Broadband Wireless Access (BWA) Networks: A Tutorial

Kuowei Hwang and V Rao Vemuri
University of California, Davis
{kuowei, rvemuri}@ucdavis.edu

Abstract

Explosive innovations are sweeping the telecommunications industry worldwide as appetite for bandwidth keeps growing unabated. Several reasons are contributing to this trend: (a) growth of the Internet and Internet-based applications, (b) increased dependence of digital transmission even for analog applications, and (c) a global trend toward deregulation. Nowhere is this trend more marked than in the so-called last mile local loop bottleneck. The rapid rise in the popularity of Web-based applications is driving industry to build the infrastructure needed to bring high bandwidth, or "broadband," communications to the home. A fixed broadband wireless access (BWA) system is being offered to the public as a choice for the last mile of access. This paper discusses the niche occupied by BWA systems and presents a tutorial introduction to physical and medium access control layers, and the radio link protocol requirements.

1. Introduction

Everything is going wireless [1, 2]. IEEE 802.11, BlueTooth, 3G, WAP, C/TDMA, IEEE 802.16, BWA, LMDS, MMDS, and so on are dotting the wireless landscape. What are all these acronyms? In short, BlueTooth is a wireless LAN for short-range communications within a 30 ft radius distance. IEEE 802.11 can achieve larger range of 300 ft, depending whether inside a building or outside. IEEE 802.11b, the currently available wireless local area network (WLAN), has 11 Mb/s data rate. IEEE 802.11a and 802.11g are expected to provide up to 50 Mb/s. They all work in ISM (Industrial, Scientific, and Medical) band. IEEE 802.16 addresses broadband wireless access (BWA). In North America, Europe and other areas of the world, a widespread demand for low- cost broadband access to new Internet protocol (IP) services is fueling a BWA revolution. These developments strongly suggest that the BWA revolution is real and that fixed BWA technologies will establish deep roots in the telecommunications industry. Figure 1 shows the different types of broadband technologies used today for large scale network.

The growing acceptance of fixed BWA is not only a function of its ability to supply increased bandwidth to large, under-served customer segments and the limited availability of fiber -optic cable but reflects important advantages as well. These advantages include rapid market entry, reduced access expense, modularity permitting flexibility and scalability; lower infrastructure costs due to ability to gradually build- up to meet evolving demand; and the cost--effectiveness of point−to--multipoint (PMP) architectures.

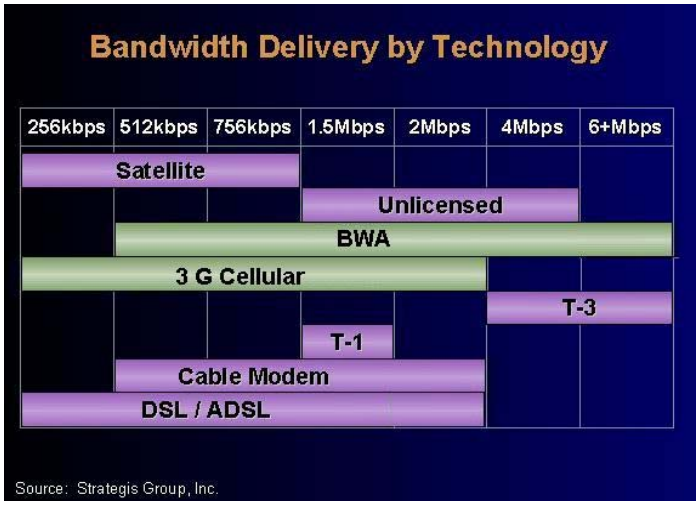

Figure 1, Different types of broadband networks used today with its data rate. (Source: Strategis Group Inc 2001)

2. Motivations

What is BWA and who needs it? Different methods for connecting users to the Internet have been proposed and deployed. The traditional method of connection from home is by using a dial-up modem, a device that converts back and forth between streams of digital data and patterns of audio frequency tones, enabling the data to be sent over telephone lines originally designed to carry voice. At the other end of the line, an Internet service provider acts as a kind of portal through which the subscriber can contact and exchange data with countless nodes around the globe. Although dial-up modems utilize the existing phone infrastructure, their performance is limited. In addition, the need to place a telephone call to establish a connection to the service provider means that access to the Internet is not continuously available. With broadband technologies, people can receive and send text, images, audio and video over the Internet at vastly greater speeds, with virtually no delays. Indeed, there are many ways to connect the home computer to telecommunications services such as the Internet with a striking difference in their speed and performance. The fastest analog modems generally receive and transmit data at 56 kilobits per second. The personal computer in an office is typically connected to others in a building with a local area network (LAN); the most common, Ethernet, has a raw speed of 10 megabits per second -- about 200 times faster than the modem. Unless the building has a dedicated high-speed line to connect their LAN to an Internet service provider (ISP), the user's Internet experience is limited by the modem. Some buildings have high-speed connections, but very few homes or small businesses do. This represents a communications bottleneck that needs to be addressed if the ever-increasing speed of computers can effectively bring the Internet experience to a broad segment of user population.

