Bachelor's Thesis (UAS)

Degree Programme: Information Technology

Specialization: Internet Technology

2013

Roshan Upreti

WiMAX: An alternative communications system.

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree Programme | Information Technology

February 2013 | 37 pages

Instructor(s): Patric Granholm

Roshan Upreti

WiMAX: An alternative communications system

The thesis aims to study the possibility of a direct distribution of wireless internet access to the end receiving devices for communication purposes in a similar manner to that of the operational procedures of cellular network services via radio communication systems. The thesis aims to serve as a report from a theoretical study regarding an efficient way of implementing wireless network, WiMAX. WiMAX, in short, is a type of Wireless Metropolitan Area Network (WMAN) technology.

The thesis mainly comprises of the aspects that summate to the fundamentals of the radio communications and wireless network system. The major focus has been on the types of wireless network in existence today, followed by a brief study on QoS, Security, and the possibility of implementing VoIP over wireless network.

KEYWORDS:

WiMAX, VoIP, QoS, WMAN, cellular, Radio communications, wireless network, security

CONTENT

FIGURES

Figure 7. A prototype WiMAX network

http://www.wimax.com/wimax-tutorial/wimax-radios

Figure 8. A WiMAX radio

http://www.wimax.com/wimax-tutorial/wimax-radios

Figure 9. Omni directiona antenna

http://image.made-in-china.com/2f0j00CBJTZFAWdmcv/Wimax-Outdoor-Omni-Directional-Figerglass-Antenna.jpg

Figure 10. Broadcasting pattern of an omnidirectional antenna

http://www.wimax.com/wimax-tutorial/wimax-antennas

Figure. 11 A sector antenna

http://www.grand-universe.com/upload//big/product05358510012675113O7.jpg

Figure. 12 Broadcast pattern of sector antenna

http://www.wimax.com/wimax-tutorial/wimax-antennas

Figure 13. A panel Antenna

http://www.mars-antennas.com/archimg/365,600x600,img.jpg

Figure 14. PSTN switching

WiMAX Handbook, Building 802.16 wireless networks, Frank Ohrtman.

Figure 15. Softswitching

http://www.cse.wustl.edu/~jain/cse574-06/ftp/wimax_voip.pdf

List of Abbreviations (OR) Symbols

AK	Acknowledgement Key
AP	Access Point
BS	Base Station
CBC	Cipher Block Chaining
CID	Connection Identifier
CPE	Customer Premises Equipment
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
FEC	Forward Error Correction
HMAC	Hash Message Authentication Code
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet protocol
ISP	Internet Service Provider
LAN	Local Area Network
LOS	Line of Service
MAN	Metropolitan Area Network
MAP	Manufacturing Application Protocol
MGCP	Media Gateway Control Protocol
MS	Mobile Station
NIC	Network Interface Card

NLOS	Non Line of Service
OFDM	Orthogonal Frequency Division Multiplex
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RSA	Rivest Shamir and Adleman (Encryption algorithm)
RTP	Real-time Transport Protocol
SAID	Security Association Identifier
SIP	Session Initiation Protocol
SS	Subscriber Station
TEK	Traffic Encryption Key
TFTP	Trivial File Transfer Protocol
UL	Uplink
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

1. Introduction

Wireless Network has undoubtedly become an everyday term in the modern day world. Whether it comes to using mobile phones or using wireless internet at home and offices, the technology of wireless network has found its way to make an impact on the daily routine of the modern day society. Easy deployment and huge scalability is gradually turning the wireless network system as an eminent choice amongst many users, as well as enterprises. Low distribution cost due to the absence of wires, a wide coverage area, customizable as per requirements, can be termed as the key benefits of adopting wireless network, among many others. Due to the variety of choices in deployment, wireless networks can be implemented in various forms like WANs (Wide Area Networks), WLANs (Wireless Local Area Networks) and PANs (Personal Area Networks) to meet the requirements .

The thesis aims to theoretically study the possibility of a direct distribution of wireless internet access to the end receiving devices, covering a wide area using a wireless network technology best suited for the task. The objective of the thesis is to plan/design, and theoretically implement a wireless network technology that would serve as an operational platform for mobile broadband internet with integrated VoIP (Voice over IP) services. Since there are several types of wireless network technology, a brief study and comparison of all the major wireless network that exist is carried out, and the technology that suits best for the objective is discussed in detail.

2. Technology Study

Wireless, is a term, massively used in the field of telecommunications and networking, to describe the type of network which operates, using electromagnetic waves as the medium to maintain communication between two or multiple nodes. The implementation of a wireless networking system involves the usage of devices, like wireless routers, NICs with wireless capabilities and APs, to maintain connectivity among the devices involved in the process. The operational range, in terms of distance of a wireless network varies depending upon the intended target range, and the spectrum of radio wave it is implemented upon. In order to create a small Wi-Fi network at home to share the internet connection, or to connect the entire city via Metropolitan Wireless Area Network, one can manipulate the wireless network in accordance to the need to meet the desired results.

Inspite of its technological perks over wired network, wireless network technology has its own sets of physical limitations. Wireless networks are vulnerable to electromagnetic waves; radiaton generated from electronic devices, associated with electric and magnetic fields and many other interferences, if deployed in improper conditions. The presence of electronic devices, like TV, cordless phones, microwave ovens in the vicinity of network range causes electromagnetic interference which highly reduces the signal strength of the network. The signal strength is also affected by many other objects, like building materials and machinery.

On the basis of their existence and operating manners, there are four types of wireless networks in use today:

1. WLANs (Wireless Local Area Networks)
2. WPANs (Wireless Personal Area Networks)
3. WWANs (Wireless Wide Area Networks)
4. WMANs (Wireless Metropolitan Area Networks)

2.1 Wireless Local Area Networks

A Wireless Local Area Network or WLANs in short, is a Local Area Network that provides the network /internet access to user(s) without having to rely on the wired Ethernet connections. WLANs are designed to operate within a certain area, most commonly within a radius of 20 to 92 meters. The operational procedure of WLANs is so that, the wireless signal is broadcasted by devices like wireless routers, APs (Access Points), and the devices equipped with wireless NICs (Network Interface Cards) detect those signals, hence establishing the connectivity with the network. They are found most commonly at homes, schools/campuses and some office buildings where there is a need of providing the network access up to a certain area limit.

