to note that the security layer only protects data at the Open System

Interconnection (OSI) layer two level. Both physical and higher layer security technologies would need to be integrated to provide a highly secure, routable communications network.

To manage the exchange and synchronization of encryption keys, IEEE 802.16's Security Sublayer employs the Privacy Key Management (PKM) protocol from the DOCSIS BPI and specification that is commonly used for cable modems. The protocol employs several different keys when setting up privacy encryption.

These are summarized in the following table. During the initial startup and ranging procedure, the SS submits its X.509 Digital Certificate to the BS. The BS verifies the authenticity of the certificate. If the SS is authorized to join the network, the BS uses the SS's Public Key to encrypt an Authorization Key (AK). The AK is used in several different ways. It is used to derive a Key Encryption Key (KEK). It is also used to derive Hashed Message Authentication Code (HMAC) keys that are used in the generation and verification of MAC management messages. Finally, the KEK is used to protect a Traffic Encryption Key (TEK) that is generated by the BS, and sends it to the SS. The TEK is the key actually used to encrypt data traffic exchanged between the BS and SS.

The standard ensures that an SS is always in possession of valid encryption keys. For both authentication and traffic encryption keys, SSs are given two sets of keys with staggered lifetimes. The key changeover schemes used for AKs and TEKs are very similar and ensure an orderly transition between key material generations.

Key	Generated by	Used for	Lifetime
Public/Private Key Pair	Manufacturer	- SS authentication - exchanging AK	Permanent
Authentication Key (AK)	BS	- generating KEKs - Calculating HMAC digests - Verifying received HMAC digests	1 day to 70 days
Key Encryption Key (KEK)	BS, SS	- encrypting TEK for transmission (BS) -decrypting TEK for use (SS)	Same as AK
Traffic Encryption Key (TEK)	BS	- encrypting data traffic	30 minutes to 7 days

Figure 7: - Summary of Cryptographic Keys Associated with the Privacy Sublayer

3.5. Network Entry and Initialization:-

When an MS acquires the network after being powered up, a WiMAX network undergoes various steps. An overview of this process, also referred to as network entry, is shown in Figure 8.

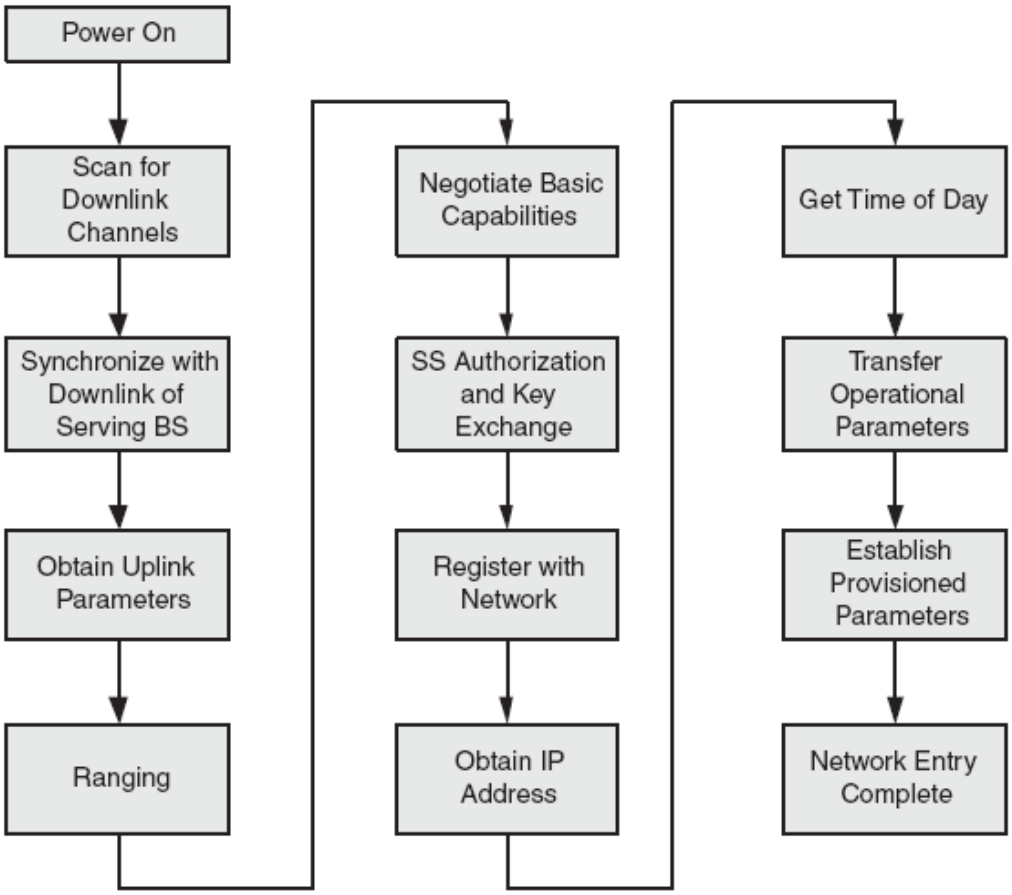


Figure 8:- Network Entry Procedure

3.5.1. Scan and Synchronize Downlink Channel:-

When an MS is powered up, it first scans the allowed downlink frequencies to determine whether it is presently within the coverage of a suitable WiMAX network. Each MS stores a nonvolatile list of all operational parameters, such as the DL frequency used during the previous operational instance. The MS first attempts to synchronize with the stored DL frequency. If this fails, the MS then scans other frequencies in an attempt to synchronize with the DL of the most suitable BS. Each MS also maintains a list of preferred DL frequencies, which can be modified to suit a service provider's network.

During the DL synchronization, the MS listens for the DL frame preambles. When one is detected, the MS can synchronize itself with respect to the DL transmission of the BS. Once it obtains DL synchronization, the MS listens to the various control messages, such as FCH, DCD, UCD, DL-MAP, and UL-MAP, that follow the preamble to obtain the various PHY- and MAC related parameters corresponding to the DL and UL transmissions.

3.5.2. Obtain Uplink Parameters:-

Based on the UL parameters decoded from the control messages, the MS decides whether the channel is suitable for its purpose. If the channel is not suitable, the MS goes back to scanning new channels until it finds one that is suitable. If the channel is deemed usable, the MS listens to the UL MAP message to collect information about the ranging opportunities.

3.5.3. Perform Ranging:-

At this stage, the MS performs initial ranging with the BS to obtain the relative timing and power-level adjustment required to maintain the UL connection with the BS. Once the UL connection has been established, the MS should do periodic ranging to track timing and power-level fluctuations. These fluctuations can arise because of mobility, fast fading, shadow fading, or any combinations thereof. Since the MS does not have a connection established at this point, the initial ranging opportunity is contention based.