A variety of techniques and technologies are being proposed to connect homes for high-speed data networks. The first two use methods that make the most out of existing wires to homes: the hybrid fiber-coax makes use of the cable TV industry's infrastructure, but includes fiber-optic lines in addition to coaxial cable; digital subscriber line (DSL) uses the same pair of copper telephone wires to send high-speed data, but relies on frequencies much higher than those used to convey conversations. Inspite of all the fancy marketing campaign promises of cable and DSL vendors, end users are still faced with these realities: limited reach, slow rollout, and poor

performance. The third approach is to run an entirely new wire to the home -- fiber-optic cable. There are several configurations for such a system, including fiber-to-the-curb and fiber-to-the-home, depending on how far the fiber reaches toward the residence. In addition to these wired technologies, there is a strong interest in wireless technologies to address the last mile problem. The fourth method, then, is to use Internet-oriented satellite networks similar to the Iridium satellite-telephone system in that the satellites would communicate directly with the subscriber. In the case of the Internet system, the user would access the data via a smalldish antenna. The fifth approach, a BWA network, is ground-based and is attractive in locations where cable or telephone network infrastructure has not been established.

Although wireless is not the only way to deliver broadband service, it is one of the fastest and most cost-effective. Geographical features such as mountains make it difficult and costly to dig trenches and lay cable in the ground. By contrast, a wireless network using microwave or millimeter wave can be deployed in matter of weeks for providing coverage to both urban and rural populations. A BWA system known as local multipoint distribution services (LMDS) is a ground-based wireless network and is similar to a cellular telephony network. It uses very high frequency radio waves (26-28 GHz) to transmit data between towers and receiver dishes mounted on rooftops. A typical BWA network would utilize the licensed high frequency spectrum, operating in the frequency range of 1.5 GHz - 66 GHz. Figure 2 illustrates the frequency spectrum allocated for BWA usage. LMDS at 26-28 Ghz and MMDS at 2.1-2.6GHz are some popular spectrum under BWA already in use today.

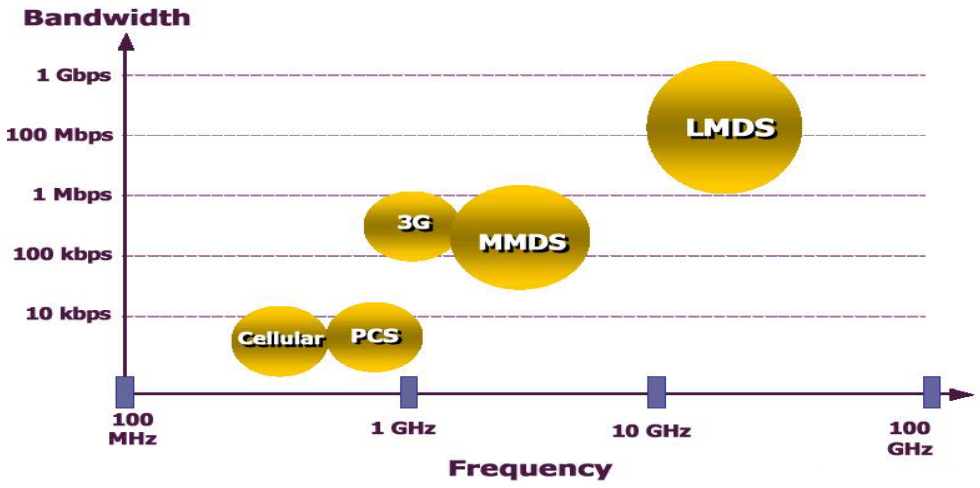

Figure 2, Spectrum allocated for BWA (LMDS, MMDS) services.

3. BWA Issues

While industry experts generally agree that fiber is the ideal networking medium, that assessment is based on technological considerations, rather than on factors such as cost and time. The basic premise behind wireless networks is that the major cost of installing any broadband system based on wire or fiber is not the cable itself but the labor to install it. In congested cities like Rome or London, the costs can easily go up to US $300,000 per square mile [3]. And this does not to include irreparable damage to buildings and roads that have historical value. Like cellular telephones, these networks use radio connections from a base station antenna to remote units at residences. Unlike cellular telephones, Internet users are generally stationary, which greatly

simplifies the system architecture.

BWA system management and maintenance practices are more involved than the wire cable network systems. Challenges such as multipath, fading, noise interference, interference from other base stations, and installation and maintenance cost are some difficulties that BWA network continues to face. Another challenge for BWA technology is for non-line of sight (NLOS) capabilities. The evolution of the smart antenna design and the second generation OFDM modulation format are targeted at overcoming this limitation. The mesh networking technique of routing wireless traffic is another approach to solve the non-line of sight problem. Neither the user nor the service providers needs to make routing decisions, the radios decide the optimum routing for both throughput and latency.