WLANs are implemented on the basis of set of standards called IEEE 802.11, created and maintained by IEEE (Institute of Electrical and Electronic Engineers) LAN/MAN standards committee (IEEE 802). They are operated in 2.4, 3.6 and 5 GHz frequency bands. The different types of WLANs standards in use today are 802.11a, 802.11b, 802.11g and 802.11n, which primarily differ from each other based on their operating range, data transfer rate and susceptance to barriers and interference provided by nearby devices like televisions, cordless phones etc. WLANs are capable of transferring data at a speed rate ranging from 1 to 54 Mbps, but the new WLAN standards like 802.11n has made it possible for the speed to range from 300 to 600 Mbps. As far as the network security is concerned, a WLAN can be secured using security standards provided by 802.11x standards. (WLAN Best Practices Guide, 2013)

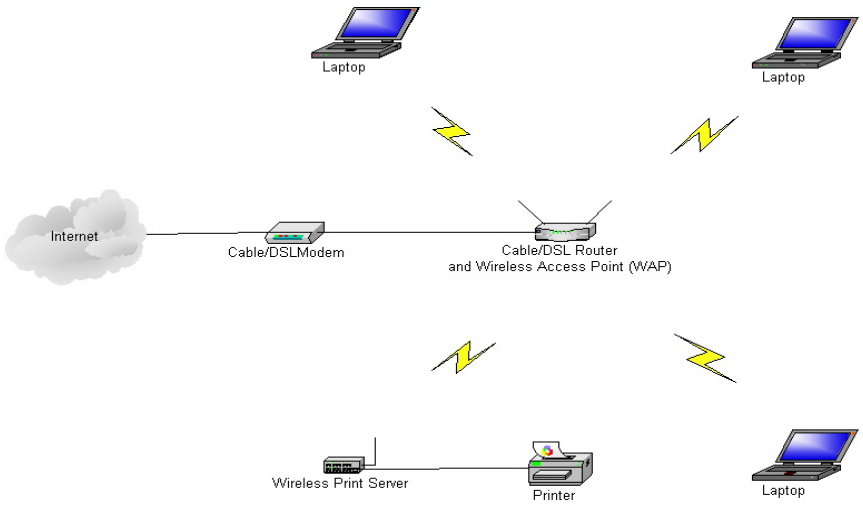


Figure 1. A WLAN network involving laptops, router, modem and network printers

2.2 Wireless Personal Area Networks

A Wireless Personal Area Network (WPAN), is a wireless network that is used to interconnect devices whose operations basically exists around an individual's personal workspace. WPANs are based on the IEEE 802.15 standards, and they only have a varying coverage area ranging from few centimeters to a few meters, depending on the type of device(s) operating. Thus, the coverage area of WPANs is relatively small; the technology is still undergoing rapid development, and is being proposed to be operational around at a frequency band of 2.4 GHz. WPANs rather serve specific purposes like interconnecting computing/communication devices that are in close proximity. There are several WPAN technologies that exist in the market today. Bluetooth ™, Infrared, and ZigBee. (SearchMobileComputing, 2013)

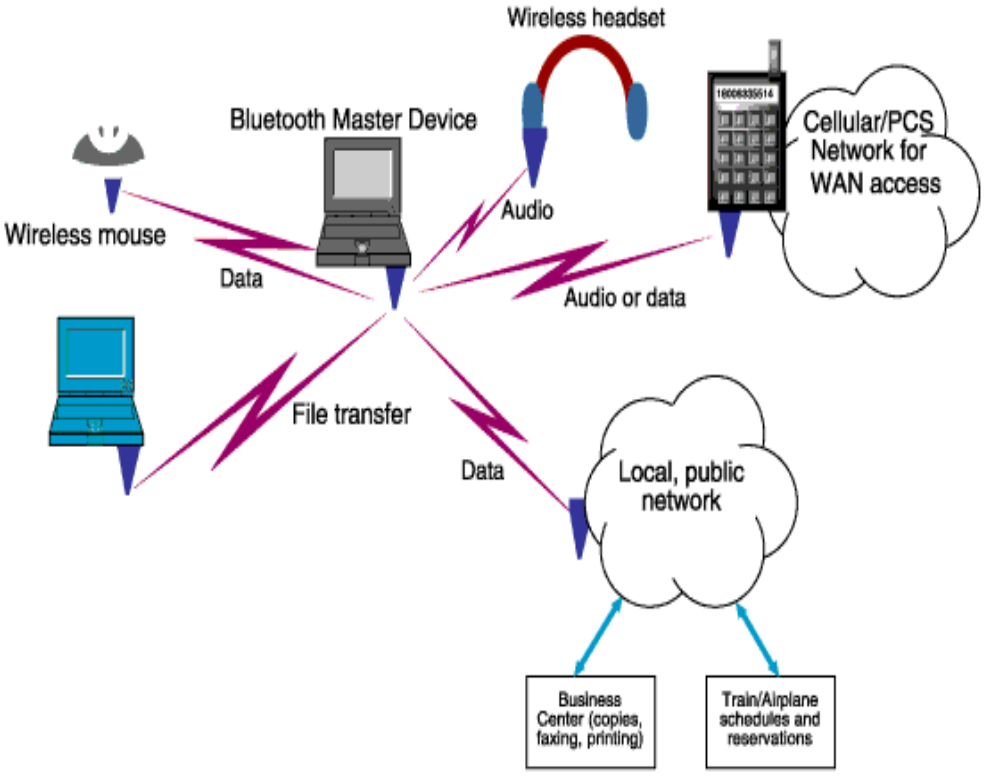
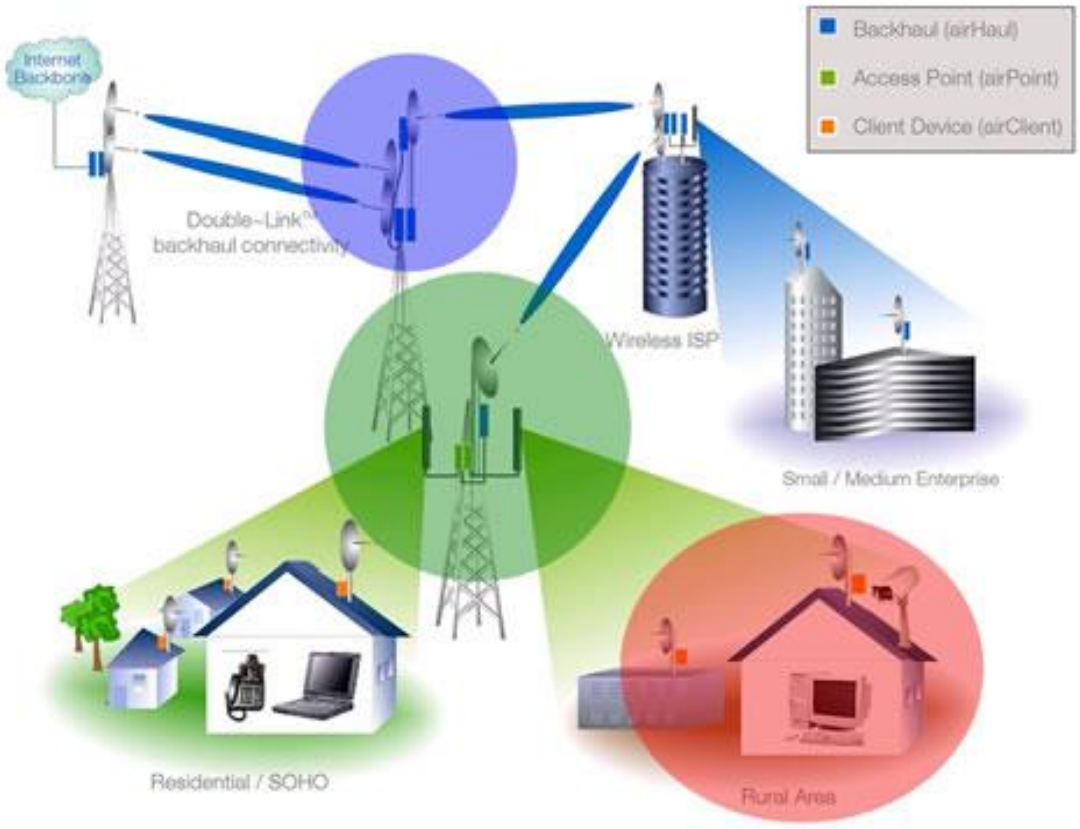


Figure 2. A WPAN network consisting of computers and other wireless devices.

