Technologies used in Physical MAC-CPS and MAC-Security Layers of IEEE 802.16j Mobile Multi-Hop Relay (MMR) Networks

D.SATISH KUMAR
Research Scholar /CSE
Anna University, Chennai
Tamil Nadu
INDIA
satishcoimbatore@yahoo.co.in
N.NAGARAJAN
Department of Computer science and Engineering
Coimbatore Institute of Engineering and Technology
Tamil Nadu
INDIA
swekalnag@gmail.com

Abstract : -The IEEE 802.16 standard was formed in 1998 and approved in Dec-2001, to develop air interface standard for wireless broadband. The relay task group of IEEE 802.16 standard extended the IEEE 802.16e-standard with a new standard called IEEE 802.16j mobile multi-hop relay (MMR) standard. The IEEE 802.16j standard supports multi-hop relay operation was a relay station relay packets between base station and subscriber station. This article provides insight and understanding of the IEEE 802.16j mobile multi-hop relay (MMR) networks and describes some of the technologies used in physical, MAC-CPS and MAC-security layers of IEEE 802.16j wireless communication. The current Technologies of Physical and MAC layers are SOFDMA, Mobile IEEE 802.16j MMR channel encoding process, Relay station grouping and Messages, Ideal mode operation, Paging and Location management, Privacy Key Management protocol, IEEE 802.16j MMR physical layer security, comparison of WIMAX OFDM, OFDMA and SOFDMA, Up-link Sub Frame: down link Sub Frame, IEEE 802.16 Protocol Stack, Privacy and Key Management Protocol and authorization. We have described completely about all the above technologies in this article.

Key-Words: - IEEE 802.16j MMR physical layer security, IEEE 802.16J MMR OFDM, Protocol Stack, Privacy and Key Management Protocol

1 Introduction

The new task group IEEE 802.16j-2009 standard [1] of IEEE 802.16 air interface for broadband wireless access was officially established in March 2006. In order to support the mobile multi-hop relay specification, mesh mode is removed from the IEEE 802.16 - 2009 standard [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13]. The specification is an amendment of the IEEE 802.16e standard [1] [15] [16] [17] [18] for achieving throughput enhancement and coverage extension. It provides multi hop wireless connectivity where traffic between a base station and a subscriber station can be relayed through a relay station. This system enables mobile stations to communicate with a base station through an intermediate relay station. The multi hop relay station is an optional deployment as shown in its architecture in fig 3, that may be used to provide additional coverage or performance advantage in an access network. The Relay Station may be fixed in place or, in the case of an access relay station, may be mobile access Relay Station. Most of the time, the relay station will act as a base station and will have its own physical cell identifier, and it should be able to transmit its own synchronization channels and control information. There should be no difference between cell control in there lay station and base station. The radio link originating or terminating at a mobile station is named as access link and the link between the base station and relay station or between a pair of relay stations is called as relay link. The access link and relay link can be used for

uplink and downlink data transmission. This standard defines the physical and the medium access control layer specifications for mobile multi hop relay networks. The medium access control layer supports functions such as network entry, bandwidth request, and forwarding of data units, connection management, and handover. The Physical layer adopts orthogonal frequency division multiple access as the primary channel access mechanism for non-line of sight communications in the frequency band below 11 GHz. Where multiple users are allocated a separate set of slots, so that they can communicate in parallel. It supports point to multipoint network topology where resource allocation is performed by the base station on a per connection basis, and the subscriber stations are treated equally. Multiple input multiple output techniques [19] has the ability to exploit non loss of sight channels and increase spectral efficiency compared to single input single output systems. Those techniques are able to provide high capacity and data rate without increasing bandwidth. The gain of multiple input multiple output [14] [16] includes multiplexing gains, diversity gains, and array gains.

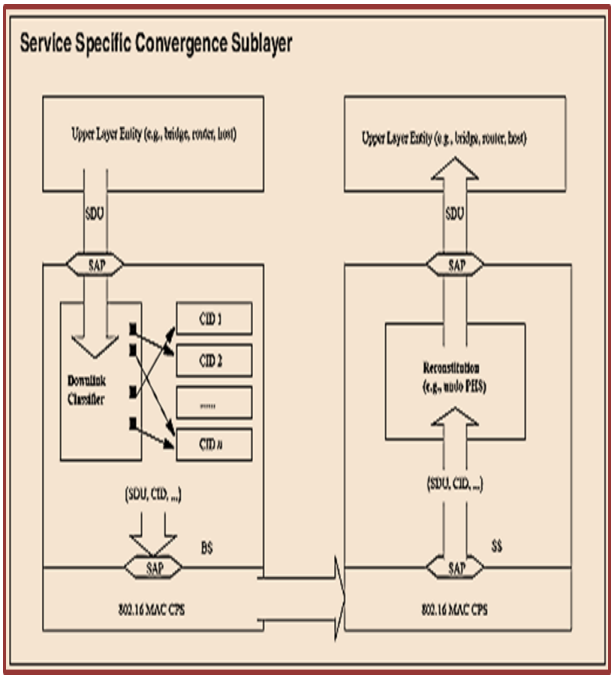

Fig 1: Service specific convergence sub layer

The Worldwide interoperability for microwave access forum was established in 2003 to promote the deployment of worldwide interoperability for microwave access as a broadband wireless access technology. It initiated several technical specifications and allowed the certification of worldwide interoperability for microwave access [22] [29] products. The WiMAX network architecture is shown in fig 3. The network specification involves interaction with other standard organization and includes internet engineering task Force, 3rd generation partnership project, 3rd generation partnership project 2, digital subscriber line forum, and open mobile alliance.

