

EE228a - Lecture 6 - Spring 2006

IEEE 802.16 / WiMAX

Lectured by Shyam Parekh,
Scribed by Jiwoong Lee (porce@eecs)

Abstract

IEEE 802.16 is an emerging wireless MAN technology. Although it was originally designed to provide wireless last mile/first mile (rhetoric expressions for access networks) deployment in a MAN, it can also be used for end-user access as an alternative to the IEEE 802.11 family. Mobility support at vehicular speeds is provided by the most recent standard. In this lecture, we review the history of IEEE 802.16 standardization, physical layer fundamentals and media access control operations.

I. REFERENCES

This lecture is based on following standards and technical references. The first two documents are IEEE standards. Among them, the first one is for fixed wireless communications and the second one is an amendment for mobile communications. Intel's White papers are good tutorials. The author of the final reference was involved in the standardization process of IEEE 802.16.

- IEEE 802.16-2004 (802.16REVd)
- IEEE 802.16-2005 (802.16e)
- Intel's White papers, 2004 (<http://www.intel.com/technology/itj/2004/volume08issue03/>)
- IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access, June 2002
- Broadband Wireless Access with 802.16/WiMAX: Current Performance Benchmarks and Future Potential, A. Ghosh et al., IEEE Communication Magazine, Feb 2005
- Wireless Communication Standards: A Study of IEEE 802.11, 802.15, and 802.16, T. Cooklev, 2004

II. INTRODUCTION

Similarly to Wi-Fi, WiMAX is an industrial consortium to promote the use of IEEE 802.16 technology. The activities of WiMAX is still going on. Interoperability, features and applications are the main concerns of that consortium.

Many companies in industry are interested in WiMAX technology and its products. In comparison to IEEE 802.11 LAN family technologies, WiMAX is a Metropolitan Area Network (MAN) standard and plays a bigger role in large scale operator networks. In the sense of geographical coverage and overall throughput, IEEE 802.16 has good potential for operation. As one example, Lucent is building a base station (BS) and integrating overall networks including backhaul connections and management plane.

In this discussion, we are interested in GHz range spectrum. Side: Another interesting spectrum ranges from 10^{14} to 10^{15} Hz - free optic spectrum.

A. History of 802.16 standards

- In 1998, The National Institute of Standards and Technology (NIST) started looking for a different wireless application and held the first initiative meeting. By the time of the first standardization of 802.16 (in Dec 2001), systems were already available. In fact, many basic ideas of 802.16 were borrowed from DOCSIS/HFC (a cable modem technology) and applied to the wireless setting, although the physical layer specification is different. There is a good analogy to note: Wi-Fi : Ethernet = WiMAX : DOCSIS/HFC.
- 802.16 is for Line-of-Sight (LOS) applications utilizing 10-66GHz spectrum. Although this spectral range has a severe atmospheric attenuation, it is suitable for connections in the operator network between two nodes with high amounts of bandwidth because many base stations are deployed at elevated positions from the ground. This is not suitable for residential settings because of the Non-Line-of-Sight (NLOS) characteristics caused by rooftops or trees.
- 802.16a is an amendment for NLOS utilizing 2-11GHz. Good for Point-to-Multipoint (PMP) and home application. Orthogonal Frequency Division Multiplexing (OFDM) is newly adopted.
- 802.16-2004 revises and replaces 802.16, 802.16a, and 802.16REVd. This is the completion of the essential fixed wireless standard. Some operators are already interested in integrating this with the Cellular backhaul. After some political debates, it was decided to support not mobile but fixed wireless and nomadic communications. Nomadicity is this: Users are attached to the network. After a session completes, they can move to a different network. But the session should be re-established (possibly including the authentication) from scratch; it does not have a hand-off mechanism.
- 802.16e is a MAC/PHY enhancement for supporting truly mobile communications at vehicular speeds. This supports a full hand-off. A user's session is maintained when he moves around.