2.3 Wireless Wide Area Networks

A Wireless Wide Area Network (WWAN), is a type of wireless network that covers a large geographical area (state, province or the entire nation). The intended coverage area is divided into smaller regions or cells, and a WWAN interconnect these cells to establish network connectivity. These services are usually provided by the cellular service providers and delivered to commonly used devices like cell phones for a certain amount of usage fees. WWANs carry both data and voice traffic via radio signals over analog, digital and PCS networks. Introduced in the early 1980s for voice communication and data communications since the early 1990s, WWANs have undergone through massive updates and revisions to catch up with the advancements in the technology and meet the growing users' demands. (SearchEnterpriseWAN, 2013)



.

Figure 3. A WWAN network consisting of base stations and different distribution areas.

2.4 Wireless Metropolitan Area Networks

A WMAN is a type of wireless network having an intended coverage area that spans, approximately throughout the size of a city. Its coverage zone is larger than that of WLAN, but smaller than that of WWAN, allowing the inter-communication of multiple terminals using a single access point, within a radius of up to 40 km. Based on IEEE 802.16 standards, WMAN networks are capable of transferring data at an average speed of 1 to 10 Mbps within the range of coverage. WMANs interconnect a number of LANs or WLANs using a high-speed backbone link, such as fiber optic, and may provide a connection to larger networks like the internet. They are used mostly by big enterprises and schools due to its easy mobility and higher data transfer speed. WiMAX is a type of a WMAN network. (IEEE 802.16 Wireless Metropolitan Area Network)

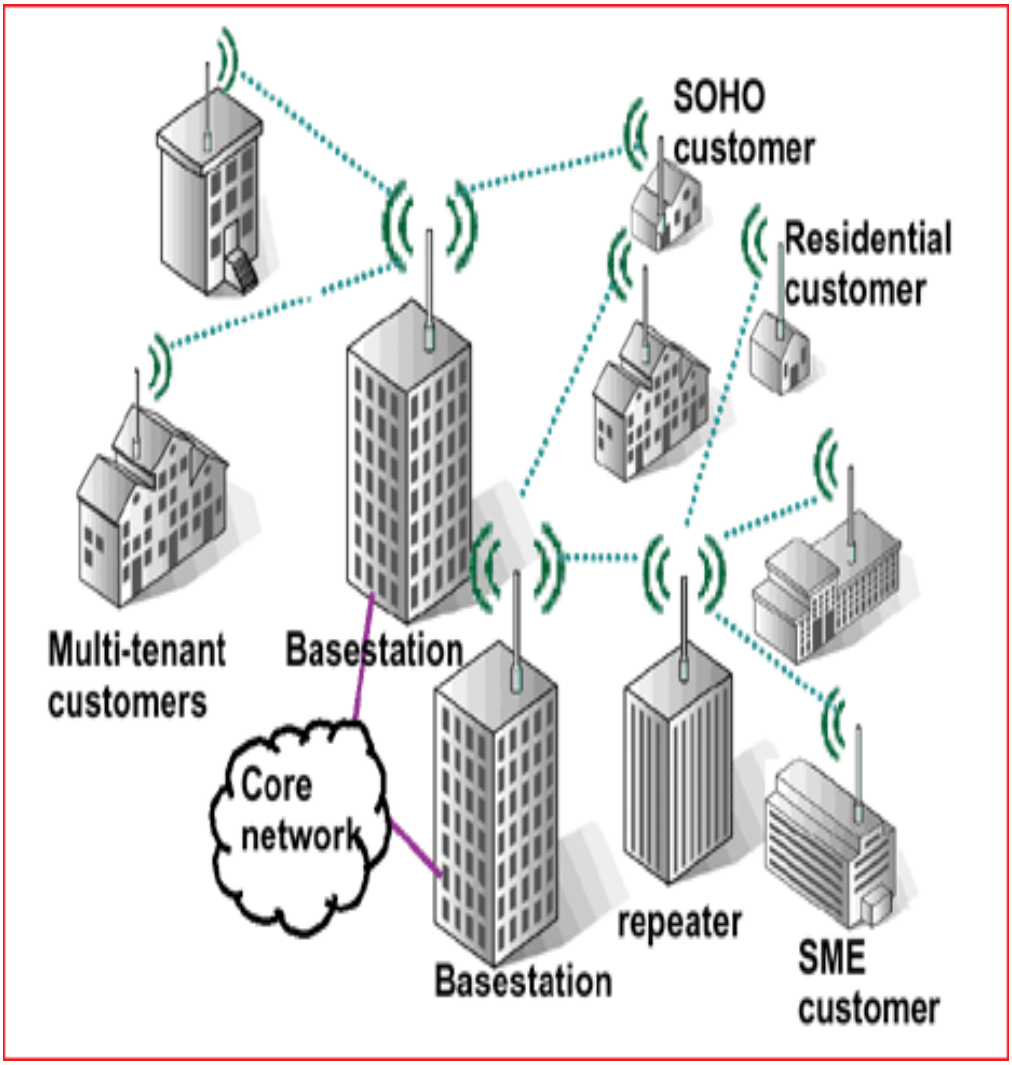


Figure 4. A WMAN network consisting of base stations, repeaters and customers.

3. WiMAX – Introduction and working mechanism

Worldwide Interoperability for Microwave Access or WiMAX in short is a form of wireless network technology intended to be implemented as a form of Wireless Metropolitan Area Network, WMAN. Its features are similar to that of WLAN, but with an intense magnitude. WiMAX covers a much larger area than that of WLAN. WiMAX can indubitably be termed as a modern day optimized technology for a better, faster and reliable mobile broadband internet access. Not only does it provide a faster data transfer rate, but also maintains a Quality of Service (QoS) required by a lot of internet applications. Due to its versatility in implementation, it can basically replace various singular technologies being used for different purposes to form a single framework that meets all those aforementioned purposes, hence proving its coherency. For instance, in a wireless scenario, it can replace the copper wiring technology to provide subscribers with different services like internet access, cable TV services, and even as a replacement to cellular network services due to its Voice over IP (VoIP) support, with an assured QoS.

The working mechanism of WiMAX is similar to that of various wireless networks. Understanding in the most basic form, a working WiMAX network involves the successful communication between the WiMAX tower and the receiving device. Enabling a successful communication system requires many intermediary but essential acts to be carried out smoothly.