The aim of this paper is to give an overview of the technologies used in IEEE 802.16j mobile multi-hop relay networks. The rest of the paper is organized as follows. In section I, we briefly recapitulate the different technologies in IEEE 802.16j mobile multi-hop relay network. In section II we briefly discuss the different technologies used in the physical layer of IEEE 802.16j mobile multi-hop relay networks and present a study of the advantages of the different physical layer technologies. This is followed in section III by a brief discussion about the different technologies used in the medium access control-security layer of the IEEE 802.16j mobile multi-hop relay networks and their relevancy. Conclusions are drawn in Section IV. Fig 1 shows the service specific convergence sub layer.

2 Technologies used in Physical layer of IEEE 802.16j MMR

2.1 SOFDMA

The scalable orthogonal frequency division multiple access is introduced to keep optimal subcarrier spacing and the FFT size should scale with the bandwidth. In Scalable orthogonal frequency division multiple access [16] [13], Subcarrier spacing is independent of bandwidth and the number of subcarriers scales with bandwidth. The smallest unit of bandwidth allocation[1], based on the concept of sub channels, is fixed and independent of bandwidth and other modes of operation and the number of sub channels scales with bandwidth and the capacity of each individual sub channel remains constant. It supports features such as AMC, H-ARQ, MIMO in DL and UL [20] and a variety of subcarrier allocation and diversity schemes.

2.2 Mobile WiMAX channel encoding process

Mobile WiMAX channel encoding process mechanism can be viewed as a process in which bits

to be sent are scrambled, FEC encoded, interleaved and modulated. Then it is finally multiplexed by an Orthogonal Frequency Division Multiple Access system. The scrambler [12] [14] [10] [9] [6] [3] is also known as randomized distributes the bits to be sent in the frequency domain, this reduces power peaks and thereby reducing the interference between adjacent subcarriers. It is carried out on the serialized bit stream of each transmission block. In the FEC encoded redundant information is added to the transmitted data, this allows error detection and correction by the receiver device. FEC encoded [1] are obtained through the application of Reed-Solomon, Convolutional Code [21], Convolutional Turbo Codes, or Low-Density Parity Check Codes, here Convolutional Code's implementation is mandatory for device interoperability, but the deployment of the other codes is optional as shown in fig 1. Then the Orthogonal Frequency Division Multiple Access system starts where, the standards use many Quadrature Amplitude Modulation constellations. The combination of Modulation constellations and FEC encoding is called Adaptive Modulation and Code configuration and the modulation constellations defined in the IEEE 802.16j standard are BPSK, QPSK, 16-QAM, and 64-QAM. The WiMAX forum mandated that all devices must support QPSK and 16-QAM, but 64-QAM is optional.

2.3 Relay station grouping and Messages

Relay station grouping as shown in fig 2 occurs when the Relay station is located close to each other, this grouping is decided by the base station, and this grouping reduces interference between relay stations. The Relay station grouping acts like one Relay station. The Relay station [1] [3] [4] [5] operates ether its own or as a group or join a new group. The Relay station group as shown in fig 2 includes base station, Relay station and Relay station grouping [22]. If Relay station grouping doesn't include base station then one of the relay station acts as a base station. The RS_Config-RCM / REQ message [1] is used for Relay station configuration; this is used to remove a relay station from the group or permeable configuration. RS_Member_List_Update message is used to update the group members in the Relay station grouping. The MR_LOC-REQ / RSP message is used for location information of the relay station.

2.4 Ideal mode operation, Paging and Location management

The Idle mode operation in IEEE 802.16j mobile multi hop relay network reduces control signalling cost and mobile station energy consumption. In this idealistic mode the mobile station [1] [2] [3] periodically listens to the downlink broadcasting paging messages without registering to a specific base station. Generally there are two types of time intervals in idle mode operation mobile station Paging Unavailable Interval and mobile station Paging Listening Interval. Two signalling messages are used to synchronize the paging listening time, deregistration message and die/Reregister Command message.