Some early failures in the U.S. indicate that the current BWA technology might not be ready as a single solution. However, success stories in South America, Asia and Europe indicate that fixed wireless can be a great supplement to offer broadband service to terminal users. A building not served by fiber may choose fixed wireless. As the building's demand for bandwidth grows, fiber may become available and fixed wireless will move out farther, serving building and customers even more remote from fiber optic links. Indeed, the first generation of BWA networks ware targeted at business customers, while the second generation is to be extended to residential users. As Figure 3 illustrates, the service can be extended to both large urban business as well as to remote residential areas.

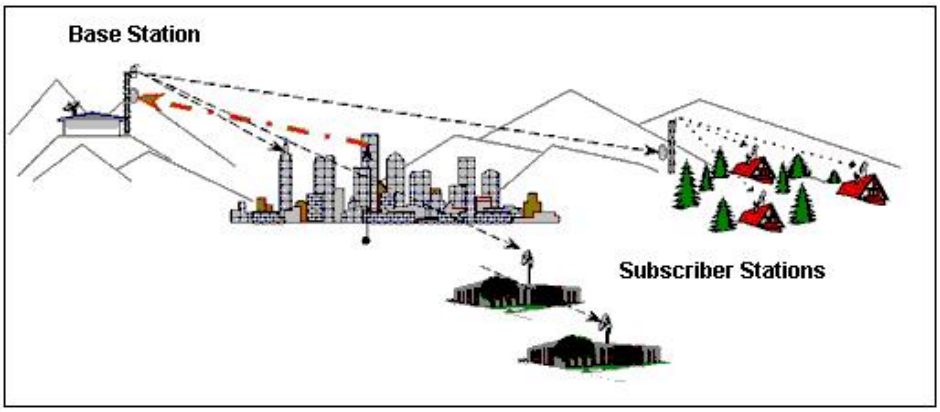

Figure 3. A graphical view a BWA network showing its broadcast point to multipoint nature to different kind of customers. The communication between the base station and the subscriber station are bi-directional.

4. BWA Network Structure

BWA network is primarily used as a point to multipoint topology with a cellular deployment of base stations, each tied to core networks and in contact with fixed wireless subscriber stations. The base stations are generally located on a tower and the subscriber stations typically include rooftop mounted antennas and radio units connected to indoor network interface units.

A completed BWA system is typically comprised of multiple subnets in a star topology. Structurally, it is similar to the historical slotted Aloha network proposed in the 1970s. The transport mechanism works in the way that the downstream, from the central base station to the

subscriber stations, is broadcast**,** while the upstream from the subscriber stations to the central base station uses time division multiple access (TDMA). Figure 4 illustrates some key components of the network. There can be thousands of customer primise equipment (CPE) on the rooftop of different buildings.

The central base station can be connected with other server applications to the Internet backbone through optical fiber. The base station (BS) is a switching device often seen as a network bridge or router that interacts directly with the subscriber station. On the subscriber station (SS), the modem will act as the data port, which resumes the data transport in wire again.

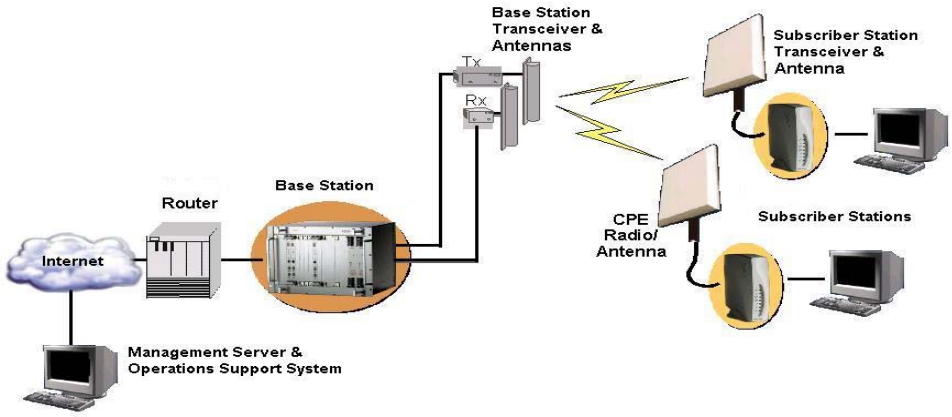

Figure 4. The component view on a micro section of the BWA network.

Referring to the OSI model, the physical and data link layers of a BWA network are the two layers that distinguish it from other networks. They specify the communication methods and requirements between the modem at the Subscriber Station (SS) and the Base Station (BS).

The network protocol of a BWA system follows the DOCSIS (Data Over Cable Service Interface Specifications) standard extensively, with modification for wireless application [4]. Different signaling formats have been used to transport the data. FDD (frequency division duplex) and TDD (time division duplex) are two competing transmission protocols while ATM (asynchronous transfer mode) and IP (Internet Protocol) are two competing network protocols.