B. Network Architecture

Backplane is implemented as either a bridge, a router or a host. When the Service Data Unit(SDU) comes into the Convergence sublayer, the Classifier in Convergence sublayer can classify the type of the traffic (eg. voice, web surfing, ATM CBR ...) and map it into a particular Connection ID(CID). In turn each CID is referred to a certain specific profile. Each profile describes modulation scheme, Forward Error Correction(FEC) scheme, etc.. Once the CID is well defined between both communication parties (such as a Base station(BS) and a Subscriber Station(SS)), the non-changing payload header information(such as ATM cell header or IP header) can be suppressed by Payload Header Suppression(PHS).

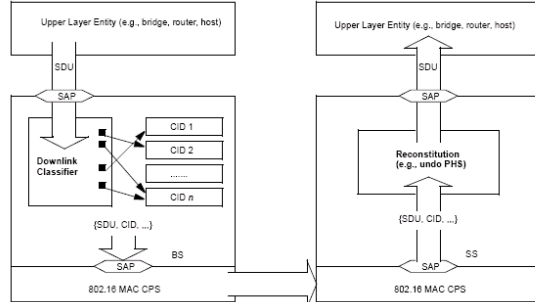


Fig. 1. Architecture

C. Scope of the Standard

The scope of 802.16 standard covers PHY, Service Access Point(SAP), Security sublayer, MAC Common Part Sublayer(CPS), and Service-specific Convergence Sublayer(CS).

D. Hand-off mechanism

The hand-off procedure of 802.16 is not radically different from that of other well-known wireless technologies. Based on Signal-to-Noise ratio, the SS sends a hand-off request to the serving BS. The serving BS negotiates the bandwidth and QoS with possible target BSs on behalf of the SS. After receiving the confirmation from one of them, the serving BS notifies the SS of hand-off response. The SS starts to use the target BS.

III. PHYSICAL LAYER

If 2-11Ghz is of interest, utilizing OFDM gives several benefits. In recent standards there are optional beneficial features. For example, Adaptive Antenna System(AAS) is a directional signal processing technique which is able to highlight the signal from a certain direction when the system is sectorized. MSH stands for Mesh Network. DFS stands for Dynamic Frequency Selection.

TABLE I
PHYSICAL LAYER SUMMARY

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

A. Channel characteristics

A 10-66Ghz frequency wave is a very focused beam. Typically it reaches the order of a few miles. One interesting effort by a company is to establish a wireless communication link between ground and a flying airplane using this frequency range.

A 2-11Ghz frequency wave can be used for NLOS communication. Also this frequency undergoes multipath effects.

B. Performance

In theory, there is no limit in the number of users that are served by a BS. Maximum data rate per sector of the antenna of one BS is around 70Mbps. One good part of 802.16 technology is that it has a lot of flexibility in choosing carrier frequencies and bandwidth. Available channel bandwidths are 10, 20, 3.5, 7, 14, 3, 6 Mhz. Typical channel bandwidth is 10 or 20 Mhz. Usually backhaul application requires larger bandwidth. Also we can frequently see 802.16 products operating at 3.5 Ghz. Maximum bps/Hz is comparatively better than other technologies such as 802.11, EDGE or cdma2000.

TABLE II
PERFORMANCE COMPARISON OF TYPICAL WIRELESS TECHNOLOGY

	Channel Bandwidth	Maximum Data Rate	Maximum bps/Hz
802.11a	20Mhz	54Mbps	2.7
802.16a	10, 20, 3.5, 7, 14, 3, 6Mhz	70Mbps	5
EDGE	200Khz	384Kbps	1.9
CDMA2000	1.25Mhz	2Mbps	1.6

C. OFDM

Orthogonal Frequency Division Multiplexing(OFDM) is a multi-carrier transmission technique that has been recently recognized as an excellent method for high-speed bi-directional wireless data communications. Fundamentally, Frequency Division Multiplexing(FDM) uses multiples frequencies to simultaneously transmit multiple signals in parallel. While each sub-carrier is separated by a guard band to ensure that they do not overlap *in the ordinary FDM, the sub-carriers* in the OFDM are squeezed tightly together in order to reduce the required bandwidth. In fact the neighboring sub-channels are overlapped in OFDM. However, the sub-carriers are orthogonal to each other such that there is no inter-carrier interference (ICI).