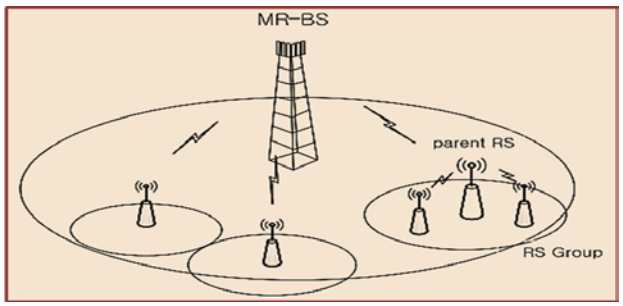

Fig 2: relay station grouping and messages

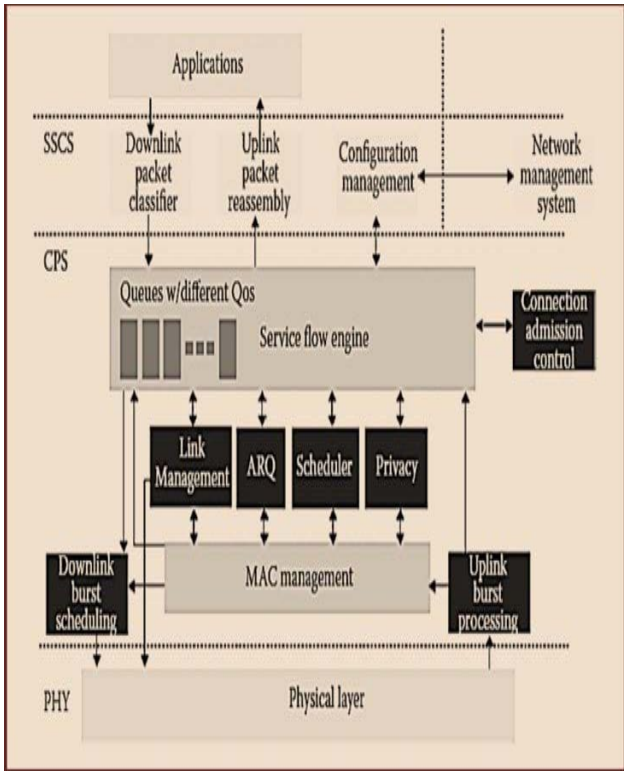

Fig 3: IEEE 802.16 Network Architecture

The Relay Station [1] will relay all deregistration messages and paging messages between the mobile station and base station. The Idle mode operation in IEEE 802.16j [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] mobile multi hop relay network consists of Mobile Station Paging Unavailable Interval and Mobile Station Paging Listening Interval, these two intervals is called paging cycle these two intervals appear alternately. The Mobile Station Paging Unavailable Interval is called paging offset as shown in fig 3. The mobile station switch down radio interface to save power in Mobile Station Paging Unavailable Interval and listens to the downlink broadcast of paging advertisement messages in Mobile Station Paging Listening Interval. The mobile station must leave idle mode and enter an active mode for normal operation when it wants to transmit data. The network re-entry process starts when the mobile station decides to terminate the idle mode, by first sending a Ranging Request [6] [7] [8] [9] [10] to base station and base station will reply Ranging Response to the mobile station. To start the normal active mode operation the Mobile station sends a location update message as shown in fig 4. The Signalling cost is a critical parameter in the wireless network paging design. The MS must notify the network about the Paging Area Notification change when the mobile station moves across the border between two different paging areas, and it updates the signalling cost of each Paging Area Notification.

Table 1: Physical Layer summary

Designation	Applicability	MAC	Duplexing
WirelessMAN-SC	10-66 GHZ Licensed	Basic,	TDD, FDD, HFDD
WirelessMAN-SC	2-11 GHZ Licensed	Basic, (ARQ), (STC), (AAS)	TDD, FDD
WirelessMAN-OFDM	2-11 GHZ Licensed	Basic, (ARQ), (STC), (AAS)	TDD, FDD
	2-11 GHZ Licensed exempt	Basic, (ARQ), (STC), (DFS), (MSH), (AAS)	TDD
WirelessMAN-OFDMA	2-11 GHZ Licensed	Basic, (ARQ), (STC), (AAS)	TDD, FDD
	2-11 GHZ Licensed exempt	Basic, (ARQ), (STC), (DFS), (MSH), (AAS)	TDD

Five physical interfaces are defined in the 802.16 standard as shown in table-1, (1) WirelessMAN-SC: using as a single carrier [1] in the 10–66 GHz band, (2) WirelessMAN-SCa: using as a single carrier in the 2–11 GHz band (3) WirelessMAN-OFDM: using OFDM transmission in the 2–11 GHz band, (4) WirelessMAN-OFDMA: using OFDM transmission and orthogonal frequency division multiple access in the 2–11 GHz band, (5) WirelessHUMAN : for unlicensed frequency

2.5 Uplink sub frame

There are two contention slots at the beginning of the uplink sub frame as shown in fig 4. The first contention slot is used by the IEEE 802.16 Mobile Stations [24] for initial ranging, the second contention slot is used by the IEEE 802.16 Mobile Stations to send bandwidth request PDUs to the Base Station. The remaining transmission slots are grouped by Mobile Stations. Each Mobile Stations have a specific slot allocated for uplink data transmission