3.5.4. Negotiate Basic Capabilities:-

After initial ranging, the MS sends an SBC-REQ message informing the BS about its basic capability set, which includes various PHY and bandwidth-allocation-related parameters. On the reception of this message, the BS responds with an SBC-RSP, providing the PHY and bandwidth-allocation parameters to be used for UL and DL transmissions. The operational PHY and bandwidth-allocation parameters can be the same as the basic capability set of the SS or a subset of it.
The various PHY and bandwidth-allocation-related parameters which the MS sends to the BS in the SBC-REQ message are shown in the table as follows:-

PHY Related Parameters	Meaning
Transmission gap	The transmission gap between the UL and DL subframe supported by the SS for TDD and HF-FDD
Maximum transmit power	Maximum transmit power available for BPSK, QPSK, 16 QAM, and 64 QAM modulation
Current transmit power	The transmit power used for the current MAC PDU (containing the SBC-REQ message)
FFT size	The supported FFT sizes (128, 512, 1,024, and 2,048 for OFDMA mode; 256 for OFDM mode)
64 QAM support	Support for 64 QAM by the modulator and demodulator
FEC support	Which optional FEC modes are supported: CTC, LDPC, and so on
HARQ support	Support for HARQ
STC and MIMO support	The various space/time coding and MIMO modes
AAS private MAP support	Support for various AAS private MAP
Uplink power–control support	Uplink power-control options (open loop, closed loop, and AAS preamble power control)
Subcarrier permutation support	Support for various optional PUSC, FUCSC, AMC, and TUSC modes
Bandwidth-Allocation-Related Parameters	
Half-duplex/full-duplex FDD support	Support for half-duplex and full-duplex FDD modes in case of FDD implementation

Table 5:- Contents of SBS-REQ message[16]

3.5.5. Register and Establish IP Connectivity:-

After negotiating the basic capabilities and exchanging the encryption key, the MS registers itself with the network. In WiMAX, registration is the process by which the MS is allowed to enter the network and can receive secondary CIDs. The registration process starts when the MS sends a REG-REQ message to the BS. The message contains a hashed message authentication code (HMAC), which the BS uses to validate the authenticity of this message. Once it determines that the request for registration is valid, the BS sends to the MS a REG-RSP message in which it provides the secondary management CID. In the REG-REQ message, the MS also indicates to the BS its secondary capabilities not covered under the basic capabilities, such as IP version supported, convergence sublayer supported, and ARQ support. The MS may indicate the supported IP versions to the BS in the REG-REQ message, in which case the BS indicates the IP version to be used in the REG-RSP message. The BS allows the use of exactly one of the IP versions supported by the MS. If the information about the supported IP version is omitted in the REG-REQ message, the BS assumes that the MS can support only IPv4.

After receiving the REG-RSP message from the BS, the SS can use DHCP to obtain an IP address.

3.5.6. Establish Service Flow:-

The creation of service flows can be initiated by either the MS or the BS, based on whether initial traffic arrives in the uplink or the downlink. When an MS chooses to initiate the creation of a service flow, an MS sends a DSA-REQ message containing the required QoS set of the service flow (Figure 9.8). On receipt of the DSA-REQ message, the BS first checks the integrity of the message and sends a DSX-RVD message indicating whether the request for a new service flow was received with its integrity preserved. Then the BS checks whether the requested QoS set can be supported, creates a new SFID and sends an appropriate DSA-RSP indicating the admitted QoS set. The MS completes the process by sending a DSA-ACK message.

If BS needs to initiate the creation of a service flow, it first checks whether the MS is authorized for such service and whether the requested level of QoS can be supported. The request for such service usually comes from a higher-layer entity and is outside the scope of the IEEE 802.16e.2005/802.16-2004 standard. If the MS is authorized for service, the BS creates a new SFID and sends a DSA-REQ message with the admitted QoS set and the CID to be used. On receipt of this request, the MS sends a DSA-RSP message indicating its acceptance. The BS completes this process by sending a DSA-ACK message. After the creation of the requested service flow, the MS and the BS are ready to exchange data and management messages over the specified CID.

Vulnerability

4.1. CCM Mode of Operation:-

CCM is a mode of operation for symmetric block ciphers. It ensures confidentiality as well as authenticity of the transmitted data, by combining both Counter mode and Cipher Block Chaining-Message Authentication code (CBC-MAC) algorithm [12] . CCM is based on an approved symmetric key block cipher algorithm whose block size is 128 bits, such as the Advanced Encryption Standard (AES) algorithm currently specified in Federal Information Processing Standard (FIPS) Pub. 197 [3]; thus, CCM cannot be used with the Triple Data Encryption Algorithm [2], whose block size is 64 bits. It is considered as a block cipher algorithm having a block size of 128-bits.
The input to CCM includes three elements [5]:

1. Data that will be both authenticated and encrypted, called the payload.
2. Associated data, e.g., a header, that will be authenticated but not encrypted
3. A unique value, called a nonce, that is assigned to the payload and the associated data

The whole process of CCM is divided into following two processes:

1. Generation-encryption
2. Decryption-verification

4.1.1. Generation – Encryption:-

To ensure Authenticity, Cipher Block Chaining-Message Authentication code (CBC-MAC) algorithm is applied to payload, associated data and the nonce (PN) to generate MAC. To ensure Confidentiality, the Payload, MAC, Associated data (Generic MAC header (GMH)) and the Nonce (PN) are encrypted by using AES in counter mode of operation. The result obtained is a ciphertext. Thus, CCM algorithm increases the size of the MPDU by 64 bits (size of encrypted MAC).
Before encrypting the payload, all the subheaders are prepended to it. The processes of fragmentation and packing are also incorporated in the standard.

4.1.2. Fragmentation Process:-

The process by which one large size MAC SDU is divided into two or more MAC PDUs is called fragmentation. This process of fragmentation is incorporated in the standard by including fragmentation subheader.

4.1.3. Packing Process:-

The process of combining variable size MAC SDUs into a single large size MAC PDU is called packing. Packing subheaders are used by the standard to incorporate packing.

Depending upon the size of the MAC SDUs, a single large MAC SDU can be fragmented into multiple fragments or a large number of small MAC SDUs can be packed into a single MAC PDU, and accordingly all the subheaders are prepended to the payload. Subheaders are also get encrypted along with the payload during the process of counter mode encryption in the CCM algorithm. In other words all the subheaders which are prepended to the payload before encryption are now become part of payload.
After prepending all the relevant subheaders, the payload and the associated data (PN, GMH) are authenticated by using AES in CBC mode to generate MAC. The CCM Nonce block (N) is obtained by using PN and GMH (excluding HCS) fields of the MPDU as shown in Figure below [1].