In mobile communication environment with the moving vehicle, there is a Doppler shift effect which causes each sub-channel to be shifted and orthogonality to be broken. To prevent this phenomena, cyclic prefix to each symbol is added. The cyclic prefix is for implementing the FFT when one needs to use circular convolution to emulate linear convolution. Instead of just sending blank during guard time, repeating the end of the symbol provides "guard time" (instead of the "guard band") to make sure all the sub-carriers are orthogonal. If the end interferes with the next symbol, we can subtract it out because we already received the prefix, which is the same.

There is another benefit of OFDM. Since each subcarrier of OFDM uses a narrow bandwidth, in the time domain each symbol is transmitted during a relatively long symbol time. This guarantees all the significant multipaths arrive within a symbol time minimizing Inter-symbol Interference(ISI). This is good news. Because it removes the need for an equalizer at a transmitter and a receiver side, reducing complexity and the cost.

Also, 802.16 provides another flexibility; a subset of sub-carriers can be grouped together to form a sub-channel.

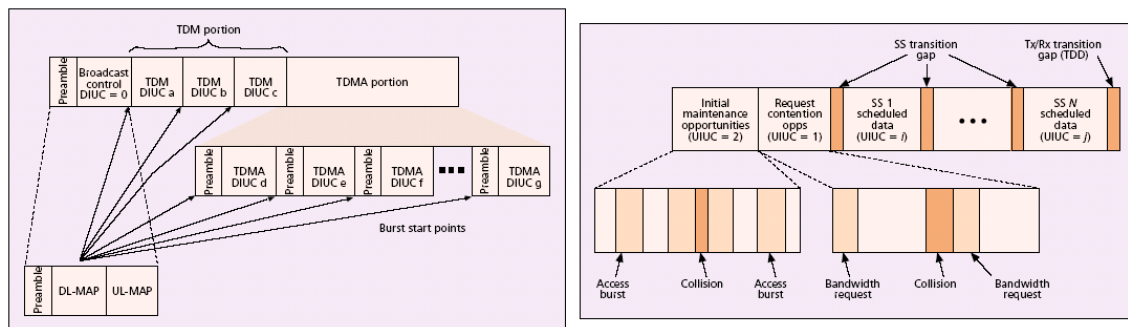


Fig. 2. Downlink / Uplink frame structures

IV. MEDIA ACCESS CONTROL LAYER

A. Frame structure and Access mechanism

Each frame has a fixed frame time in the order of a few milliseconds. A certain number of Physical Slots(PS) is given to each user. In Time Division Duplexing(TDD), the downlink frame comes first and the uplink comes next. Since the end of downlink/the start of uplink varies adaptively, this flexibility gives a good stream control in comparison to 802.11 protocols.

There are some basic notions. In the beginning of every frame, the Downlink-MAP(DL-MAP) tells how the rest of the frame will be used; DL-MAP describes which part of the frame shall be used for whom with a certain Downlink Interval Usage Code(DIUC). DIUC is a scalar number indicating which specific Burst Profile will be used for a certain portion of the frame. A Burst Profile that is determined by DIUC is a preconfigured group of information specifying the Forward Error Correction(FEC) type and modulation type. The mapping between a DIUC and a Burst Profile is done by the BS, and is periodically broadcast to network in the Downlink Channel Descriptor(DCD) message. The same story applies to uplink, Uplink-MAP(UL-MAP), Uplink Interval Usage Code(UIUC), and Uplink Channel Descriptor(UCD) message.

Within a Time Division Multiplexing(TDM) portion of a single frame, the modulation scheme gets fancier (equivalently less robust, equivalently again, more efficient) as TDM portions proceeds. By this clever strategy, the node who has better channel condition will successfully decode the received signal without losing synchronization while the nodes with worse channel condition do not care about the synchronization under the fancier modulation after it successfully decodes the signal addressed to itself.

In the Time Division Multiple Access(TDMA) portion, every subframe carries its own preamble because some half-duplex nodes might be not able to listen to TDMA portion from the beginning because of possible prior transmissions.