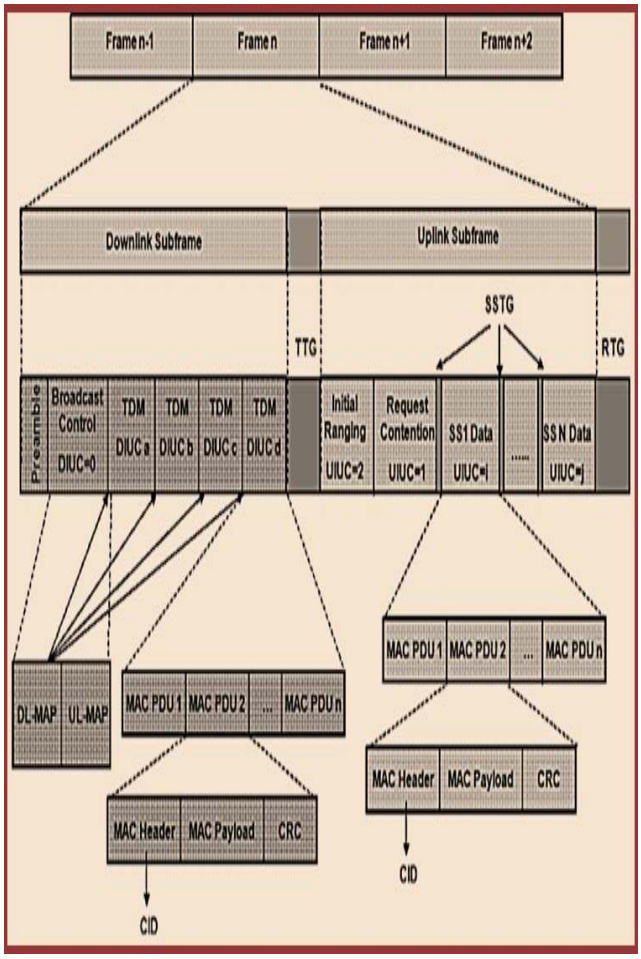

Fig 4: IEEE 802.16j Frame structure

2.6 Downlink sub frame

Each downlink sub frame [1] consists of (1) preamble: It is used for synchronization; it is the first OFDM as shown in fig 5 symbols of the frame. (2) Frame control head: It provides the frame configuration information such as MAP message length, coding scheme [20] [21] [22], and available sub channels. It also contains the down link frame prefix to specify the burst profiles and the length of burst profiles of one or several downlink [25] bursts immediately following the Frame control head. (3) Downlink map: It indicates the burst profile, location, and duration of zones within the Downlink frame. It is BPSK modulated and protected with rate 1/2 code by the mandatory coding scheme. (4) Uplink map: It provides the sub channel and slot allocation and other control information for the uplink sub frame. (5) The downlink channel descriptor is transmitted by the base station at periodic intervals to define the characteristics of a downlink frame as shown in fig 4. (6) The uplink channel descriptor is transmitted by the Base station at periodic intervals to define the characteristics of an uplink frame.

2.7 Protocols stack

The Service Specific Convergence Sublayer provides an interface between the 802.16 system and the upper layers of the protocol stack. It receives the higher layer MAC [26] [27] Service Data Units coming through the Service Specific Convergence Sublayer Service Access Point [28] and classifying them to the appropriate connection. Two main types of Service Specific Convergence Sublayer are defined, Packet Service Specific Convergence Sublayer and the Asynchronous Transfer Mode Service Specific Convergence Sublayer [1] . Asynchronous Transfer Mode Service Specific Convergence Sublayer is used to support cell-based protocols and Packet Service Specific Convergence Sublayer is used to support packet-based protocols. The Medium Access Control Common Part Sublayer receives classified packets arriving from the Service Specific Convergence Sublayer and is responsible for addressing, construction and transmission of the MAC PDUs, scheduling, bandwidth allocation, request mechanisms, contention resolution etc.

2.8 Classifier

For each packet a set of packet matching criteria is applied and this is called as IEEE 802.16 classifier. This IEEE 802.16 classifier [1] [20] [20] [26] consists of some protocol-specific fields, a classifier priority and a reference to a particular CID. A specific action such as the packet can be discarded, sent on a default connection, or a new connection can be established if no IEEE 802.16 classifier is found. Downlink classifiers [1] [31]are applied by the worldwide interoperability for Microwave access Base Station and uplink classifiers are applied by the worldwide interoperability for Microwave access mobile Station.

2.9 Frequency reuse pattern

The frequency reuse pattern is calculated by the expression:

Frequency reuse pattern = N_C x N_S x N_F.

Where
N_C = number of cells in the network cluster
(Determine inter-cellular frequency reuse).
Ns= represents the number of sectors in a cell
N_F demonstrates intracellular frequency reuse.

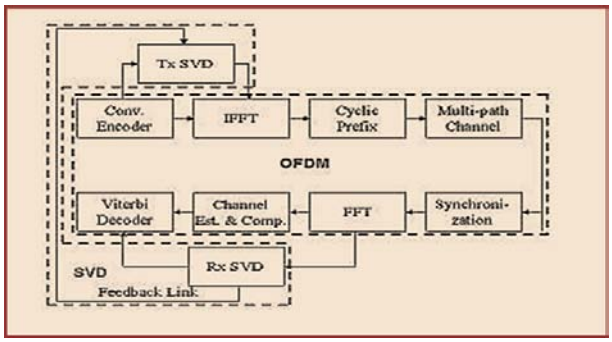

Fig 5. OFDM block diagram

2.10 New standards

Worldwide interoperability for microwave access provides a cost-effective and efficient platform for network operators. It is suitable for a variety of deployment scenarios, ranging from simple fixed and mobile Internet access. The new standard IEEE 802.16-2009 persistent air interface resource assignments for VoIP operation and MIB for mobile systems. Currently two new standards are under development, IEEE 802.16h [1] [22] standard includes specifications for operation in license exempt frequencies and the IEEE 802.16m standard specify a new enhanced air interface for IEEE 802.16 systems which will be compliant with the International Mobile Telecommunications Advanced system requirements.

3 Technologies used in a Security sub - layer of IEEE 802.16j MMR

3.1 Privacy Key Management protocol

The Privacy Key Management protocol [13] [14] [35] [36] is responsible for Security of connections in IEEE 802.16j MMR. This protocol periodical authorization the mobile stations and distribution of key material to them. It supports encryption and authentication algorithms to the exchanged MAC Protocol Data Units. This Privacy Key Management protocol uses X.509 certificates [1] and symmetric cryptography to secure key exchange between the mobile stations and Base Stations. The mobile stations send an authorization Request Message to the attached Base station, requesting an Authorization Key[37]. This message contains the mobile station certificate and cryptographic procedure supported by the mobile stations. The mobile stations are authorized based on the verification of its certificate. In IEEE 802.16 encryption can be done by means of the Data Encryption Standard using Cipher Block Chaining mode with 56 bits. An encryption algorithm is used for encipher the MAC protocol data units.