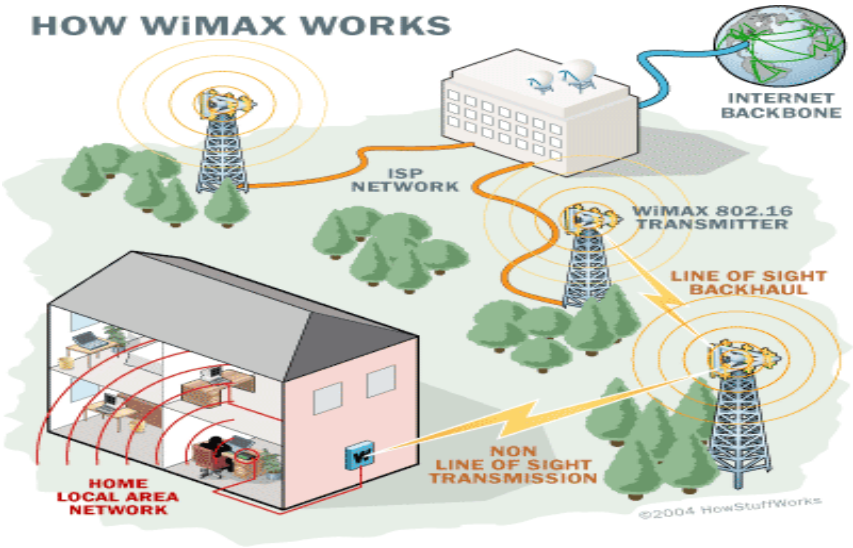


Fig. 5 A WiMAX network with various components and receivers.

Based on Figure 5, the WiMAX system illustrated consists of WiMAX tower stations, (similar to that of tower that gives away the mobile phone signals) capable of connecting to the internet using a high bandwidth, cable connection through the ISP network. The WiMAX tower or Base Station (BS) has a capacity to cover up area as large as 7770 square kms, along with the ability to connect to another WiMAX tower (can be also referred to as backhaul) using a line of sight via a microwave link. The line of sight is a type of propagation where the data transmission occurs when the sending and receiving stations are in a view of each other with an absence of any obstacle between them. Line of sight transmissions use higher frequencies with ranges reaching a possible frequency range of 66 GHz. There is also a non line of sight transmission in which the sending and receiving stations need not be in a view of each other. For example, this sort of transmission is used when a small WiMAX receiver antenna on a computer connects to the WiMAX tower. A lower frequency range is used when implementing the non line of sight transmission, ranging from 2-11 GHz, similar to that of Wi-Fi. (Marshall and Grabianowski. 2012)

Based on the operational endeavors, WiMAX can be deployed in two forms:

3.1 Fixed WiMAX

Fixed WiMAX refers to the type of WiMAX deployment in which the distribution of WiMAX services look similar to that of fixed-wire line service, with most of the devices being confined to the air interface. In a fixed WiMAX, the communications take place via a wireless link between the CPE and a remote NLOS WiMAX base station, and the whole process is usually aided by the usage of an antenna mounted on the rooftop. A fixed WiMAX operates in the 2.5 and 3.5 GHz frequency bands, and the license free 5.8 GHz band.

3.2 Mobile WiMAX

In Mobile WiMAX, the WiMAX enabled mobile devices connect to the WiMAX services via a wireless link, in a frequency range of 2-6 GHz. The type of connection is NLOS. In a mobile WiMAX, the clients are able to hand off between Base Stations and roam between the service areas.

(WiMAX, 2013)

3.3 Orthogonal Frequency Division Multiplexing (OFDM)

WiMAX uses OFDM to manage its air transmission process. OFDM is a process of splitting digitally modulated signals into several narrowband channels at different frequencies. OFDM uses a technique called spread spectrum that distributes the data over a large number of carriers, precisely spaced frequency wise. This precise spacing forms orthogonally, thus isolating a particular demodulator from frequencies other than its own. OFDM is useful, especially when multi-path channels are involved. The transmitted signals reach the subscriber travelling across different paths of different length, creating difficulties extracting the original information due to the Inter Symbol Interference (ISI).

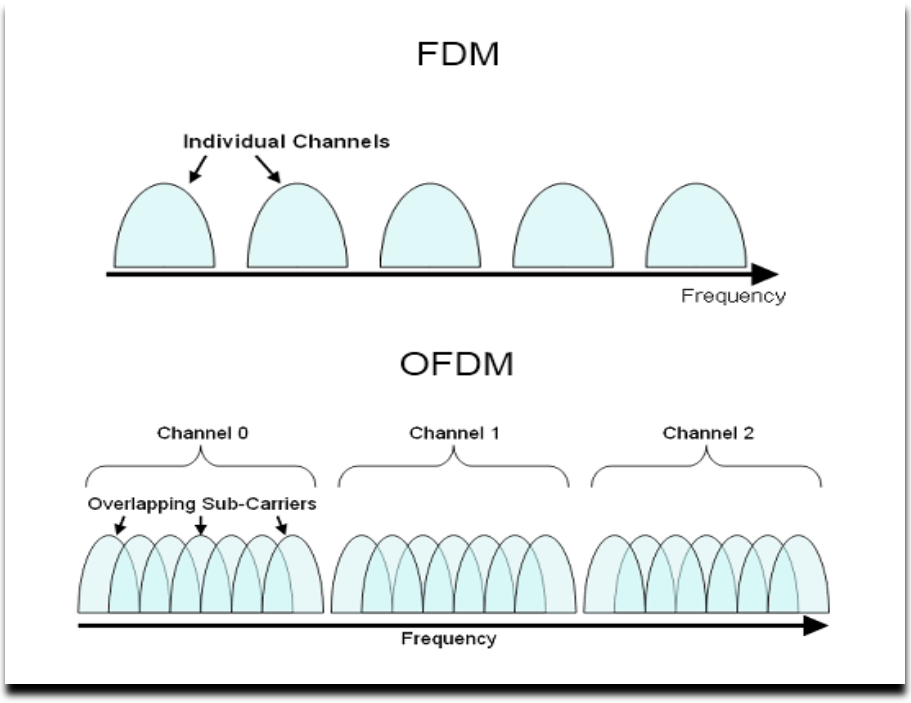


Figure 6. A diagram illustrating the conventional FDM and OFDM techniques

The physical layer of the WiMAX is based on the OFDM to meet the requirements for the flow of different type of IP packets traversing across it. The physical layer comprises of a combination of hardware and software programming techniques to define transmission technology of a network. (Wireless Cafe, 2013)

4. Proposed Network Study and Layout

WiMAX is a technology that supports the deployment of multiple network services in a singular platform. Especially due to its support for VoIP services in an efficient and effective manner, it has the potential to be an alternative choice to existing telephony techniques. Easy deployment and wireless existence make it inexpensive to operate and maintain. Advance QoS and security features ensure the flow-priority and security of data packets at the same time.