5. ISO layers

Physical Layer

The BWA network is a two-way communication network. The digital data goes through a sequence of signal processing steps, as illustrated in Figure 5. For the downstream, the processed signal would be transmitted from the base station to the transmitter, to the antenna, repeater, receiver and eventually to the subscriber modem. The physical distance of the link can be extended for hundreds of kilometers at the receiving end [5]. For the upstream, the reverse processing would take place. The modulated and processed microwave signal would be transmitted from the subscriber side back to the base station through multiple transceivers. Modulation scheme is an important process that defines the spectrum utilization at the physical layer.

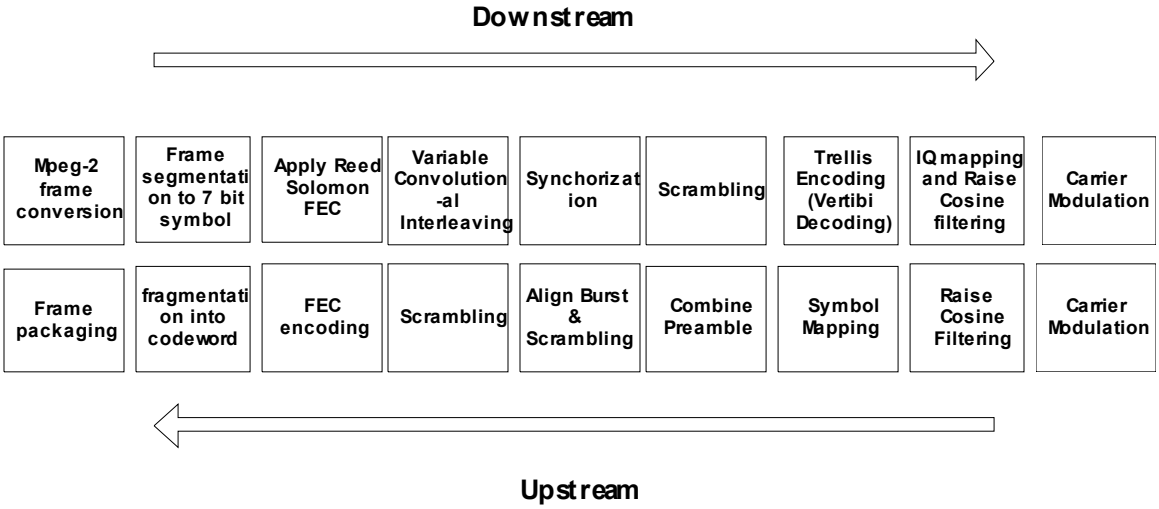

Figure 5. The processing work by step in both the base station and the subscriber station [3].

The modulation format can be OFDM (Orthogonal Frequency Division Multiplexing) with interleaving and coding,, direct sequence CDMA (Code Division Multiple Access) with rake receiver, or standard single carrier QAM (Quadrature Amplitude Modulation) with equalization in each sub channel for a frequency between 1.5 GHz - 66 GHz. A commonly used 6 MHz channel bandwidth in the U.S. corresponds to channel symbol rates of 5 mega symbols per second (MSb/sec). 128-QAM modulates 7 bits per symbol, which is equivalent to a channel data rate of up to 35 Mbps [5].

Channel coding adds redundancy to the transmitted data to allow the receiver to correct transmission errors. Reed Soloman convolutional coding (3rd step of Figure 5) combined with variable-depth interleaving is used as the coding scheme for error protection. Interleaving here refers to the shuffling the symbol positions by inserting unrelated symbols to the normally adjacent but related symbols. Based on the level of interleaving, the data on the forward (downstream) path is protected from noise burst lengths. This allows the system to deliver 128-QAM signals with a bit error rate (BER) of less than 10 ^ -8 at a carrier to noise of 30 dB, a minimal level that the system has to achieve in order to have steady performance [6]. Although variable depth interleaving allows about 10 dB of improvement, one of the side effects is that it adds latency to the downstream.

The return path (upstream) modulation format typically uses 16-QAM for the purpose of a lower transmission power, while it maintains the same signal to noise quality. Unlike the downstream, which is a broadcast, the return path channel uses time division multiple access (TDMA) for which the upstream channel is divided into equal-time segments called mini-slots. A mini-slot size is generally 128 bytes for every 0.1 msec [6]. The base station controls the use of each mini-slot by assigning contiguous intervals of mini-slots to individual modems to transmit in, or makes them available for contention by groups of modems to transmit in.

Data Link Layer − LLC

The data link layer is comprised of the logical link control and medium access control layers. The logical link control (LLC) provides the Service Access Point (SAP)**,** which supports the multi-access and shared medium functionality. Four different MAC-layer Protocol Data Units (PDU) are specified: variable-length, multiple ATM cell, multiple Synchronous Transfer Mode (STM) cell, and MAC management. The variable-length and MAC management PDUs are encapsulated as 802.2 LLC frames [7]. A SAP is provided to allow mapping of ATM and STM cells into the native MAC format. LLC also provides higher layers of QoS requirement mapping into the MAC format QoS mechanisms. It associates the transport and QoS requirements with different services and prioritize transmission over up- and downlink. Figure 6 shows the location of the logical link layer in the OSI model and it also shows where the process take place.