3.2 IEEE 802.16j MMR physical layer security

The IEEE 802.16j MMR physical layer is affected by two basic types of attacks, jamming and packet scrambling. In jamming is relatively straightforward and is the result of interference. Packet scrambling occurs when control packets in the respective downlink and uplink sub frames are sniffed then scrambled and returned to the network. This attack is much harder to mount than the other. WIMAX OFDM, OFDMA [20] [1] [2] [3] and SOFDMA [1]. IEEE 802.16j MMR systems support Orthogonal Frequency Division Multiplex as shown in fig 5, Orthogonal Frequency Division Multiple Access and Scalable Orthogonal Frequency Division Multiple Access as shown in fig 6. Orthogonal Frequency Division Multiplex is a multi carrier modulation scheme, but Orthogonal Frequency Division Multiple Access and Scalable Orthogonal Frequency Division Multiple Access are a multiple access scheme as shown in fig 6.

For improved multi-path performance in non-line of sight environments, mobile IEEE 802.16j MMR Air Interface adopts Orthogonal Frequency D ivision Multiple Access. To support scalable channe l bandwidths Scalable Orthogonal Frequency Divisi on Multiple Access [38]is introduced in the IEEE 80 2.16e Amendment in 1.25 to 20 MHz. .

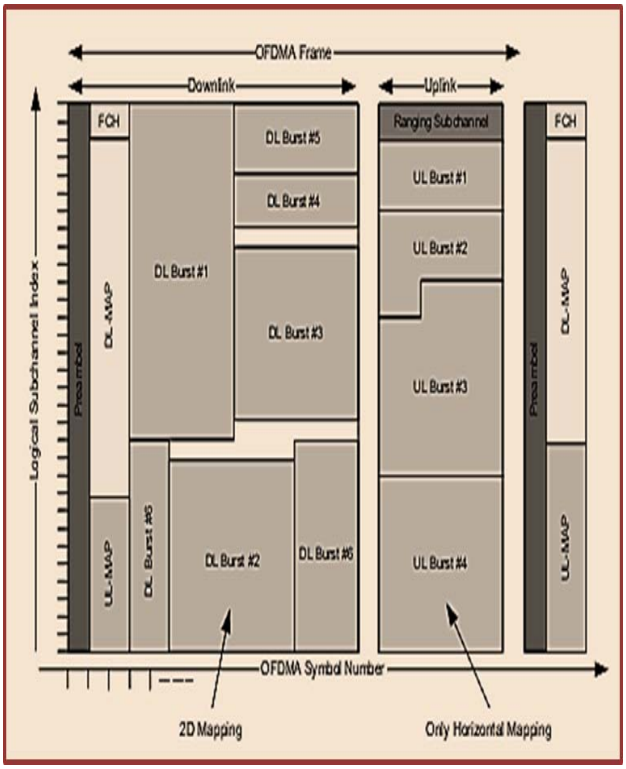

Fig. 6. Orthogonal Frequency Division Multiple Access frame Structure.

The difference between Orthogonal Frequency Division Multiplex and Orthogonal Frequency Division Multiple Access is that Orthogonal Frequency Division Multiple Access has the ability to dynamically assign a subset of those subcarriers to individual users, making this the multi-user version of Orthogonal Frequency Division Multiplex, using either Time Division Multiple Access or Frequency Division Multiple Access for multiple users [1]. Orthogonal Frequency Division Multiplex technologies typically occupy nomadic, fixed and one-way transmission standards, ranging from TV transmission to WI-Fi [19] [28] [17] as well as fixed IEEE 802.16j MMR and newer multicast wireless systems [20] like Qualcomm's Forward Link Only. Orthogonal Frequency Division Multiple Access as shown in fig 6 however adds true mobility to the mix forming the backbone of many of the emerging technologies including LTE and mobile WiMAX. Orthogonal Frequency Division Multiplex is a broadband multicarrier modulation method. Compared to single-carrier modulation methods Orthogonal Frequency Division Multiplex offers superior performance and benefits. Orthogonal Frequency Division Multiplex is the most spectrally efficient methods, and it mitigates the severe problem of multipath propagation that causes massive data errors and loss of signal in the microwave and UHF spectrum.

The IEEE 802.11a/g/n standards, 4G cellular technology standard Long-Term Evolution uses Orthogonal Frequency Division Multiplex. It is used in TV broadcasting in Europe. The high-speed short-range technology known as Ultra-Wideband uses an Orthogonal Frequency Division Multiplex standard set by the WiMedia Alliance. Orthogonal Frequency Division Multiplex is also used in wired communications like power-line networking technology. One of the first successful and most widespread uses of Orthogonal Frequency Division Multiplex was in data modems connected to telephone lines. ADSL and VDSL used for Internet access use a form of Orthogonal Frequency Division Multiplex known as discrete Multitone.

In Orthogonal Frequency Division Multiplex, serial digital data stream to be transmitted is split into multiple slower data streams, and each is modulated onto a separate carrier called subcarriers or tones in the allotted spectrum [9] [10] [4]. In Orthogonal Frequency Division Multiplex the outputs of all the modulators are linearly summed, and the result is the signal to be transmitted. The modulated signal could be unconverted and amplified [29]if needed. To implement Orthogonal Frequency Division Multiplex with hardware is a challenge even with modern semiconductor technology. The whole process can be accomplished in computer hardware by using the fast Fourier transform or inverse fast Fourier transforms. Orthogonal Frequency Division Multiplex is highly resistant [39]to the multipath problem in high-frequency wireless, very short-wavelength signals normally travel in a straight line -line of sight from the transmit antenna to the receive antenna. Orthogonal Frequency Division Multiplex is Sensitive to frequency offset and phase noise. The Peak-to-average problem in Orthogonal Frequency Division Multiplex reduces the power efficiency of RF amplifier at the transmitter. Orthogonal Frequency Division Multiplex is very easy and efficient in dealing with multi-path, and it is Robust again narrow-band interference.