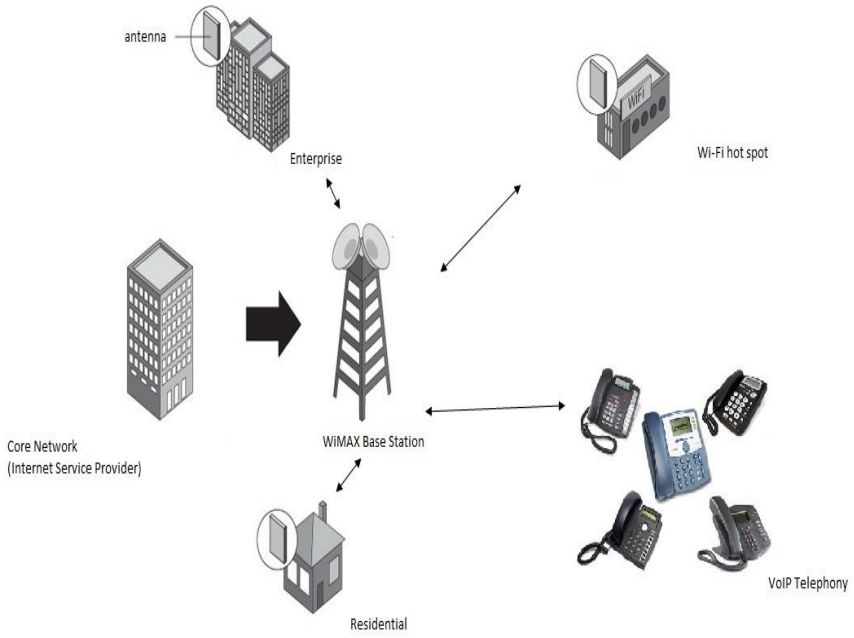


Figure 7. A prototype WiMAX network consisting of several components.

As depicted in Figure 7, a network system comprises of several, but essential components, that maintain the overall functionality of the network as different types of traffic with different priority level traverses across the network. Figure 7 shows the same WiMAX base station being used for wireless broadband internet distribution for home and enterprises, along with Wi-Fi hotspot and telephony services.

Prompt technological advancements are being introduced in the field of WiMAX development, so as to improve the efficiency of the technology. But, as we simplify the network, to form a basic level of understanding about the operational endeavor of the network, a WiMAX network basically comprises of BS and SS.

4.1 Base Station

Base Station, or BS in short, is a unit in the formation of a WiMAX network, comprised of radio transmitters and receivers. The primary function of the BS is to provide the Mobile Station (MS) with wireless signals in order to give the network access to the end users. A typical base station consists of a tower equipped with internal devices to broadcast WiMAX signals. The internal devices in the BS comprises of WiMAX radios and antennas.

4.1.1 WiMAX radio

WiMAX radio forms the core of the WiMAX network, since it is responsible for the wireless transmission of signals, an inevitable process in the formation of an operational network. A WiMAX radio contains both transmitters and receivers to send and receive wireless signals, generating electrical oscillations at a frequency, also known as carrier frequency, the value of which is usually between 2 – 11 GHz in WiMAX. In a sense, the WiMAX radio can be compared to networking devices like wireless routers or bridges, due to the fact that it comprises of circuit boards with complex chipset and is software controlled.

Figure 8. A WiMAX radio placed inside an enclosure box for safety.

4.1.2 Antennas

Antennas are devices that send and receive radio signals. Similar to their common usage, Antennas, in WiMAX are used as a signal enhancement aid to the WiMAX radios. There are three main types of antennas that are used in WiMAX deployment.

1. Omni directional antenna

Omni-directional antennas are generally used in network with Point to Multipoint configuration, and they broadcast wireless signals in a certain range making an angle of 360 degrees from the base station. Omni-directional antennas are useful in the scenario where the subscribers are located in a close range with the base station.

Figure 9. Omni directiona antenna.

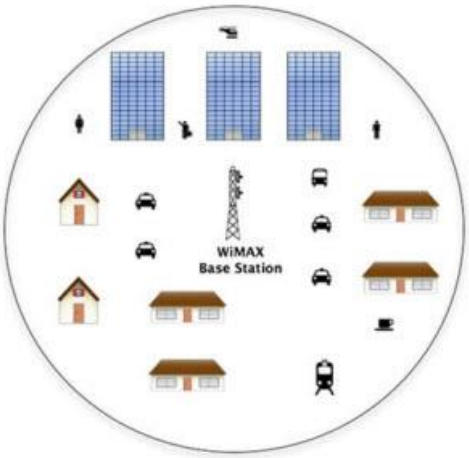


Figure 10. Coverage area of an omnidirectional antenna as shown inside the circle.

2. Sector Antenna

As the name suggests, these antennas are used to broadcast signals over a certain sector making an angle of certain degrees with the base station, usually 60, 90, and 120 degrees. Sector antennas focus on a specific zone, thus offering great coverage range and strong signal strength with less energy throughput.

Figure 11. A sector antenna

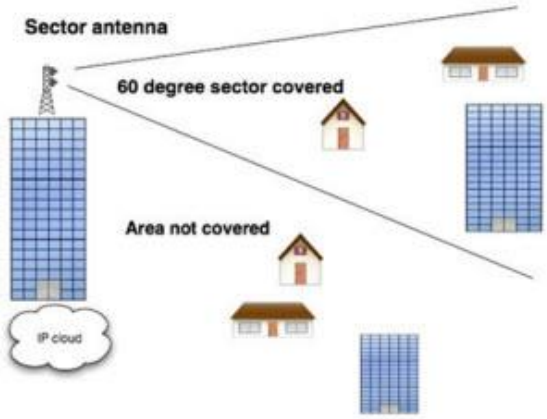


Figure 12. Coverage area of sector antenna shown inside the angular area formed.

3. Panel Antenna

Panel antennas are used to broadcast signals in one specific direction, and are usually used for point to point configurations. Due to their unidirectional broadcasting, panel antennas offer a better signal strength and a greater coverage. Panel antennas are shaped like a flat square panel and are usually attached to a mounting bracket. They can be used both indoors and outdoors.

Figure 13. A mounted panel Antenna

4.2 Subscriber Station (SS)

In its most basic form, a SS, a technical term used for CPE, is a device that enables a subscriber to gain access to a WiMAX network. The SS receives the signal given away by the BS, and after a few basic procedures involving calibration and authorization, it gives network access to the subscribers. Based on the generally accepted marketing concept, SSs can be classified into indoor and outdoor SSs. An Indoor SS is a device that is installed inside the premises to receive the signal being broadcasted by the BS. An outdoor SS is a device that is installed outside of the premises, usually on the rooftop to recieve the signal given by the BS.

(WiMAX, 2013)

4.3 Network Working Mechanism

There is a number of procedures that needs to take place for a successful WiMAX transmission. The diagram below shows all the procedures in an ascending order of their occurrence.

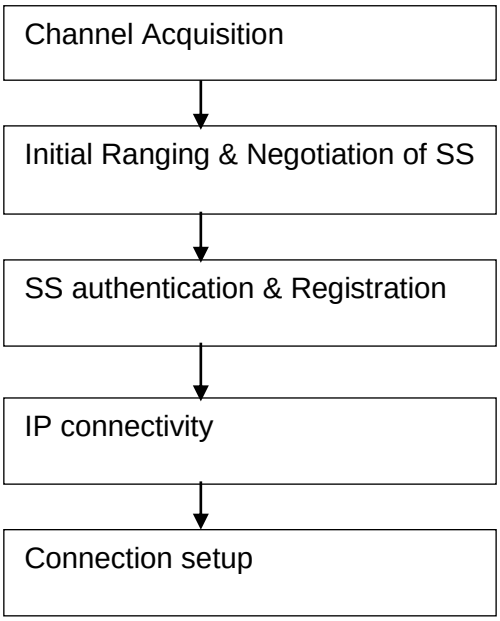


Figure 14. Working Mechanism of WiMAX on ascending order.