Byte number	0 4	5 8	9 12
Field	Generic MAC header	*Reserved*	PN
Contents	Generic MAC header omitting HCS	0x00000000	packet number field from payload

Figure 9:- Nonce N construction

Initialization vector or Initial CCM block (Bo) used in CBC mode is constructed as shown in Figure below [1].

Byte number	0	1 13	14 15
Byte significance:			MSB LSB
Number of bytes	1	13	2
Field	Flag	Nonce	L
Contents	0x19	As specified in Figure 135a	Length of plain text payload

Figure 10:- Initial CCM block B_o

The generated MAC and the payload (including subheaders) are then encrypted by using AES in Counter mode to generate ciphertext. Counter blocks (Ctr_i) used in the counter mode are constructed as shown in Fig. 3 [1].

Byte number	0	1 13	14 15
Byte significance:			MSB LSB
Number of bytes	1	13	2
Field	Flag	Nonce	Counter
Contents	0x1	As specified in Figure 135a	i

Figure 11:- Initial Counter Ctr_i

The PN should be incremented by one to obtain a fresh PN for each MPDU so that it can never repeat for the same session key (TEK). Thus PN acts as unique nonce for each frame, and is protected by the session key.
The whole process of encryption is depicted in the Figure below.

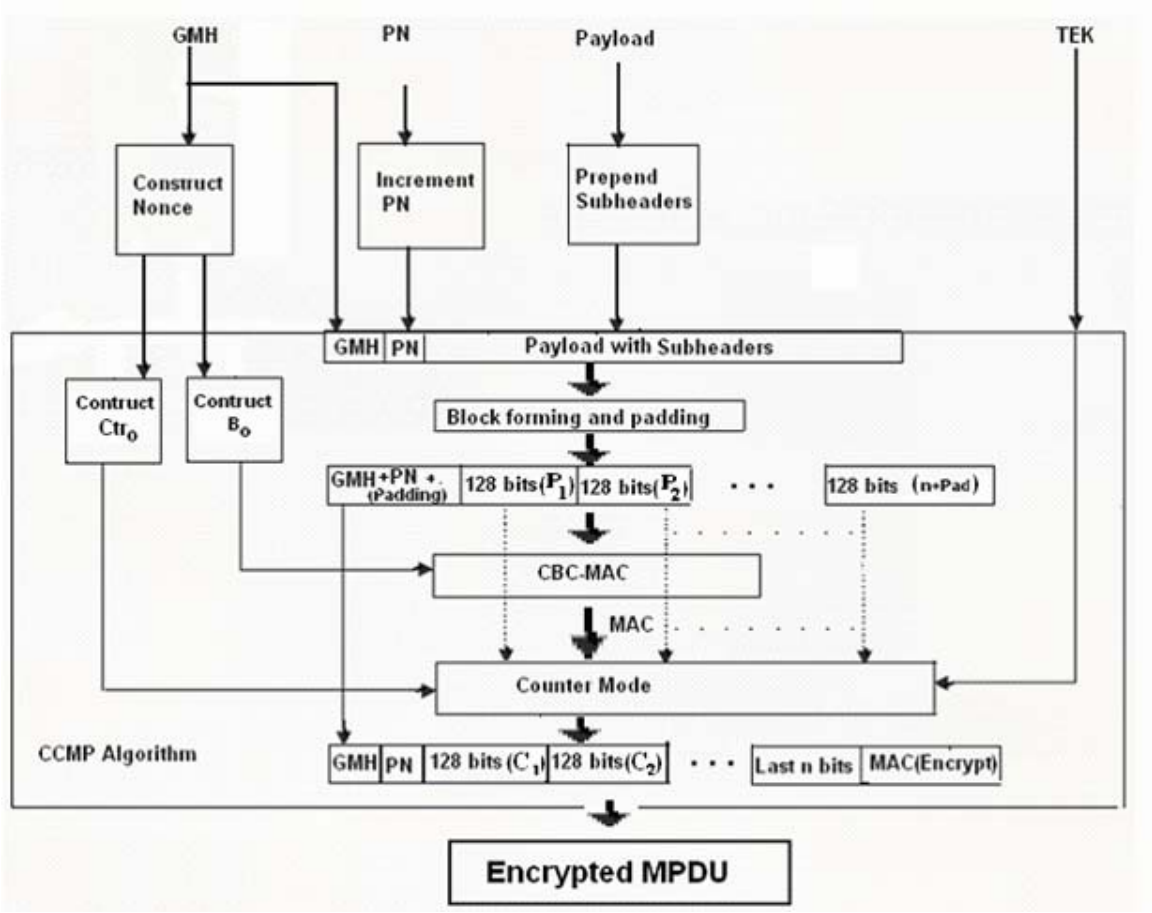


Figure 12:- CCM Encryption

Plaintext MPDU is divided into 128-bitss blocks by block forming and padding as shown in the diagram above. It is not essential that the whole payload is divided into 128-bits block. Padding is required at the last block (last n bits) of the payload to make it a 128-bit block. Separate padding is done to convert an associated data into a block size of 128-bits. 128-bits blocks of associated data and the payload are then input to the CBC-MAC algorithm to generate 128-bit unencrypted MAC. This MAC block and the payload blocks (P1,P2,…,Pn) are then input to the counter mode to convert them into an unreadable form, called ciphertext. Ciphertext consists of ciphertext payload blocks (C1,C2,…,Cn) and an encrypted MAC. Ciphertext payload is of the same size as that of the plaintext payload but the size of encrypted MAC reduces to 64-bits in length. Thus the size of encrypted MAC PDU increases by 64-bits. A MAC provides stronger assurance of authenticity than a checksum or an error detecting code. The verification of a (non-cryptographic) checksum or an error detecting code is designed to detect only accidental modifications of the data, while the verification

of a MAC, as occurs in CCM, is designed to detect intentional, unauthorized modifications of the data, as well as accidental modifications [5].
How the MAC is generated and how the encryption of payload and the MAC is done is illustrated in the diagram below [21].