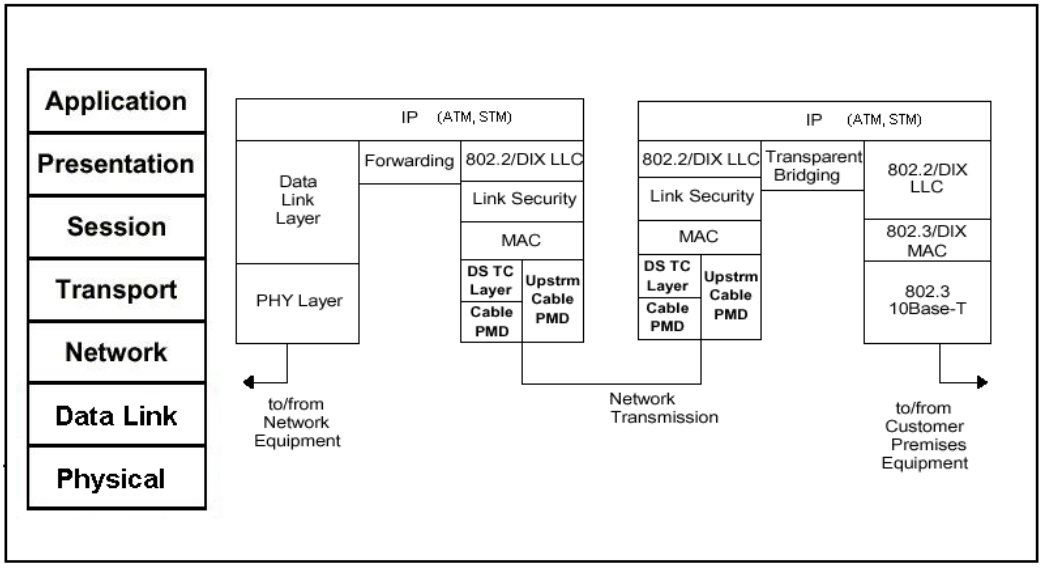

Figure 6. IEEE 802.16 allows four different protocol data formats: IP, ATM, STM and MPEG to co-exist [7].

Data Link Layer − MAC

Medium Access Control (MAC) is critical in a BWA network. The major MAC functions include−controlling up and downstream transmission scheduling, admission control to utilize available channel capacity, and link initialization and maintenance. Figure 7 illustrates the frame format [8]. Note how the original IP packet header is replaced with It replaces some unique fields. A frame is comprised of a variable length header followed by its payload. The MAC header varies in size based upon the MAC message type and the use of extended headers. Extended headers convey information such as keying material for security. And of course, the payload varies as a function of the payload content. Alternatively, the payload may contain multiple ATM cells, each 53 bytes in length.