In Orthogonal Frequency Division Multiplex the date stream is divided into multiple parallel low rate data streams. Each low rate data stream is mapped to an individual data subcarrier and modulated. The modulation may be Phase Shift Keying or Quadrature Amplitude Modulation such as Binary Phase Shift Keying, Quadrature Phase Shift Keying, 16 Quadrature Amplitude Modulation, and 64 Quadrature Amplitude Modulation. The Orthogonal Frequency Division Multiplex signal used in LTE comprises a maximum of 2048 [27] different sub-carriers having a spacing of 15 kHz. In Wireless

Metropolitan area network- Orthogonal Frequency Division Multiplex physical layer, the number of subcarriers is 256 [24][25][26] where three types of subcarriers can be categorized: 192 data subcarriers carrying payload, 8 pilot subcarriers mainly for channel estimation, and 56 null subcarriers for guarding purposes. The pilot subcarriers distribute evenly among the data subcarriers. Orthogonal Frequency Division Multiple Access allows many users to receive data simultaneously on different subcarriers. They receive data [22] simultaneously during the same symbol period by dividing channels into sub-channels and uniformly allocating subcarriers to them. Orthogonal Frequency Division Multiple Access is adopted in IEEE 802.16-2004 [1][2][3] [4] [5] [6] [7] WiMAX networks for non-line-of-sight (NLOS), in frequency bands below 11 GHz. In Orthogonal Frequency Division Multiple Access the basic unit of resource for allocation is a slot. It is comprised of a number of Orthogonal Frequency Division Multiple Access symbols in time domain, and one sub channel in the frequency domain. The actual data bits do not map exactly to the assigned Orthogonal Frequency Division Multiple Access symbols and sub channels so it leads to resource waste due to this mapping inefficiency.

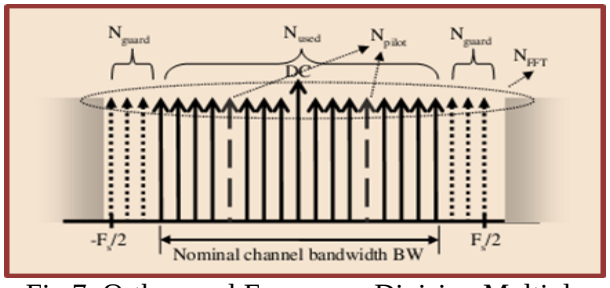

Fig 7: Orthogonal Frequency Division Multiple Access symbol in the frequency domain

The data transmission in IEEE 802.16 networks is divided into frames in the time domain where each frame consists of downlink and uplink sub frames. Theses frames are duplexed using either Frequency Division Duplexing or Time Division Duplexing. There is a time gap between Downlink and Uplink sub frames for transmitter and reception of each frame called TX/Rx Transmission Gap and Rx/TX Transmission Gap. These sub frames are divided into several slots for actual data transmission. Each of the frames begins with DL-Map as shown in fig 7 and the UL-Map into the DL sub-frame. The DL-Map [1] [2] [3] [4] and the UL-Map into the DL sub-frame provides resource allocation and other control information for DL and UL sub-frames. The first symbol in the DL sub - frame is occupied by a preamble. Then it is followed by Frame Control Header and it describes the sub-channels and the length of the DL-MAP.

To over-come the indoor coverage problem and also growth of traffic within macrocells Orthogonal Frequency Division Multiple Access femtocells have been pointed out by the industry as a good solution. However, the deployment of a new femtocell layer may have an undesired impact on the performance of the macrocell layer. There are guidelines provided on how the spectrum allocation and interference mitigation problems can be approached in these Orthogonal Frequency Division Multiple Access macro/ femtocells networks. Orthogonal Frequency Division Multiple Access femtocells can exploit channel variations in both frequency and time domains for the avoidance of interference.

Orthogonal Frequency Division Multiple Access Femtocells can be configured in three ways to allow or restrict their usage by certain users, they are (1) Open access: Open access [28] all the users are allowed to connect. The open access improves the overall capacity of the network; open access will increase the number of handoffs and signalling. Open access is commercially challenging for operators were not keen to accept nonsubscribers as users of their own femtocells (2) Closed access: Closed access the femtocell allows only subscribed users to establish connections. (3) Hybrid access: In Hybrid access nonsubscribers use only a limited amount of the femtocell resources.

The LTE uplink [1] uses a different concept of the access technique. It is using a form of Orthogonal Frequency Division Multiple Access technology; the implementation is called Single Carrier Frequency Division Multiple Access

3.3 Mobility Task groups

WiMAX members have promoted two mobility task groups: the Evolutionary Task Group [1] and the Mobility Task Group in order to accelerate time to market and optimize performance vs. Applications. The Mobility Task Group focuses on Scalable Orthogonal Frequency Division Multiple Access strengths and is aimed at top mobility performances. The Evolutionary Task Group builds on Orthogonal Frequency Division Multiplex 802.16-2004 evolution to optimize throughput and availability for fixed to basic mobility applications. The Evolutionary Task Group addresses a wide range of business models going from backhaul to DSL extension to wireless laptop connectivity.