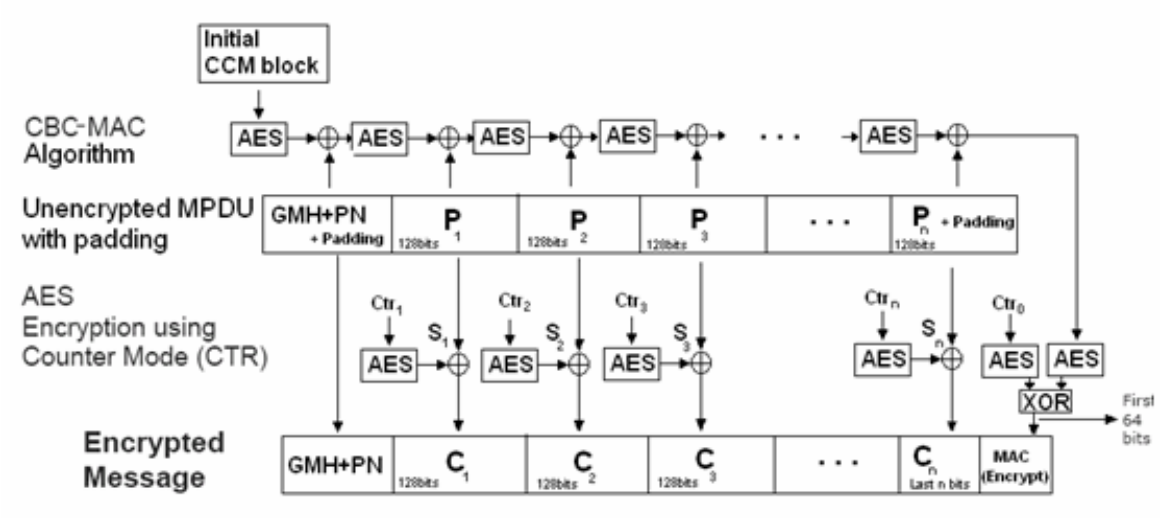


Figure 13:- CBC-MAC and Counter modes of CCM

Plaintext payload is divided into n blocks of 128 bits (P1,, P2, P3,…,Pn). Counter generation process is used to construct n+1 counter blocks. Initial counter (Ctr0) is used to encrypt MAC while the counter blocks Ctr1, Ctr2, Ctr3,…, Ctrn to encrypt P1,, P2, P3,…,Pn respectively. Every counter block is unique within the scope of same session key. The counter blocks used in different MPDUs are made unique by using unique nonce for each MPDU. Furthermore counter blocks within each MPDU are made unique by using unique [i]8q for each block encryption.

4.2. CCMP Decryption:-

Encrypted payload and MAC are decrypted by using session key, nonce, initial block and the initial counter block. CCM nonce block is constructed by using unencrypted fields of encrypted MPDU. CCM nonce block is used to construct initial CCM block (Bo) and counter blocks (Ctrj). By using counter blocks and Bo, decrypt the ciphertext to obtain plaintext payload and plaintext MAC. CBC-MAC mechanism is applied to payload and the associated data to verify MAC. If verification succeeds, then it means that the received data is unaltered.

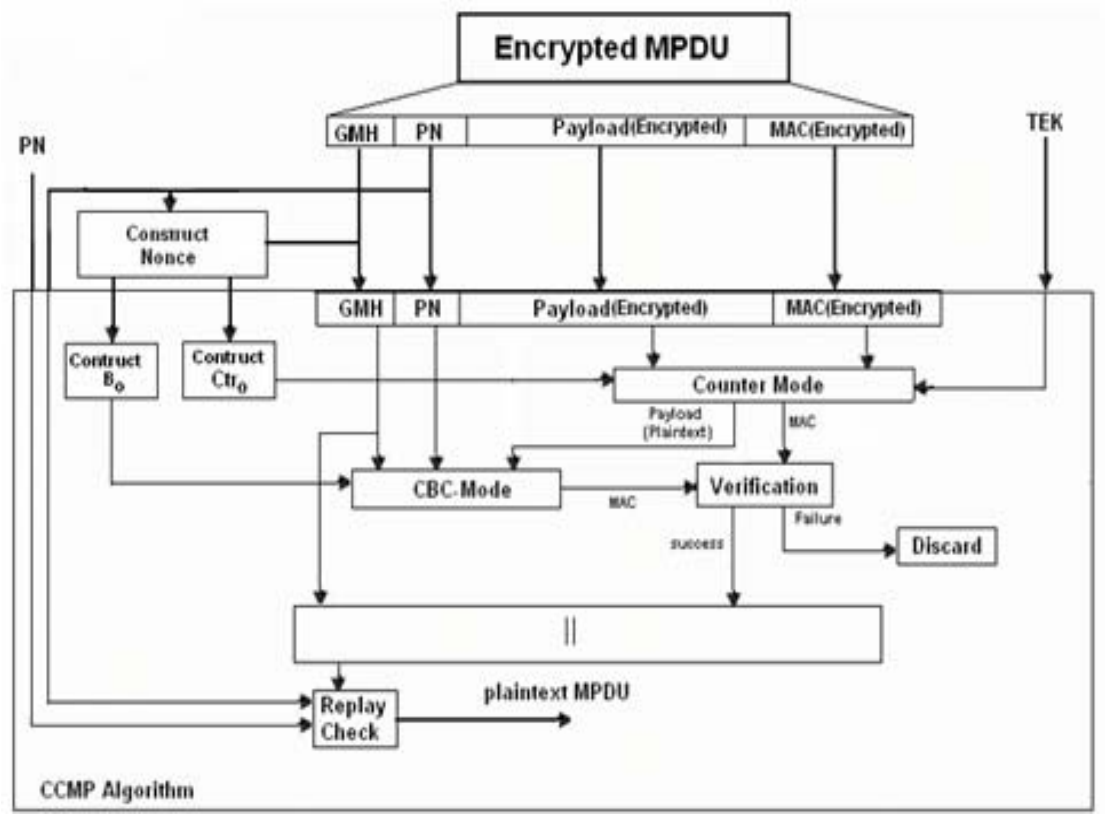


Figure 14:- CCM Decryption

4.3. Initial Counter Prediction:-

The counter blocks are given by:

$$Ctri = Flag \parallel Nonce \parallel [i]8q$$

Ctri corresponds to the counter block of ith iteration within one MPDU. Ciphertext blocks are given by:

$$Ci = Pi \ \Theta \ Si$$

Where $Si = e_k (Ctri)$

Pi and Si corresponds to plaintext and key stream blocks of ith iteration respectively. Ctr_0 is used to encrypt MAC while the Ctr_1, Ctr_2, Ctr_3,…, Ctr_n are used to encrypt P_1,,P_2, P_3,…,P_n respectively [20]. Nonce field is the only field which is responsible to make initial counter blocks unique among successive MPDUs, within the scope of single session key (TEK). Counter blocks, used in counter mode of CCMP, can be precomputed very easily because flag, nonce and counter (i) fields are predictable. Counter blocks are formatted as shown in fig [1]. flag field is one byte in length and it has a constant value of 0x01 [1].Nonce field is also predictable as described in previous section. C field of counter blocks is set to zero for encrypting MAC while values 1,2,…,n are used to encrypt P_1,,P_2, P_3,…,Pn blocks respectively. So the initial counter value and subsequently all counter values are predictable. Consequently, any unauthorized user (attacker) can construct the counter value without going through successful authentication process.