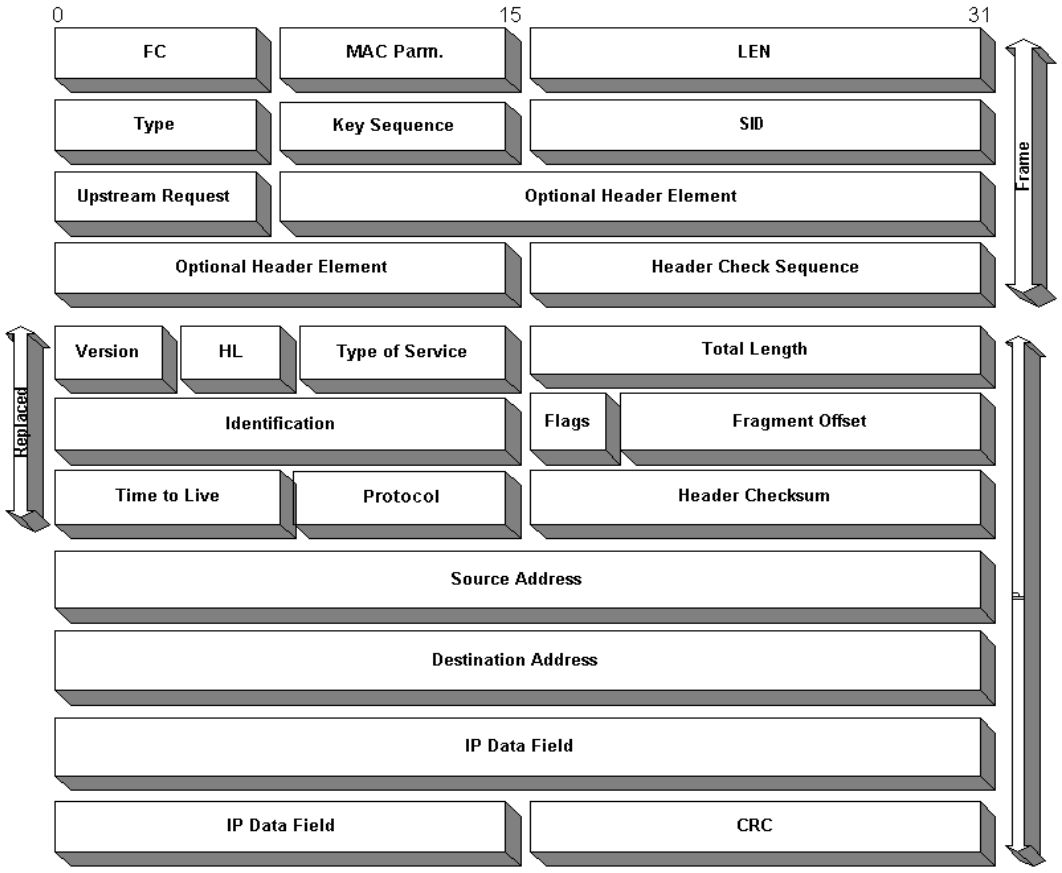

Figure 7. BWA unique frame header format on top of the standard IP header packet. SID (Service Identification) is the sole representation for each individual data segment in the network.

Extending from Figure 7, frames are further segmented into MPEG cells. MPEG is the standard transmission protocol, which allows multiple services to share the same RF (Radio Frequency) carrier. MPEG enables operators to broadcast voice, video and data in the same forward channel as long as all three traffic types are encapsulated with MPEG. The unified MPEG cell size of 188 bytes shares some of the benefits of the ATM cell control mechanism. A 5 bytes MPEG header enables a modem to identify individual packets within the stream so the devices know which packets to decode. This mechanism, called a program identifier (PID), is present in all MPEG frames [4]. This PID value is unique for each vendor, and modems will operate only on MPEG packets with this PID. In addition, MPEG provides a frame structure that facilitates channel lock.

The MAC layer protocol controls access of the return path. Because several modems may have data to transmit at any given time, the MAC protocol enables the base station to indicate when each modem can transmit and for how long. A good coordination would avoid collisions to occur and therefore increases usage efficiency. The MAC protocol provides a request/grant mechanism. This "request and grant" mechanism works as the follow: A modem requests from the base station an opportunity to transmit a certain amount of data. As the BS receives requests from all the modems, it reserves mini-slots on the return path. Periodically, the base

station broadcasts a message to the modems over the forward path indicating the specific mini-slots granted to each modem. By reserving bandwidth through this request and grant mechanism, modems are guaranteed a collision-free interval for transmittance. The BS allocates bandwidth to modems based on the types of service that the user subscribes to.

6. Auto Discovery and Provisioning

Modem registration process is critical in understanding how the communication link is established. It is the first initial communication for the modem to obtain key information of the network. When a modem is turned on, it performs the following sequence**:**

Channel acquisition: The modem scans for a downstream channel, obtains QAM lock, and finds MPEG cells with the pre-defined PID. The MPEG framing will be stripped away and the resultant MAC frames are passed to the MAC layer for processing.

Obtain upstream parameters: The modem waits to receive three MAC messages that the base station repeatedly sends on all downstream channels. The first message is the time synchronization (SYNC) message to provide a common time reference to all modems. The next message is the upstream channel descriptor (UCD). The modem must find a UCD that describes an upstream channel and modulation format that matches the modem's capabilities. The final message is a bandwidth allocation map (MAP) that describes transmission opportunities on the upstream channel referred to in the UCD. The MAP message contains the mini-slot information that indicates when a modem can transmit and for how long.

Ranging: Ranging allows SS to calibrate timing, power, frequency and equalizer ooefficients. Because each modem is a unique distance from the base station, each modem will have unique settings at these parameters. To begin the ranging process, the modem transmits a ranging request message to the Base Station. Upon receipt of this message, the BS sends a ranging response message addressed to that modem. If the modem does not receive a ranging response message, it will adjust its transmit parameters such as output power and wait a random number of initial maintenance opportunities before sending another request. The BS keeps track of the parameter offset and determines corrections. Upon receipt of the ranging response, the modem adjusts its parameters based on the corrections and transmits a second ranging request to the BS. This process continues until both sides are satisfied with the timing, frequency and power settings. In addition to the initial connection establishment, the ranging process is repeated for each modem at regular intervals during periodic maintenance opportunities that the Base Station schedules.

IP layer establishment: Once timing, frequency and power are set, the modem must establish IP connectivity. It does so by invoking the dynamic host configuration protocol (DHCP), which causes the modem to be assigned an IP address. Once an IP address is obtained, the modem requests time of day (ToD) to get the real date and time to timestamp certain messages and log files. This differs from the SYNC message, which simply maintains a continuous 32-bit counter that reflects time ticks in the MAC layer.

Registration: Registration is a form of capability negotiation. Registration begins with the modem downloading a configuration file. The modem uses the trivial file transfer protocol (TFTP) to download the configuration file from a server. The configuration file contains information such as how much bandwidth or services levels the modem is allowed to use. During the final registration phase, the modem sends a message to the Base Station confirming the configuration

file it received. The BS also retrieves a copy of the configuration file from the configuration file server to ensure that the modem will be using only authorized services. Only after the Base Station crosschecks the configuration file data is the modem finally allowed to transmit real user data onto the network.