Channel Acquisition

Channel acquisition is the primary step when the subscriber station (SS) is powered up and given an interface to connect to Ethernet, for example. After the initial setup of the SS, the SS starts to scan its frequency lists to determine and obtain an operating channel to connect to a BS which is generally preconfigured by the service provider to overcome the obstacles that may arise if done manually. The SS then selects a BS based upon the signal strength in case there are multiple BSs to select from. Upon the completion of the process, the SS synchronizes to the downlink transmission (DL), which is the transmission path from the BS, to the SS. Once the synchronization takes place, the SS determines the modulation and Forward Error Correction (FEC) scheme, a technique to control data transmission error over wireless platform, based on the BS configuration.

Initial Ranging & Negotiation of SS

In wireless communications, when more than one station or node tries to maintain connectivity by accessing the same wireless channel at the same time, a packet collision occurs. It repeats if the nodes try to access the channel again since a timely synchronization is maintained between nodes. In order to avoid the packet collision between two nodes, both nodes choose a random waiting time before attempting to maintain connectivity again. In case this attempt is not successful, the nodes double their contention window and chose another random time before the re-attempt. The feature that enables this process is called backoff algorithm. Using backoff algorithm, the SS determines the initial ranging slot to send a ranging request message. After the channel acquisition and the uplink-MAP (UL-MAP) scanning is completed. To provide the SS with basic and primary management CIDs (Connection Identifiers), BS adjusts the timing advance and power to the SS with ranging response (RNG-RSP), determined as the result of the burst sent by SS using the minimum power setting in the beginning. Higher power setting is applied in case no response is received from the BS. Thus, the initial ranging and negotiation of SS occurs.

SS authentication & Registration

In WiMAX network, each SS contains manufacturer-issued and installed x.509 digital and certificates of the manufacturer. A digital certificate is a set of cryptographic processes to encrypt and protect the data from unauthorized access. The data is encrypted using a second data record known as a ‘key’. The key is applied in such a way that it produces an altered data record from the user data, using a mathematical process so as to prevent the original content from being identified. The key always occurs in a pair of private and public keys for encryption and decryption purposes. During the authentication and registration process of SS with the BS, these digital certificates are included in the authorization request and authentication information sent by the SS, thus creating a link between the 48-bit mac address of the SS and its public RSA key, to the BS. Using these certificates, the identity of the SS can be verified by the network as well as checking the authorization level of the SS. Provided that the SS has the authority to join the network, the BS will send an authorization reply containing an authorization key (AK) encrypted with the public key that SS contains and proceeds to secure further transactions, and finally registering with the with the network if followed by a successful authorization.

IP connectivity

After a successful authorization with the BS, the SS gets an IP address from the network via a DHCP server and establishes the time of the day using internet time protocol. To configure the SS, based on the vendor-specific configuration information in an automatic manner, the DHCP also provides the SS with the address of the TFTP server for configuration file download.

Connection Setup

After the connectivity has been ensured, and when the network is ready for an actual data transmission, WiMAX uses a concept of service flow, based on QoS parameters to define one –way transport of packet related to, either DL or UL. QoS is a network feature responsible for allocating bandwidth to a network application, based on the priority. For example, more bandwidth is allocated to the services where latency and jitters are unfavorable. In order to ensure an efficient utilization of vital network resources like bandwidth and memory, WiMAX adopts a two-phase activation in which the resources allocated to particular network services may not be activated unless asked for. Each service running in WiMAX network is assigned a unique CID mapped to a MAC connection, making it easier to identify and optimize the type of service flow.

(Ohrtman, 2013)

5. **QoS in WiMAX**

QoS enables the ability of network to transport different types of data with varying priority level. QoS minimizes the effect of factors like latency and jitter that causes the network traffic congestion. The basic functionality of QoS is to classify the type of the service flow on the network and allocate the right amount of bandwidth according to the priority level of the service flow. QoS carries a great deal of importance, as it performs the scheduling mechanism of the service flow in the network, especially when the network involves the real-time services, like VoIP, which require high precision. QoS in WiMAX comprises of five classes, that are activated depending on the type of type of application running across the network. The elements responsible for the maintenance of QoS in WiMAX are listed below.

5.1 Unsolicited Grant Service (UGS)

It is a type of QoS class that aids the applications that need a Constant Bit Rate (CBR), like a leased line circuit emulation (T1 and E1). UGS supports real-time service flow in which fixed-size packets are generated over a certain amount of time. When UGS is in progress, the BS grants fixed-sized data packets at a periodic interval.

5.2 Real-time Polling Services (rtPS)

It is a type of QoS class that aids the applications with a real-time service flow, generating variable sized data packets over a period of time. Its functions are similar to that of UGS, except that when rtPS grants dynamic distribution, while UGS grants fixed-size data packets. Applications like tele-conferences, MPEG video streaming uses rtPS services.

5.3 Extended real time Packet Services (ertPS)

It is a type of a QoS class that contains the features of both UGS and rtPS, and aids in the operation of real-time applications generating variable-sized data rates. Applications like VoIP with silence suppression use this service.

5.4 Non-real time Polling Services (nrtPS)

It is a type of QoS class that provides its services to the applications that require no real-time services with minimum data rates required for variably-sized data packets. Its primary function is the delay management in the service flow and is used by FTP.

5.5 Best Effort (BE)

It is a type of QoS class that causes long delays in case of network traffic congestion since it lacks the support for applications requiring minimum service guarantees. Applications like E-mail services and internet-browsing services where delay is not of that much significance use this service.

(Elgered, Moghaddam and Vedder, 2013)

6 Integrating VoIP in WiMAX

An important aspect of WiMAX is its capability to support the flow of voice traffic in its network. Due to its relatively faster speed and easy deployment, a WiMAX network can be considered as an efficient and alternate platform to deploy VoIP services to facilitate the subscribers with telephony services. VoIP is a set of protocols that enables a user to initiate the telephony services, voice transmissions and other multimedia sessions over the IP network. VoIP services are being offered by a several companies today for a certain amount of charge, but the technology is not yet as popular and as common as it could have been. To use VoIP services, a subscriber basically needs a communicating device with an internet connection. The subscriber logins to the VoIP server of the service provider using the credentials required for authorization, and once logged in, can start using the services. A stable and high speed internet connection is inevitable and works as a backbone while accessing VoIP services. Nevertheless, the availability of mobile internet might not always be available. VoIP services can be accessed through wire technology like DSL and ADSL, but the major drawback is that, since they are wire technologies, it is rather difficult to maintain mobility. Wi-Fi is an alternate, but being a LAN technology, the range it covers is much lower compared to WiMAX, and it is generally expensive to subscribe to 3G internet. On the other hand, WiMAX, being a technology based on WMAN, covers a much larger coverage area and has a higher connection speed compared to that of Wi-Fi. Based on these factors, WiMAX can be indubitably considered as an efficient platform to deploy VoIP services.