4.4. TMTO Precomputation Attack:-

The knowledge of the counter value to attacker provides the basis for TMTO precomputation attack. The TMTO attack [7] provides a shortcut over exhaustive key search. To launch TMTO attack, an attacker needs a larger storage space in order to decrease computational effort. By using techniques from error correcting codes, TMTO attack can be used even when there is uncertainty in plaintext during attack stage [8]. Precomputation attacks are launched on cryptographic systems using many keys. A system is considered as subverted if even a small fraction of traffic encryption keys are found by adversary [6], providing fruitful ground for precomputation attacks. Successs of TMTO attack is dependent on the amount of data available. IEEE 802.16 standard includes length field (LEN) of 11 bits in GMH. This LEN field includes length of GMH(6 bytes in length), Payload and 32 bit CRC. So the maximum size of the payload is given by:

maximum size of the payload = 2^11 - (length of GMH + length of CRC)
= 2^11 – (6+4)
= 2038 bytes

Size of PN is 32 bits [1], so 2^32 MPDUs are allowed per session key (TEK). Therefore, the amount of data is sufficient to launch TMTO attack. Counter mode is vulnerable to TMTO precomputation attack if counter update is predictable [9]. It is shown in this paper that both initial counter and its update are predictable. Therefore, TMTO attack is possible. Effective key size of TMTO is 2n/3 [7], where n is the cipher key size. So 128 bit AES key size in IEEE 802.16 standard reduces to effective key size of 85 bits as shown below:

Effective key size = 2n/3
= (2*128)/3 since n=128bits
≈ 85 bits

The 1996 ad-hoc report on minimal key lengths [10] recommended 75 bits key length for symmetric ciphers to provide adequate security at that time. [10] also recommends to add 14 bits to keep it secure for next 20 years atleast. Applying Moore's laws [11], if we add key bits for 8 years(1996 to 2004) and 5 more years for the validity of [1], then the recommended current strength for the cipher is 97 bits. In TMTO scenario, we deduced that the Effective key size of IEEE 802.16 AES counter mode in CCMP is 85 bits. The effective key size should be atleast equal to 97 bits to thwart the TMTO precomputation attack. Thus the security mechanism of IEEE 802.16 standard is vulnerable to TMTO attack. Following points are recommended to provide defence against TMTO precomputation attack [6]:

1. There must be 64 bits unpredictable value to the initial counter, which is considered as part of the AES CM
2. key, or
3. Use a predictable but uniformly distributed component in the initial counter, or
4. The key length should be larger than 128 bits.

IEEE 802.16 standard's security is vulnerable to precomputation attack as none of these recommendations has been incorporated in it.

Design

5.1. Defence against TMTO attack:-

As an interim solution, unpredictable reserved field is recommended to guard 802.16 wireless MANs against TMTO attack. A 32 bit reserved field is concatenated with the GMH and PN fields. Reserved field in the nonce should be set to any pseudo random number upon initialization / refreshness of traffic encryption key. These pseudo random 32 bits give 32 bit unpredictability to nonce and therefore 32 bit unpredictability to initial counter. These 32 bits can be considered as part of AES counter mode key. This strengthens the 128bit AES key by 32 bits. If TMTO attack is launched, the effective key size of AES becomes:

$$\text{Effective key size} = 2n/3$$
$$= (2*160)/3 \qquad \text{since } n = (128+32) = 160 \text{ bits}$$
$$\approx 106 \text{ bits}$$

The effective key size is greater than 97 bits and therefore provides a reasonable strength against TMTO attack. By initializing PN by a 32 bit pseudo random number upon initialization or refreshness of TEK, the effective key strength of 128 bit AES key further increases to 128 bits from 106 bits.

5.2. Per Packet Authentication Mechanism:-

In our devised mechanism the initial counter is generated from TEK by using PRF-128 as shown in Fig.7. Practices for generating random numbers are provided in [B30], which is also recommended by [1] in its subclause 7.5.4. It is suggested to add an encrypted nonce value to the MPDU before its transmission, in order to obtain per packet authentication instead of session based authentication.

TEK (first element of the encryption key (EK) array which is N[2*PN-1]= N[1]) is used to encrypt the first packet (PN=1) and an encrypted nonce value of N0(second element of encryption key array which is N[2*PN]= N[2]) is added to MPDU before transmission to the SS. The BS will be able to decrypt the packet only if it has a valid initial counter and the traffic encryption key (TEK in this case). BS will recover correct nonce (N0), only if it successfully decrypts the encrypted MPDU. This recovered nonce is used by BS to encrypt the next packet to the SS, and in addition to that it adds an encrypted nonce, N1 (N[3]), to MPDU before the packet is sent to SS. On reception, the SS will only be able to decrypt the packet successfully, if it has a valid initial counter and nonce (used as encryption key, N0 in this case). If SS successfully decrypts the encrypted MPDU, SS will recover correct nonce, N1. This recovered nonce is

used by SS to encrypt the next packet to the BS, and in addition to that it also adds an encrypted nonce, N2 (N[4]), to MPDU, before the packet is sent to BS. This process continues until renewal of TEK.

We can also summarize our proposed solution that if odd elements of array N[k] (when k=odd) are used to encrypt packet at one end (say BS), then even number of elements of array N[k] (k=even) are used to authenticate the packet at other end (SS). It provides per packet authentication as each packet is encrypted by using unique key. For retransmission, the packet is sent by using same nonce (nonce used previously to send same packet).