In uplink, two initial parts of the uplink frame are subframes for contention based access. The contention based portion of the frame is used for the initial ranging of the newly joining stations or the best effort traffics/bandwidth requests of already

associated stations. If a station wants to transmit only a single packet to the base station, it may well use this contention based portion of the frame instead of acquiring a dedicated bandwidth.

An elaborate power control scheme used in 802.16 is worthy of a few words. When a SS joins a network, it transmits its initial ranging request with the minimal transmission power. If the SS does not receive the ranging response from the BS, then it assumes the BS did not hear its request because the power was too weak. Then it repeats its ranging request with a slightly higher power. This process is repeated until the SS gets a proper response from the BS.

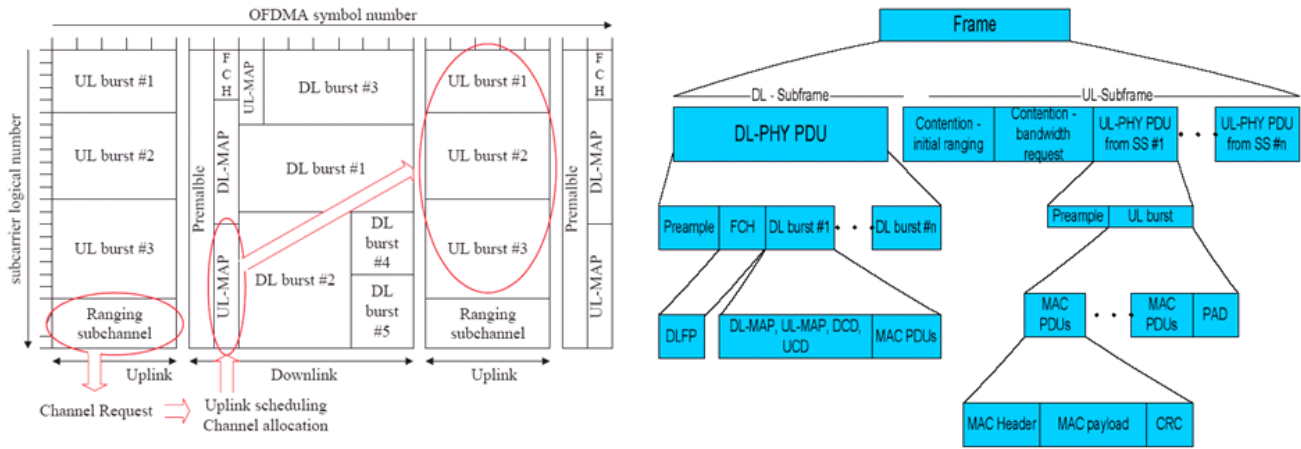


Fig. 3. Frame structure of 802.16. Y axis is for subchannel, X axis is for symbol time in the left figure

B. Network Entry Process

To be operated under the 802.16 network, a SS should ementer and register itself to the network. On initialization, a SS scans the possible channels of the downlink frequency band of operation until it finds a valid downlink signal. Once the PHY achieves, the SS searches DL-MAP and obtain downlink parameters. After this stage, the SS waits for UCD message to retrieve a transmission parameters and perform initial ranging. Ranging is the process of acquiring the correct timing offset and power adjustments. Ranging Request(RNG-REQ) is performed on contention based slots. Ranging Response(RNG-RSP) is sent to the SS to adjust power level, frequency offset and timing offset. Once successfully ranged, the SS joins normal data traffic in the uplink. The SS and the BS perform capability negotiation, authorization, key exchange, registration, IP version negotiation, DHCP address allocation, and operational parameter transfer. Finally they set up connections for preprovisioned service flows belonging to the SS. For clear understanding, the error handling procedure is omitted.