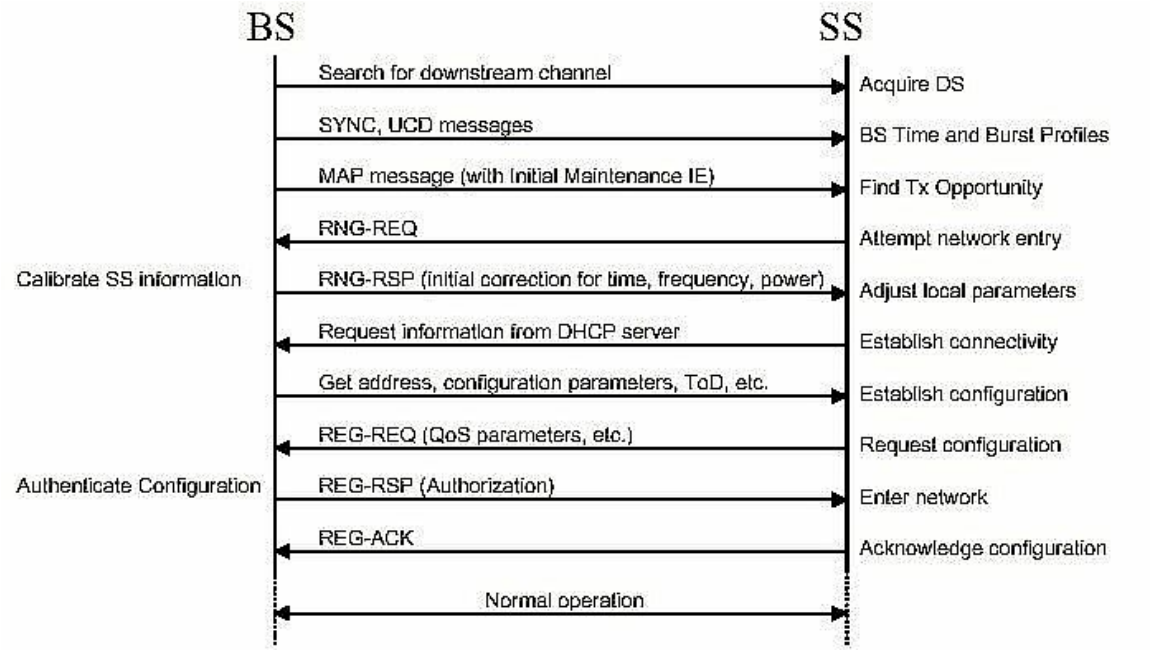

Figure 8. Interaction between the base station and the subscriber station during provisioning. This shows the process that the devices have to go through to establish a communication link [4].

7. Security

Security issues for IEEE 802.16 have not yet been thorougly studied. However, much of the process articulated for 802.11 is expected to be the same. The discussion in this section pertains to 802.11 practice.

Wireless security is not much different from wired security. There are several standard security issues [10], wired or not: authenticate whom you are talking to, secure the data as it travels from the source to the destination host, and ensure that the traffic hasn't been altered en route. These steps are not unlike what Amazon.com or E-Trade does in the wired world. However, wireless has some unique difficulties, such as limited bandwidth, high latency and unstable connections. Several options, still evolving, address these issues. Many of these options were first developed in the context of web-enabled mobile and cellular phones. Prominent among these is the Wireless Applications Protocol (WAP) which is really a set of *de facto* protocol standards developed by the mobile telephone industry. WAP evolved out of Hypertext Transfer Protocol (HTTP) so widely used by desktop computers to process Web pages. WAP performs this fucntion on a mobile device through Wireless Transport Protocol (WTP). That is, HTTP is to desktop computers as WTP is to mobile devices.

This anlaogy between a desktop computer and a mobile device can be carried further. A web browser can encrypt data transmitted from a desktop PC to a Web page server via Secure Socket

Layer (SSL) protocols. (The little padlock icon on the web browser tells if this protocol is active or not. That is, when a Web browser sets up an SSL session with Web server, the browser and server are talking directly and only the Web server will be able to receive the information.) WAP has a similar capability called Wireless Transport Layer Security (WTLS) to encrypt communications between a wireless device and the gateway (i. e., the interface between the wireless and the wired world.), but with a difference. WTLS is not SSL, so it can't directly communicate with SSL-enabled Web servers. Although communications between the mobile device and the gateway can be encrypted and from the gateway to the wired network can be encrypted, there is a potential security vulnerability at the transition point because the translations between wireless and wired protocolos is done under un-encrypted conditions. In other words WTLS does not provide for full end-to-end security.

Two options are becoming available for end-to-end WTLS security. The first is WTLS tunneling, which tunnels WTLS traffic through a service provider's network to a remote WAP gateway. WTLS proxy, meanwhile, proxies WTLS connections through the carrier's WAP gateway. Neither solution is widely deployed and each will require partnerships with carriers and phone manufacturers to implement.