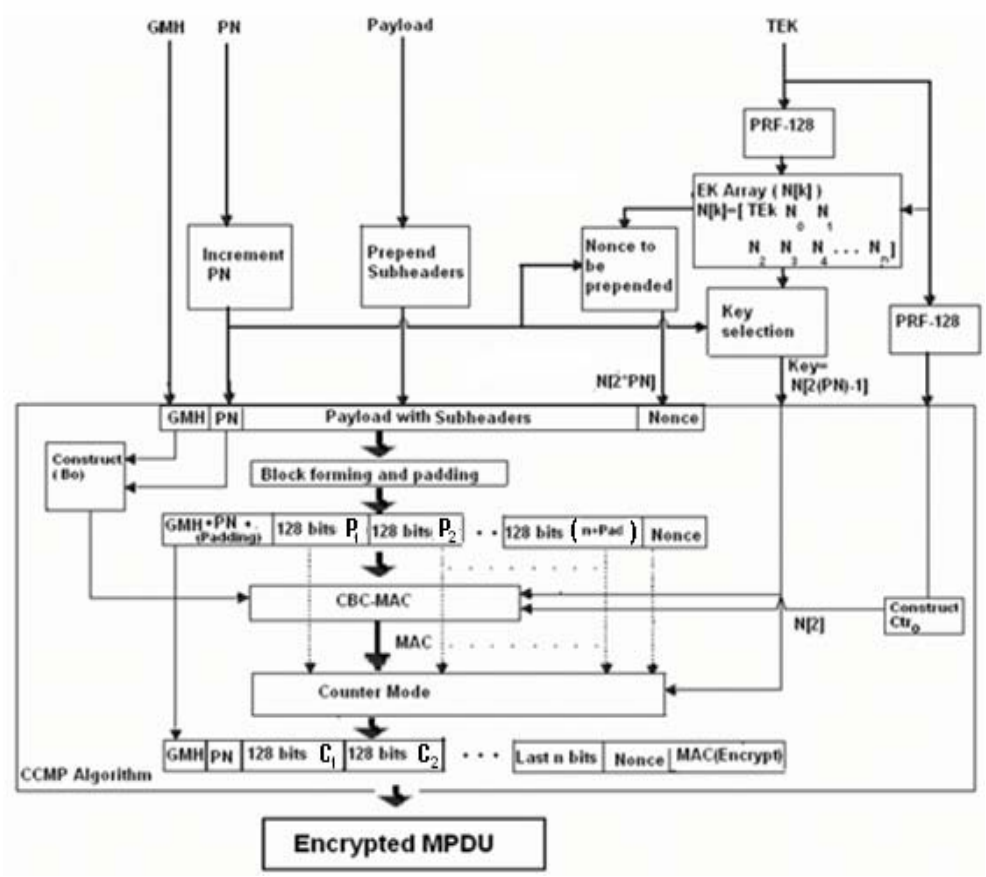


Figure 15:- Per Packet Mechanism

Simulations

6.1. Implementation of Security Sub layer in NS2:-

Ns is a discrete event simulator targeted at networking research. Ns provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks.
Network Simulator-2 can be installed on a Linux platform as well as on a windows platform using cygwin. We have used Red Hat Version 4 Enterprise Edition.

We are using the NIST's WiMAX module for our simulation. In the current module the PHY layer and MAC layer are implement. The module does not feature support for encryption and decryption. In fact the complete security sub layer was not implemented. It was a big task.
In ns2, two languages are used tcl and C/ C++.
We used C language to create support for implementation of AES in CCM mode for session based and packet based authentication mechanisms.

6.1.1. Session based Authentication Mechanism:-

For that purpose we had to create the following files:

aes3.cc
aes3.h
cbc3.cc
cbc3.h

Aes3.h and aes3.cc include the classes and function definitions for the implementation of AES (Advanced Encryption Standard) in ns2.
AES can be used in different modes. In IEEE 802.16 e standard the recommended mode of operation is CCM (Counter with CBC MAC). Cbc3.h and cbc.cc include the classes and function definitions necessary for the implementation of CCMP mode in ns2.
We had to modify the following files:

mac802_16BS.cc
mac802_16SS.cc
mac802_16pkt.h

The files mac802_16BS.cc and mac802_16SS.cc contain functions necessary for implementation of BS and SS objects respectively. We added support of encryption and decryption in these files.
mac802_16pkt.h contains packet header format.

6.1.2. Packet based Authentication Mechanism:-

For this purpose we had to create the following files:

blchain.cc
blchain.h

encrypt.cc
encrypt.h

blchain.h and blchain.cc include the classes and function definitions for the implementation of AES (Advanced Encryption Standard) in ns2 for packet based authentication. In these files new key is used for each packet.

We had to modify the following files:

mac802_16BS.cc
mac802_16SS.cc
mac802_16pkt.h

In order to compile ns2 to incorporate the changes we need to recompile the code. From ns-2.31 directory
execute:

. /configure;
make depend;
make;
make install;

Once the changes have been incorporated. We are ready to run a simulation. The simulation scripts are written in tcl. Visualization of the simulation is shown in the nam.

The simulation shows communication between a subscriber station and a base station. The packets sent are encrypted and decrypted in the background in C language. The same scenario is created for packet based authentication mechanism.

The following file containing the packets encrypted and decrypted was obtained.

```
//////////////////////////////////////
//////  TRANSMITTER  //////
//////////////////////////////////////


********** THE PLAIN TEXT IS: **********
53  56  4d  f  5d  23  56  5c  31  15  3e  1b  5a  3b  3f  1a  28  1a  48
24  b  44  43  1d  52  1e  3e  17  43  23  1d  2
**********  ROUND NO----------  0 **********


********** THE 128 BITS INPUT IS: **********
53  56  4d  f  5d  23  56  5c  31  15  3e  1b  5a  3b  3f  1a
```

********** THE CBC OUTPUT IS: **********
e1 d7 8d 24 e6 98 be 3b f3 e4 75 c6 17 e9 c1 4

********** THE OUTPUT OF COUNTER MODE IS: **********
59 c2 46 ba 1c 4d a6 19 c0 d6 aa 43 9c 68 d5 40
********** ROUND NO---------- 1 **********

********** THE 128 BITS INPUT IS: **********
28 1a 48 24 b 44 43 1d 52 1e 3e 17 43 23 1d 2

********** THE CBC OUTPUT IS: **********
97 53 48 3 ca 6f e1 f5 c ad 16 53 5 63 e2 c8

********** THE OUTPUT OF COUNTER MODE IS: **********
22 8e 43 91 4a 2a b3 58 a3 dd aa 4f 85 70 f7 58

********** THE CIPHER IS: **********
59 c2 46 ba 1c 4d a6 19 c0 d6 aa 43 9c 68 d5 40 22 8e
43 91 4a 2a b3 58 a3 dd aa 4f 85 70 f7 58 9d c7 43 b6
8b 1 11 b0 f1 c3 94 58 c6 53 ea 5a

********** TRANSMITTED CIPHER PACKET NO 0 AT 0.009996
****
59 c2 46 ba 1c 4d a6 19 c0 d6 aa 43 9c 68 d5 40 22 8e
43 91 4a 2a b3 58 a3 dd aa 4f 85 70 f7 58 9d c7 43 b6
8b 1 11 b0 f1 c3 94 58 c6 53 ea 5a

channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5, distCST_ = 513.3

//
////// TRANSMITTER //////
//

********** THE PLAIN TEXT IS: **********
16 3a 45 43 5d 38 b 2a 1d 49 15 13 54 25 62 18 f 46 d
1a 5b 50 38 49 3e 46 60 51 5 19 54 1b
********** ROUND NO---------- 0 **********