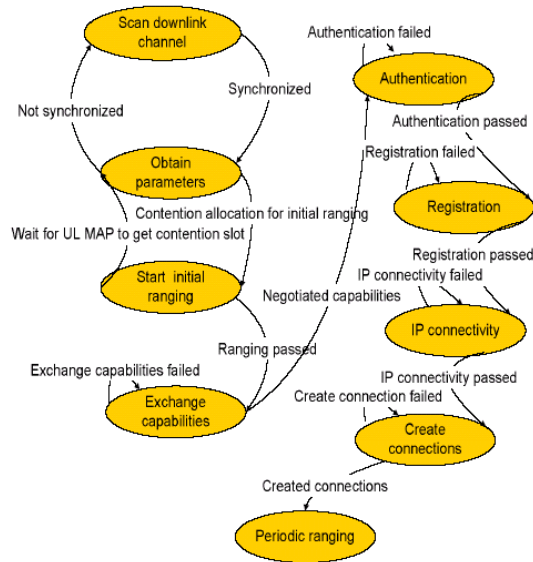


Fig. 4. Network entry process of a newly joining station

C. Connection and services

802.16 is a completely connection oriented protocol. Even the management message is based on the preset Connection ID(CID). Each CID is associated with a Service Flow ID(SFID) that determines QoS parameters that the network tries to guarantee. In

general we know there are many kinds of traffic - TDM voice, VoIP, HTTP, FTP, etc.. That traffic is mapped into each CID in one-to-one manner or many-to-one manner. Each CID is associated with a certain type of scheduling type and QoS parameters.

TABLE III
SCHEDULING TYPES AND QoS

Scheduling Type	QoS
Unsolicited Grant Service (UGS)	Max Sustained Traffic Rate, Maximum Latency, Tolerated Jitter
Real-Time Polling Service (rtPS)	Max Sustained Traffic Rate, Min Reserved Traffic Rate, Committed Burst Size, Maximum Latency, etc
Non-real-time Polling Service (nrtPS)	Committed Information Rate, Maximum Information Rate
Best Effort (BE)	Maximum Information Rate

In UGS, the SS does not have to request the bandwidth every time. This is the same concept with DOCSIS. The uplink time slot for the SS is preallocated. rtPS/nrtPS is Request - Polling - Grant service. In this service, the BS periodically polls the SS and the SS responds to the poll with the request of a certain amount of bandwidth(in terms of bytes). The SS does not use the contention based frame to request the bandwidth.

D. Message format

Understanding of Message format is rather straightforward. There are two types of header formats; a Generic header and a management header. Important header fields include Type, Length, CID. In a Bandwidth request message, BR(Bandwidth Request) field is also important. Currently 38 kinds of management messages are defined. They include UCD, DCD, DL-MAP, UL-MAP, Ranging, Registration, Primary Key Management, Dynamic Service Addition/Change/Deletion, TFT file exchange, ARQ, Reports of channel status, and Power Control.

V. ADVANCED FEATURES AND RELATED ACTIVITIES

A. Advanced 802.16 features

Some advanced features are noteworthy. The first one is MIMO channel capacity, which improves range and capacity. The second one is Hybrid-ARQ. We remember Forward Error Correction(FEC) has two major roles: Error detection and Error Correction. Imaging the receiver station detects an error but is not able to correct it. In Hybrid-ARQ mode, instead of discarding the error packet the receiver sends a particular ARQ message to the transmitter and the transmitter sends back a stronger FEC information. The receiver exploits both messages - the error packet and the stronger FEC information to recover the original packet. Dynamic Frequency Selection(DFS) helps in minimizing interference, and Space-Time Coding(STC) enhances performance in fading environments through spatial diversity.

B. Implementation, deployment and other research activities

Wibro is a serious large-scale deployment effort of 802.16 in South Korea.

Currently in WiMAX forum, there is an ongoing research activity in building the model of 802.16 and simulating it. Since this area is new, there are good opportunities to be deeply involved in. Especially, the resource management, traffic shaping, or access control in the BS is out of the scope of the standard and completely depends on the implementation and operation. Many vendors and operators are highly interested in those areas but do not know the answer yet.

VI. ANNOUNCEMENT

- There is an interesting project dubbed as GENI (Global Environment for Network Investigation). This is a 300 million dollar testbed for trying a new idea and creating a new network architecture. While the Internet2 project maintains the conventional core protocols, GENI's focus is to think over the design seriously. GENI's website is <http://www.geni.org>
- Any meticulous comments on contents, typos, or grammatical inappropriateness will be welcome.