Understanding WTLS

WTLS provides for client or server authentication and allows for encryption based on negotiated parameters between the handheld device and the WAP gateway. WTLS's key exchange protocol is uniquely suited for wireless applications. Vendors can implement any of three classes of authentication types.

Class 1 (anonymous authentication) has limited use -- mainly for testing purposes -- because end users have no way of determining to whom they are talking. The client forms an encrypted connection with an unknown server. Class 2 (server authentication) probably will be the most common model used. As with SSL, once clients are assured they are talking securely to the correct server, they can authenticate using alternative means such as user name/password. Class 3 (server- and client-authentication) is possibly the strongest class, as the server and the client authenticate each other's WTLS certificate.

Client certificates required for Class 3 authentication pose special management problems. Not only must the key pairs be generated on the mobile device (or generated in bulk and securely loaded onto the mobile devices), but the client certificate has to be safeguarded and managed until the certificate expires. Client certificates need not be retained on the handheld device. Rather, during negotiation, the client may refer the WTLS gateway to a directory to retrieve the client certificate from a directory. That saves the bandwidth needed to send the client certificate over the air and may improve negotiation performance; however, the WAP gateway needs to trust the directory the client refers to in order to have any assurance of authentication. The directory that holds user certificates also must be available at all times, or it won't be able to retrieve the certificate when requested. The key pair associated with the client certificate resides only on the client.

The WTLS specification does specify cryptographic algorithms that may be supported by WAP devices, but doesn't require any for basic functionality. For example, the WTLS specification provides support for the RSA, Diffie-Hellman and Elliptic Curve Diffie-Hellman key exchanges, but in practice, most vendors are focusing support on RSA because of its widespread use. Similarly, bulk encryption ciphers such as RC5, DES, 3DES and IDEA are specified; however, DES and 3DES promise to be the most widely used because of existing implementations.

One of the concerns with cryptography regards export of certain key lengths to other countries. The WAP Forum is sensitive to this issue, and the WTLS draft supports various key lengths used with the bulk encryption algorithms, so that the security parameters can be negotiated according to geographic need rather than server support.

WTLS is all about adding security to low CPU-powered wireless devices by making the cryptography efficient. Because PDA and cell phone CPUs are typically slow, using SSL end to end can take anywhere from 30 seconds to several minutes, depending on the key size used to negotiate an SSL connection. WTLS can use familiar public key exchange algorithms, such as RSA or Diffie-Hellman, but these algorithms are resource-intensive and, therefore, slow. Elliptic Curve (EC) cryptography promises to require far fewer resources and should find wide deployment for CPU-starved PDAs and cell phones.

Conclusion

Broadband wireless access is emerging as a legitimate local access platform for the delivery of high quality digital data, video and voice services. Wireless cable technology has limitations, but it also has key benefits, most notably the ability to rapidly introduce high speed data access throughout a metropolitan area with the cost for delay of wired plant upgrades. Rather than stringing thsouands of miles of fiber, coax, or twisted pair wiring, a wireless operator installs a headend and transmission tower and is open for business. It is hoped that through this tutorial paper, which provides an introductory explanation of the BWA network, and through the physical and the network characteristics, user can have a better understanding of the technology.

Acknowledgement

This work is supported in part by the AFOSR grant F49620-01-0327 to the Center for Digital Security, University of California, Davis.

References

[1] Scoro, J., LMDS: "Broadband Wireless Access," *Scientific American*, 10, 1999. http://www.sciam.com/1999/1099issue/1099skoro.html

[2] Clark, D. D., "High-speed Data Races Home," *Scientific American*, 10, 1999. http://www.sciam.com/1999/1099issue/1099clark.html#authors

[3] Bolcskei, H., Paulraj, A. J., Hari, K. V. S. Nabar R. U., Lu, W. W. "Fixed Broadband Wireless Access: State of the Art, Challenges, and Future Directions" *IEEE Communications Magazine* 1, 2001

[4] Sater, G., Arunachalam, A., Stamatelos, G., Elwailly, F. "Media Access Control Protocol Based on DOCSIS 1.1" IEEE 802.16 Air Interface Specification in IEEE 802.16.1 Medium Access Control 2000

[5] Kim, B. Shankaranarayanan N. K. , Henry, P. S., Schlosser, K., Fong, T. K. "The

AT&T Labs Broadband Fixed Wireless Field Experiment" *IEEE Communications Magazine* 10, 1999

[6] "Data-Over-Cable Service Interface Specifications－SP-RFI-I04-980724", Cablelabs, June, 2000.

[7] Jones, D. "DOCSIS Dissected－The Nuts and Bolts of Version 1.0," *Communications Technology*, 1999.

[8] Peterson, D. *Computer Networks－A System Approach*. Morgan Kaufmann 2000.

[9] "Data-Over-Cable Service Interface Specifications－SP_OSSIV1.1_I02_000714", Cablelabs, September, 2000.

[10] Fratto, J., "Tutorial: Wireless Security," *Mobile and Wireless Technology*, January 22, 2001. http://www.networkcomputing.com/1202/1202f1d1.html