3.4 Attacks

The commonly Message replay attack is one of the attacks on authentication and authenticated key establishment protocols and another commonly attack is Man-in-the-middle attack. The Other attacks are parallel session attackers, reflection attack, interleaving attack [1] attack due to type flaw, attack due to name omission etc. Interleaving Attack: Interleaving Attack uses the messages from previous protocol sessions being run concurrently to the main protocol session, in order to provide the messages in the main protocol session. The request message is easy to be modified or impersonated without a mobile station signature. The attack still exists even with the signature from the mobile station. Multiplicity Attack: A new attack called Multiplicity Attack is on the original X.509 3- way authentication protocol

3.5 Privacy and Key Management Protocol and authorization

The 802.16 standard specifies a security as a separate layer called MAC security sub layer. Two protocols are used in this MAC security sub layer an encapsulation protocol for encrypting packet data, and Privacy and Key Management Protocol as shown in fig 8 distribute the key and provide secure communication between base station and a mobile station. The Privacy and Key Management Protocol uses X.509 digital certificates, RSA public-key algorithm, and strong encryption algorithm to perform key. A two-tier key system is used in IEEE 802.16 system Authentication Key and Encryption Keys. The Authentication Key is used for authenticating mobile station to base station and the Authentication Key is used to secure the exchange of Transport Encryption Keys as shown in fig 8 and also mobile station also needs to authenticate a base station to keep away from malicious ones. The Privacy and Key Management authorization consists of a three-message exchange between a mobile station and a base station. The mobile station initiates the protocol by sending first the two messages and the base station responds to the third message. The mobile station uses Message 1 to push its Manufacturer X.509 certificate [23] to the base station so that the base station decide the mobile station as a trusted node, sometimes the security policy of the base station ignore this message as it is not a trusted node.

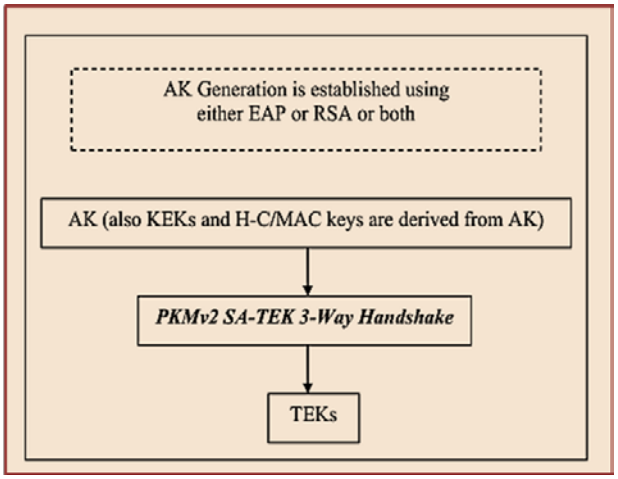

Fig 8: Privacy and Key Management version 2 Protocol

Then the mobile station immediately sends Message 2 to the base station consists of its X.509 certificate and its identity SAID. Then the base station verifies the mobile station X.509 certificate [1] and authorizes the mobile station by sending Message 2 consists of authorization Security association between the two stations which is an authorization to access the WMAN channel. The Privacy and Key Management Protocol [25] consists of a two/three message exchange between the mobile station and a base station. The base station sends the first message which is an optional one unless it wants to rekey a data Security association or create a new Security association. The mobile station initiates the protocol by sending the second message by request Security association parameters and the base station responds with the third message as shown in fig 8. The mobile station must take Security association identifier from the authorization protocol Security association identifier [21] List or from a Message 1 as shown in fig 10 with valid Hash function-based message authentication code. If Hash function-based message authentication code is valid and Security association identifier identifies one of mobile station Security association, base station configures the Security association using Message 3.

4 Conclusions and Future Perspective

The first IEEE 802.16 standard was approved in 2001 and published in 2002 includes air interface standard for wireless broadband. The IEEE 802.16j standard approved in 2009 provides multi-hop relay operation. The relay architecture in IEEE 802.16j standard provides coverage extension and capacity increase with reduced cost. The IEEE 802.16j standard defines two layers physical and MAC

layers. The current technologies of physical and MAC layers are SOFDMA, Mobile WiMAX channel encoding process, Relay station grouping and Messages, Ideal mode operation, Paging and Location management, Privacy Key Management protocol, WiMAX physical layer security [1] , comparison of WIMAX OFDM , OFDMA and SOFDMA, Uplink Sub Frame: down link Sub Frame, IEEE 802.16 Protocol Stack, Privacy and Key Management Protocol and authorization.

5 Acknowledgments

This work was supported by Department of Computer Science and Engineering, Coimbatore Institute of Engineering and Technology, Coimbatore, INDIA. We thank the management for providing facility to do research in networks laboratory.

References:

[1] "IEEE Standard for Local and Metropolitan Area Networks: Part 16: Air Interface for Broadband Wireless Access Systems, IEEE Std 802.16-2009", May 2009, 2094 pp.

[2] C. So-In, R. Jain, and A. Al-Tamimi, "Scheduling in IEEE 802.16e WiMAX Networks: Key issues and a survey," *IEEE J. Select. Areas Commun.*, Vol. 27, no. 2, pp. 156–171, Feb. 2009.

[3] D. Satishkumar, N. Nagarajan, "A Survey on Technical Issues in IEEE 802.16j Mobile Multi-hop Relay Networks," *The Smart computing Review*, vol. 1 No 1, pp. 12–33, Oct. 2011.

[4] D. Satishkumar, N. Nagarajan, "Technical Issues in IEEE 802.16j Mobile Multi-hop Relay Networks," *European Journal of Scientific research*, Vol.65 No.4 (2011), pp. 507-53

[5] D. Satishkumar, N. Nagarajan, "A new Adaptive Model for Throughput Enhancement and Optimal Relay selection in IEEE 802.16j Networks" *Wseas Transactions on Communication*, Issue 2, Volume 11, February 2012

[6] D. Satishkumar, N. Nagarajan, "Relay technologies and technical issues in IEEE 802.16j Mobile Multi-hop Relay (MMR) networks". J. Network and Computer Applications 36 (1): 91-102 (2013).