The working mechanism of VoIP is pretty much similar to the transmission of normal datapackets using Internet Protocol, except that the process has to go through processes to convert the analog voice to digital packet to make it able to traverse across the network. The processes include the digitization of voice, isolation of unwanted noise, and, finally, the compression of the voice using compression codecs. After the completion of the aforementioned processes, the voice is ready to be sent over an IP network in packets, similar to data packets in data transmission. Each packet, in order to traverse across the network, needs a destination address as well as a sequence number and data for error checking to preserve accuracy throughout the transmission, and that is where the term 'signaling protocols' comes into effect. Signaling protocols, in their most basic sense of operation, are responsible for setting up and ending calls, carrying information required locating users and capabilities negotiation. There are several signaling standards for VoIP,

on the basis of which VoIP carry out operations. Some of the popular VoIP signaling standards are as follows:

1. H.323

H.323 is the International Telecommunications Union (ITU-T) recommended signaling protocol for packet-based multimedia communication.The first version was published in November 1996, and was originally developed for multimedia conferencing over LAN, but was later modified to support VoIP, too. It is an interoperable standard and supports both point-to-point and multipoint capabilities. It has sub protocols like H.255.0 and H.245 used for various functions like registration, call signaling, and terminal capability exchange.

2. SIP

SIP is an Internet Engineering Task Force (IETF) defined signaling protocol, and uses a text-based syntax similar to HTTP, used in web addresses. It is compatible with PSTN phone numbers for PSTN interfacing. Alike H.323, SIP maintains the setup, tear down, and modification of multimedia sessions, voice included. In a SIP network, a web address is comparable to a telephone number.

3. MGCP

Media Gateway Control Protocol (MGCP) controls the gateway functions such converting digital media streams between different networks like PSTN, 2G, and 3G.

4. MEGACO/H.248

Megaco is an enhanced version of MGCP.

(Maneesh, 2013 **)**

6.1 Soft switching

Soft switching is a technology that enables the routing of data and voice via IP-based networks, independent of the location of the network resources, as long as the connectivity is maintained. The traditional switched network, PSTN, for example, relies entirely on the inter-connectedness of the communications hardware located on dedicated facilities, primarily designed to serve the purpose of voice communications. Unlike the operating mechanism of the circuit switched network, soft switching is based on the concept of the separation of the network hardware from the network software. In soft switching, several network protocols function in a soft switch device to perform tasks like call control, signaling, and many other features that enable telephony services as well as other multimedia services across possible networks. Apart from that, soft switching also performs administrative tasks like billing statistics along with other value added services, and it is also interoperable with circuit switching technology.

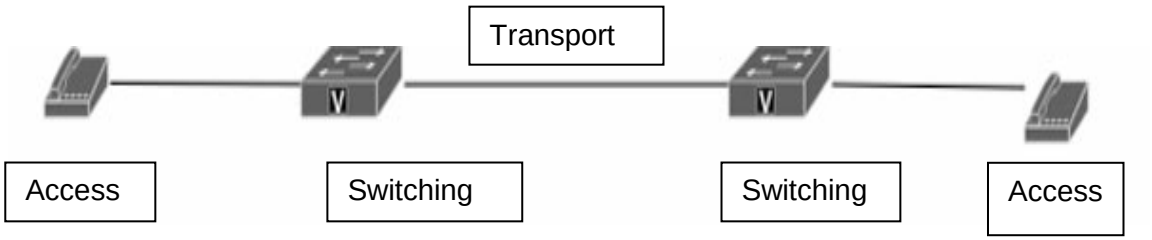


Figure. 14 PSTN switching showing the traditional way of communication.

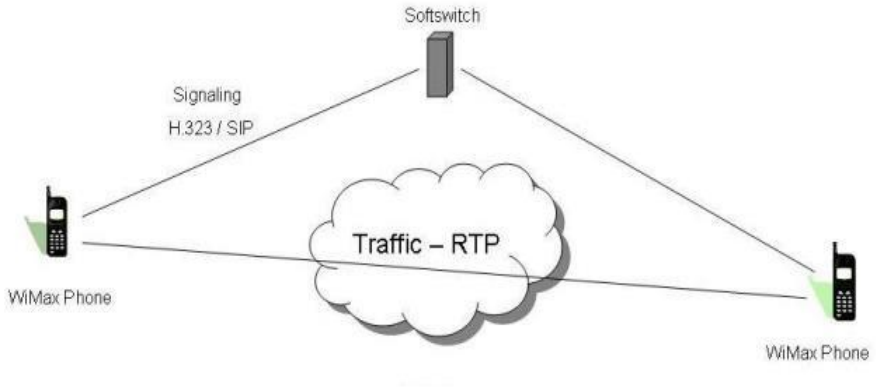


Figure 15. Soft switching showing the flowing of RTP traffic between two WiMAX phones.

With reference to Figure 15, the working mechanism of soft switching can be clearly understood. The central component involved in soft switching is a device called Soft switch whose main responsibility is to maintain IP telephony and other multimedia services, using its features. As seen in Figure 16, the Real-time Transport Protocol (RTP) traffic between two WiMAX enabled phones is handled by a soft switch using signaling protocols like SIP and H.323. The greatest advantage of using soft switching technology is that the entire communication operation is supervised by a single computer software system, thus a timely software upgrade is possible to ensure the better system performance.
(Ohrtman, 2013)

There are several components that make a soft switching system operable which are listed as follows:

1. Signaling gateway:

It is a device that enables the connectivity between different networks with different signaling techniques by using standardized signaling protocols to resolve signaling differences. For example, a signaling gateway is used to maintain connectivity between PSTN and VoIP networks. A signaling gateway uses protocols like SS7, C7, and C5.

2. Media gateway

A media gateway is a device that turns an analog voice stream to a packetized one, and contains at least one pair of conventional telephone port and an Ethernet port.

3. Application server

The Application server is configured with all the parameters and features that a service provider intends to provide its customers with. The features may include services like call forwarding, voice mail, billing services and so on. The softswitch access the application server and provides the required services to the subscribers as needed.

(Maneesh, 2013)

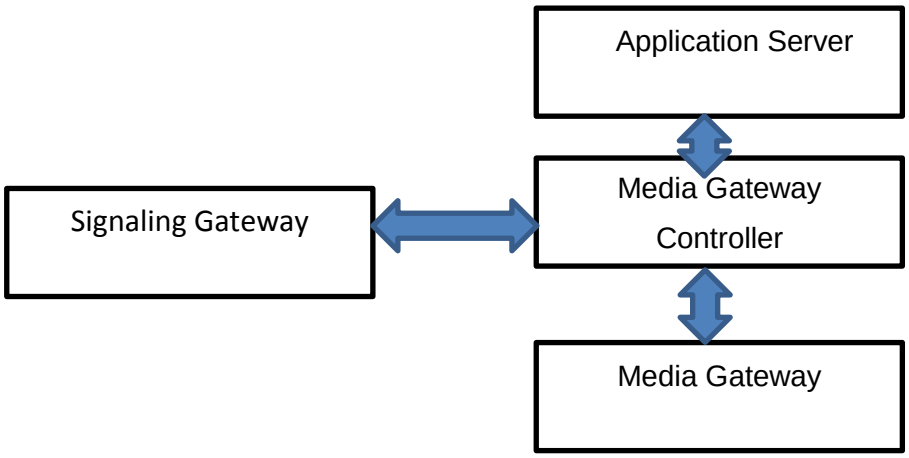


Figure 16. Interconnectedness of several components in soft switching.