********** THE 128 BITS INPUT IS: **********
16 3a 45 43 5d 38 b 2a 1d 49 15 13 54 25 62 18

********** THE CBC OUTPUT IS: **********
a3 7b 86 35 bb 12 11 2e ce f2 21 4f 5 18 e5 19

********** THE OUTPUT OF COUNTER MODE IS: **********
1c ae 4e f6 1c 56 fb 6f ec 8a 81 4b 92 76 88 42
********** ROUND NO---------- 1 **********

********** THE 128 BITS INPUT IS: **********
f 46 d 1a 5b 50 38 49 3e 46 60 51 5 19 54 1b

********** THE CBC OUTPUT IS: **********
3c 2f 27 5b cc 22 6e 3a ae f1 aa 63 b5 65 2b 84

********** THE OUTPUT OF COUNTER MODE IS: **********
5 d2 6 af 1a 3e c8 c cf 85 f4 9 c3 4a be 41

********** THE CIPHER IS: **********
1c ae 4e f6 1c 56 fb 6f ec 8a 81 4b 92 76 88 42 5 d2 6
af 1a 3e c8 c cf 85 f4 9 c3 4a be 41 36 bb 2c ee 8d 4c
9e 7f f1 c3 94 58 c6 53 ea 5a

********** TRANSMITTED CIPHER PACKET NO 1 AT 0.010022
****
1c ae 4e f6 1c 56 fb 6f ec 8a 81 4b 92 76 88 42 5 d2 6
af 1a 3e c8 c cf 85 f4 9 c3 4a be 41 36 bb 2c ee 8d 4c
9e 7f f1 c3 94 58 c6 53 ea 5a

////////////////////////////////////
//////// RECIEVER ////////
////////////////////////////////////

******** ROUND NO---------- 0 *****

****** THE 128 BITS CIPHER IS: ******
59 c2 46 ba 1c 4d a6 19 c0 d6 aa 43 9c 68 d5 40

******* THE OUTPUT OF COUNTER MODE IS: ******

```
53  56  4d  f  5d  23  56  5c  31  15  3e  1b  5a  3b  3f  1a

*****  THE INPUT TO CBC IS: *****
53  56  4d  f  5d  23  56  5c  31  15  3e  1b  5a  3b  3f  1a

******  THE CBC OUTPUT IS: *****
e1  d7  8d  24  e6  98  be  3b  f3  e4  75  c6  17  e9  c1  4

********  ROUND NO----------  1 *****

****** THE 128 BITS CIPHER IS: ******
22  8e  43  91  4a  2a  b3  58  a3  dd  aa  4f  85  70  f7  58

******* THE OUTPUT OF COUNTER MODE IS: ******
28  1a  48  24  b  44  43  1d  52  1e  3e  17  43  23  1d  2

*****  THE INPUT TO CBC IS: *****
28  1a  48  24  b  44  43  1d  52  1e  3e  17  43  23  1d  2

******  THE CBC OUTPUT IS: *****
97  53  48  3  ca  6f  e1  f5  c  ad  16  53  5  63  e2  c8

********  ROUND NO----------  2 *****

****** THE 128 BITS CIPHER IS: ******
9d  c7  43  b6  8b  1  11  b0  f1  c3  94  58  c6  53  ea  5a

******* THE OUTPUT OF COUNTER MODE IS: ******
97  53  48  3  ca  6f  e1  f5  0  0  0  0  0  0  0  0

*****  THE INPUT TO CBC IS: *****
28  1a  48  24  b  44  43  1d  52  1e  3e  17  43  23  1d  2

****** THE ORIGINAL MAC WAS: *******
97  53  48  3  ca  6f  e1  f5  0  0  0  0  0  0  0  0

******* THE MAC IS: ******
97  53  48  3  ca  6f  e1  f5  0  0  0  0  0  0  0  0

Success
******* Recieved Packet No 0 at 0.010022 is  *******

****** THE RECOVERED PLAIN TEXT IS: ******
53  56  4d  f  5d  23  56  5c  31  15  3e  1b  5a  3b  3f  1a  28  1a  48
24  b  44  43  1d  52  1e  3e  17  43  23  1d  2
```

Algorithm

7. ALGORITHM:

The purpose of this code is to implement CCM (Counter with Cipher Block Chaining Mode) protocol used in WiMAX for authentication purposes. Since AES is different for both encryption and decryption (unlike DES) so we have to implement it separately. Further more encryption and decryption is implemented for both session based authentication and packet based authentication.
The scheme is as follows:
Initially the 256 bits frame is taken as input to the code through random generator. This frame is then fragmented into 128 bits packets which are passed one by one through CBC and then COUNTER mode. In the CBC mode, each 128 bit plain text is first XORed with the IV and then fed to the AES for encryption purposes. The most significant 64 bits of output of CBC mode in the last round of loop are stored as CBC MAC. Then this CBC MAC is appended with the plain text and passed on to the counter mode for further processing. In the COUNTER mode, the counter is fed to the AES for encryption. Fragmentation of the plain text is done again and the output of this AES is XORed with the Fragmented plaintext and the results are stored as the cipher text. Also the last 128 bits of counter mode's output are termed as encrypted MAC. This Cipher text is then transmitted along with encrypted MAC to the Subscriber Station.
At the subscriber station, the cipher is first fragmented again into 128 bit blocks and the resulting blocks are passed through the counter mode first. This generates the plaintext of the corresponding cipher text. Here, on decryption side, the AES used by both CBC and Counter modes is different from what we have used on encryption side. Here it is used in the decryption mode. The last 128 bits of the counter mode's output are referred CBC MAC. On Decryption side each output of the counter mode is fed to the CBC mode for the generation of CBC MAC. At the end both the MACs are compared. If found exactly same then success is printed otherwise the code displays failure.
In addition to this, the Initialization Vector is changed for every round i.e. the output of the CBC mode replaces the IV and the counter is also incremented for every 128 bit packet.
The only difference between packet based authentication scheme and session based authentication scheme is the generation of key. Here , in the former, we generate separate 128 bit key for every 128 bit packet through a random number generator unlike session based authentication which uses same key for the entire session.