[7] D. Satishkumar, N. Nagarajan, "Simulation of Hard Hand over (HHO) Mechanism in IEEE 802.16 j Transparent Mode networks" International Journal of Computer Applications 14 (2), 35-39,2010.

[8] D. Satishkumar, N. Nagarajan, "An Improved Network Topology Acquisition process in IEEE 802. 16 j non-transparent mode relay networks" Journal of Discrete Mathematical Sciences & Cryptography 15 (1), 57-71, 2012.

[9] D. Satishkumar, N. Nagarajan "Analysis of Transparent and non-Transparent relay modes in IEEE 802. 16 j Mobile Multi-Hop relay networks" Journal of Discrete Mathematical Sciences & Cryptography 15 (1), 73-87, 2012.

[10] D. Satishkumar, N. Nagarajan "Problems faced in Communicate set up of Coordinator with GUI and Dispatcher in NCTUns network simulator", Computer Engineering and Intelligent Systems 2 (6), 61-71,2011.

[11] D. Satishkumar, N. Nagarajan "NCTUns Simulation model for IEEE 802.16 j Mobile multi hop Relay (MMR) WIMAX networks", Innovative Systems Design and Engineering 2 (5), 74-81,2011.

[12] D. Satishkumar, N. Nagarajan "Relay Technologies in IEEE 802.16 j Mobile Multi-hop Relay (MMR) Networks" Computer Engineering and Intelligent Systems 2 (3), 105-113, 2011.

[13] D. Satishkumar, N. Nagarajan "Simulation of Relay modes in IEEE 802.16 j Mobile Multi-hop Relay (MMR) WIMAX Networks", Innovative Systems Design and Engineering 2 (4), 75-84, 2011.

[14] D. Satishkumar, N. Nagarajan "A Survey of IEEE 802.16j Multi Hop Relay Based Wimax Networks, Journal of High Performance", Communication Systems and Networking: An International Journal, Volume .3 No.1, 2011, 9-14

[15] C. So-In, R. Jain, and A. Al-Tamimi, "Capacity evaluation for IEEE 802.16e MobileWiMAX," *J. Comput. Syst., Networks, and Commun.*,Vol. 2010, Apr. 2010.

[16] K. Wongthavarawat and A. Gains, "IEEE 802.16 based last mile broadband wireless military networks with quality of service support," in *Proc. Military Communications Conf.*, 2003, vol. 2, pp. 779–784.

[17] A. Sayenko, O. Alanen, and T. Hamalainen, "Scheduling solution for the IEEE 802.16 base station," *Int. J. Comp. and Telecommun. Netw.*,vol. 52, pp. 96–115, Jan. 2008.

[18] R. Jain, C. So-In, and A. Al-Tamimi, "System level modeling of IEEE 802.16e Mobile WiMAX networks: Key issues," *IEEE Wireless Comm.Mag.*, vol. 15, no. 5, pp. 73–79, Oct. 2008.

[19] A. Ghosh *et al.*, "Broadband Wireless Access with WiMAX /802.16: Current Performance Benchmarks and Future Potential," *IEEE Commun. Mag.*, vol. 43, Feb. 2005, pp. 129–36.

[20] IEEE 802.16-2004, "Local and Metropolitan Networks — Part 16: Air Interface for Fixed Broadband Wireless Access Systems," 2004.

[21] IEEE 802.16e-2005, "Local and Metropolitan Networks — Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum1," 2006.

[22] Q. Liu, X. Wang and G. B. Giannakis, "A Cross-Layer Scheduling Algorithm with QoS Support in Wireless Networks," *IEEE Trans. Vehic. Tech.*, vol. 55, no. 3, May2006, pp. 839–46.

[23] J. He, K. Guild, K. Yang, and H. Chen, "Modeling contention based bandwidth request scheme for IEEE 802.16 networks," *IEEE Commun. Lett.*, vol. 11, no. 8, pp. 698–700, Aug. 2007.

[24] H. L. Vu, S. Chan, and L. L. H. Andrew, "Performance analysis of best-effort service in saturated IEEE 802.16 networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 1, pp. 460–472, Jan. 2010.

[25] Y. P. Fallah, F. Agharebparast, M. R. Minhas, H. M. Alnuweiri, and C. M. Leung, "Analytical modeling of contention-based bandwidth request mechanism in IEEE 802.16 wireless networks," *IEEE Trans. Veh.Technol.*, vol. 57, no. 5, pp. 3094–3107, Sep. 2008.

[26] C. Cicconetti, A. Erta, L. Lenzini, and E. Mingozzi, "Performance evaluation of the IEEE 802.16MAC for QoS support," *IEEE Trans. Mobile Comput.*, vol. 6, no. 1, pp. 26–38, Jan. 2007.

[27] Q. Ni *et al.*, "Investigation of bandwidth request mechanisms under point-to-multipoint mode of WiMAX networks," *IEEE Commun.Mag.*, vol. 45, no. 5, pp. 132–138, May 2007.

[28] C. Mohanram, S. Bhashyam, "Joint subcarrier and power allocation in channel-aware queue-aware scheduling for multiuser ofdm", IEEE Transactions on Wireless Communications 6 (9) (2007) 3208– 3213.

[29] G. Kulkarni, S. Adlakha, M. Srivastava, "Subcarrier allocation and bit loading algorithms for OFDMA based wireless networks", IEEE Transactions on Mobile Computing 4 (6) (2005) 652–662.