7 Security in WiMAX

Security is an essential factor in any type of network. A secure network always leads to efficiency and reliability. A large amount of data traverses across the network at any given time, and those data could be of any kind, ranging from normal e-mail message to highly confidential documents. The primary purpose of security policies is to safeguard those data by preventing the unauthorized access to the network resources and preventing the network breaches. WiMAX, based on IEEE 802.16 architecture, has its own set of security protocols to ensure the security of the network against hackers and breaching to prevent the theft, misuse, and manipulation of data traversing across the network.

WiMAX security architecture is made up of five components:

7.1 Security Associations

Security Associations (SA), based on its primary parameters, is a set of protocols that a WiMAX BS and SS share in order to maintain a secure connection between the two. SA operates at the MAC layer, and has two types- namely data SA and authorization SA. Between these two, only data SA is explicitly defined by IEEE 802.16 and consists of a 16-bit SA identifier, two 2-bit TEK, an initialization vector for each key and a TEK lifetime with a minimum value of 30 minute and a maximum value of 7 days. Whereas the authorization SA consists of X.509 certificate for the SS identification, a 160-bit secret AK, an AK lifetime ranging from one to seven days, a key encryption key (KEK), and a downlink and uplink based HMAC providing the data authenticity of key distribution messages between the BS and SS.

7.2 Certificate profile

As already discussed before, regarding the use of X.509 digital certificates during the authentication and registration process of the SS with the BS. X.509, digital certificates are required to contain X.509 version 3 digital certificate, a serial number, Issuer's signature, validity period, MAC address and signature algorithm, identical to the issuer's signature algorithm.

7.3 Privacy and key management (PKM) authorization

After the SS is registered and authorized to join the network, PKM initiates the distribution of an authorization key (AK) to that SS in a process that involves the exchange of three messages between the SS and the BS. First, the SS sends the BS its x.509 certificate issued by the manufacturer to ensure its authenticity. After that, the SS sends another message immediately, consisting of SS's certificate, capabilities and SA identification, and using these values, the BS verify the authorization of the SS. Finally, the BS verifies the SS' authority, the BS responds with the message 3, thus creating an SA between the two stations. The correct use of the AK that PKM distributes verifies the authority to use the wireless channel by the nodes.

7.4 Privacy and key management

Once connected to the network, the SS can establish a data SA with the BS using the PKM protocol, similar to that of the PKM authorization. The process involves the exchange of two or three messages that involve the usage of several authorization entities like HMAC, SAID, and TEK to verify the data authenticity and to allow the BS to detect forgeries.

7.5 Encryption

By default, WiMAX supports the DES-CBC encryption method. DES-CBC stands for Data Encryption Standard – Cipher Block Chaining, meaning that an encryption standard is operated in a cipher block chaining mode. DES has a block size of 64-bits and uses 56-bits for execution, and when used, both the sender and the receiver must use the same secret key to encrypt and decrypt the data whereas Cipher Block Chaining is a mode of operation, which uses an initialization Vector (IV) to encrypt a sequence of bits as a single unit, or a block using a cipher key. CBC supports the encryption of the blocks less than 64-bits in size.

(El-Gammal, 2013)

8. WiMAX limitations

Being deployed as a wireless technology, WiMAX has its own set of limitations that affect its performance under certain conditions. Listed are some of the major WiMAX drawbacks.

WiMAX is capable of reaching a comparatively long distance up to 70 Km, and a high bit rate of 70 Mbps. But, as the distance continues farther, a decrease in the bit rate will occur. So, in order to achieve the optimum bit rate, a subscriber needs to maintain a close distance with the tower.

There are always more than one subscriber using all existing wireless technologies, and the bandwidth is shared between users in a particular radio sector. Therefore, there is always a probability of the network functionality slowing down due to the existence of multiple subscribers, and more radio cards are required in the base station to boost up the network capabilities.

Setting up a Wi-Fi network is easy and inexpensive, compared to that of WiMAX, and also, WiMAX requires a frequency license, while being set up in a region.

Because of its features like low bit rate over long distance, and sharing of bandwidth among users, granular and dispersed network architectures are not being supported into WiMAX during autonomous progress. (Ramos & Serrano, 2011)

9. Conclusion

WiMAX, due to its support for the multiple traffic types and wireless implementation, is indubitably a great choice of technology to adopt for a network. Since different network related applications require varying bandwidth and priorities, WiMAX is capable of sorting that out and allocating the amount of bandwidth required by an application depending upon its activeness, or in other words, it provides a service with an assured QoS. The thesis studied and discussed a WiMAX based network that would work as a singular platform for voice, video and data traffic with all the security measures adopted as well as an assured QoS.

Deployment in both fixed and mobile state further extends the scope of WiMAX, making it possible to access high speed wireless broadband services both at home and on the go, with roaming services due to its OFDM techniques.

The thesis explicated the basics of wireless technology in a simple manner. Different aspects regarding the deployment and usage of WiMAX network, like infrastructures, broadband access, VoIP support, QoS and security measures have been tried to be made as elaborative and as simple as possible. The thesis also provided a general information regarding WiMAX as a VoIP platform, in particular. Since WiMAX is an emerging technology, gathering resources was a challenging task, but the internet blogs were helpful enough to provide with required information and resources.

REFERENCES

El-Gammal, 2013. Retrieved February 13, 2013, from

http://www.cs.washington.edu/education/courses/csep590/06wi/finalprojects/el-gammal.doc

Elgered, Moghaddam and Vedder. Retrieved Februrary 16, 2013 from

http://www.mehrpouyan.info/Projects/Group%2010.pdf

IEEE 802.16 Wireless Metropolitan Area Network. Retrieved January 20, 2013 from

http://www.hadassah.ac.il/CS/staff/martin/Wireless/slide05.pdf

Maneesh, 2013. Retrieved February 6, 2013, from

http://www.cse.wustl.edu/~jain/cse574-06/ftp/wimax_voip/index.html

Marshall and Grabianowski. Retrieved December 6, 2012, from

http://computer.howstuffworks.com/wimax1.htm

Ohrtman, 2013. Retrieved January 11, 2013 from

http://maiden.verat.net/pub/MCGraw-Hill%20Osborne%20WiMAX%20Handbook%20Building%20802.16%20Wireless%20Networks.pdf

Ramos & Serrano. Retrieved February 20, 2013, from

http://net.infocom.uniroma1.it/corsi/Network%20Infrastructures/lucidi/VoIP_over_WiMax.pdf

SearchEnterpriseWAN. Retrieved January 15, 2013 from

http://searchenterprisewan.techtarget.com/definition/wireless-WAN

SearchMobileComputing. Retrieved January 16, 2013 from

http://searchmobilecomputing.techtarget.com/definition/WPAN

Types of Wireless Networks. Retrieved January 16, 2013 from

http://computernetworkingnotes.com/wireless-networking-on-cisco-router/types-of-wireless-networks.html

WiMAX, 2013. Retrieved February 17, 2013 from

http://www.wimax.com/table/wimax-tutorial/

wireless café. Retrieved February 20, 2013 from

http://wirelesscafe.wordpress.com/2008/03/26/what-is-ofdm-and-its-wireless-applications/

WLAN Best Practices Guide. Retrieved January 17, 2013 from

http://education.alberta.ca/media/6607528/wireless%20guide%202011%20publication%20edition.pdf