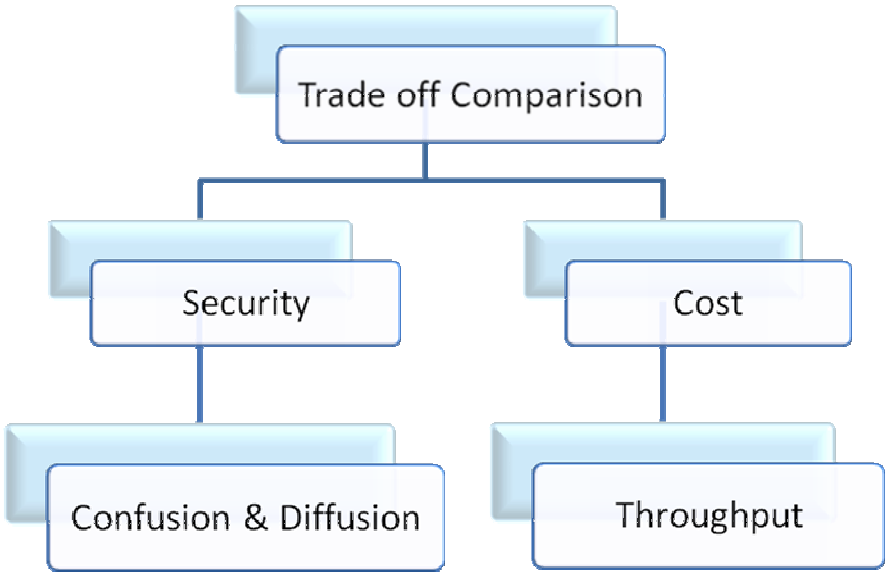
Future Work

8. Future Work:-

This section describes the guide line for any individual willing to continue the project.

8.1. Trade off Comparison

A trade off comparison can be done. It is a comparison in which the security of the algorithm can be weighted against its cost.



8.1.1. Security

By using the confusion and diffusion tools and using the key, cipher text and plain text generated as inputs, the values of confusion and diffusion can be computed for the session based and packet based authentication scenarios.

8.1.2. Cost

In this analysis, the throughput for Packet based authentication and Session based authentication will be calculated. And the results of the two scenarios will be compared.

Once the Security provided by the algorithm and its throughput has been calculated, we can weigh the additional security provided by the algorithm against the additional cost required.

Based on such a comparison we can force a change in the IEEE standard.

8.2. Development of complete security sub layer in ns2:-

In addition to the trade off comparison, one project can be the inclusion of security sub layer state machines and security related management messages by extending our work. It can be taken as a complete UG level project. This can then be sent to ns forum for integration into the network simulator. This will be a major contribution on part of MCS students in NS2.

Conclusion

9. Conclusion

Packet based Authentication mechanism provides integrity and confidentiality to users. It uses new key for every individual packet. As a consequence, the attacker now has a data bank in which every packet is encrypted with a new key . Thus disabling him to launch a TMTO attack. It thus provides unconditional security.
The proposed Packet Based Authentication Mechanism is not limited to WiMAX systems. Infact this can be applied to all wireless scenarios in which security is of prime importance such as military application etc. But like every other thing this enhanced security has a cost to be paid in terms of increased overhead.

References

10. References

[1] Institute of Electrical and Electronics Engineers, Inc., IEEE Std.802.16e-2005, Amendment to IEEE Standard forLocal and metropolitan area networks– Part 16: "Air Interface for Fixed and Mobile Broadband Wireless Access Systems:Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands", Dec, 2005.

[2] FIPS Publication 46-3, Data Encryption Standard (DES). U.S. DoC/NIST, October 25, 1999. Available at http://csrc.nist.gov/publications/.

[3] Specification for the Advanced Encryption Standard (AES), FIPS 197, U.S. National Institute of Standards and Technology. November 26, 2001. [Online] Available: http://www.nist.gov/aes

[4] D. Whiting, R. Housley, and N. Ferguson. "Counter with CBC-MAC (CCM)". RFC 3610, September 2003.

[5] NIST Special Publication 800-38C, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality". May 2004. [Online] Available: http://csrc.nist.gov/publications

[6] David A. McGrew, "Counter Mode Security: Analysis and Recommendations", Cisco Systems, November, 2002.

[7] M.E. Hellman, "A cryptanalytic time-memory trade-off", IEEE Transactions on Information Theory, July, 1980, pp. 401-406.

[8] D. A. McGrew and S. R. Fluhrer, "Attacks on Additive Encryption of Redundant Plaintext and Implications on Internet Security", The Proceedings of the Seventh Annual Workshop on Selected Areas in Cryptography (SAC 2000), Springer-Verlag, August, 2000. [Online] Available: http://www.mindspring.com/~dmcgrew/dam-srf-sac00.pdf

[9] Jin Hong, Palash Sarkar, "Rediscovery of Time Memory Tradeoffs", 2005. [Online] Available: http://cr.yp.to/2005-590/hong.pdf

[10] M. Blaze, W. Die, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Weiner, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security", January 1996. [Online] Available: http://www.counterpane.com/keylength.html

[11] Moore's law [Online] Available: http://www.Webopedia.com/TERM/M/Moores_Law.html

[12] D. Whiting, R. Housley, N. Ferguson, Counter with CBC-MAC (CCM). Available at http://csrc.nist.gov/ CryptoToolkit/modes/proposedmodes/.

[13] John.Wiley.and.Sons.The.Business.of.WiMAX.Jun.2006

[14] ITU. Telecommunications indicators update—2004. www.itu.int/ITU-D/ict/statistics/.

[15] In-stat Report. Paxton. The broadband boom continues: Worldwide subscribers pass 200 million, No.IN0603199MBS, March 2006.

[16] IEEE. Standard 802.16-2004. Part16: Air interface for fixed broadband wireless access systems. October 2004.

[17] IEEE. Standard 802.16e-2005. Part16: Air interface for fixed and mobile broadband wireless access systems—Amendment for physical and medium access control layers for combined fixed and mobile operation in licensed band. December 2005.

[18] Carl Eklund, Roger B. Marks, Kenneth L. Stanwood, and Stanley Wang, "IEEE Standard 802.16: A Technical Overview of the WirelessMANTM Air Interface for Broadband Wireless Access", IEEE Communications Magazine, 2002

[19] Jamshed Hasan, "Security Issues of IEEE 802.16 (WiMAX)", 2006

[20] Network Working Group [Online] Available: http://www.faqs.org/ftp/rfc/pdf/rfc3610.txt.pdf

[21] Opera-D13: Reference guide on the design of an integrated PLC network, including the adaptations to allow the carriers' carrier model [Online] Available: http:// www.ist-opera.org/drupal2/files/OP2_WP2_D13_v1.0.pdf