Abstract— the explosive growth of the Internet from last few years has led to an increasing demand of high speed, everywhere Internet access. Broadband Wireless technologies are increasingly gaining popularity by the successful global deployment of the Some technology like as Wireless Personal Area Networks (Bluetooth- IEEE 802.15.1), Wireless Local Area Networks (WiFi- IEEE 802.11n), and Wireless Metropolitan Area Networks (WiMAX IEEE 802.16). WiMAX (Worldwide Interoperability for Microwave Access)/ IEEE 802.16 is a very promising and latest 4G technology. WiMAX is now in the testing via implementation stage at various locations like Taiwan [1], India [2]. The main target of these technologies provides low-cost, high-performance Wireless access to residential and business applications. As technology evolves to address portable and mobile applications, the required features and performance of the system will increase.

Recently, WiMAX and WiFi have been proposed as attractive wireless communication technologies for providing broadband access for metropolitan areas. This paper presents a study of the basic concept of the WiFi and WiMAX technologies.

Keywords— WiMAX.
(Wireless Fidelity)-IEEE 802.11n, and part-V explores how WiMAX works and function of WiMAX, part VI, describe how emerging Wireless technologies differ from one another and conclusions are drawn in section VII.

II- Integrated WiMAX-WiFi Network

Figure 1 shows the integrated WiFi and WiMAX network, it consist typical WiMAX and WiFi network components. The original aspect in this integrated network is that we created and develop the logical component of WiFi Gateway in this architecture, which makes WiFi and WiMAX become architecturally consistent.

![Figure 1: Integrated WiMAX-WiFi network](image)

The integration of WiFi and WiMAX happens in both network access network and core service network. In the core service network, common network servers (AAA, DHCP, and HA) are used for both WiFi and WiMAX. An AAA server is responsible for authenticating and authorizing the network access of a client, a Home Agent (HA) serves a user client when it roams from WiFi to WiMAX or vice versa, and a DHCP server works to provide IP addresses to a client device at the beginning of a network access or in a handoff operation from one network to another. In access network layer, both WiMAX Gateway and WiFi Gateway play the same role in connecting a wireless client device to the backend IP network.

III - WiMAX-WiFi Hybrid Network

The hybrid network is shown in Fig. 2. There are several AP hotpots providing WiFi access and the WiMAX BS is a significant complement to covering the laps between different APs. A fast pre-authentication architecture is proposed in WiFi-WiMAX hybrid networks in order to reduce the authentication delay. The proposed scheme is divided into two phases: pre-authentication and re-authentication. The pre-authentication phase is completed in the user's network initiation stage. And the re-authentication is executed after handover. Without loss of generality, the EAP-TLS method is considered in both WiFi and WiMAX authentication.
A comparative study of Technical aspect of WiMAX & WiFi Networks Technology

IV- WiFi (Wireless Fidelity)-IEEE 802.11n

WiFi is a brand originally licensed by the WiFi alliance to describe the underlying technology of Wireless Local Area Networks (WLAN) based on the IEEE 802.11 specifications. It was developed to be used for mobile computing devices, such as laptops, in LANs, but is now increasingly used for more services, including Internet and VOIP phone access. WiFi technology is most commonly found in notebook computers and Internet access devices such as routers and DSL or cable modems. WiFi is helping to extend the technology beyond the PC and into consumer electronics applications like Internet telephony, music streaming, gaming, and even photo viewing and in-home video transmission. These new uses, as well as the growing number of conventional WLAN users, increasingly combine to strain existing WiFi networks [9] [10]. The next WiFi speed standard, 802.11n, will likely offer a bandwidth of around 108Mbps.

A- Range Feasibility for WiFi

Each access point in WiFi has a finite range within which a Wireless connection can be maintained between the client computer and the access point.

Typical indoor ranges are 150-300 feet. But can be shorter if the building construction interferes with radio transmissions. Longer ranges are possible; but performance will degrade with distance. Outdoor ranges are quoted up to 1000 feet. But again this depends upon the environment conditions.

B- Devices requirements for WiFi technology

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Requirement for WiFi technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Laptop/Desktop/PDA</td>
</tr>
<tr>
<td>2.</td>
<td>802.11a Adapter for Desktop/Laptop</td>
</tr>
<tr>
<td>3.</td>
<td>802.11b Adapter Desktop/Laptop</td>
</tr>
<tr>
<td>4.</td>
<td>802.11g Adapter Desktop/Laptop</td>
</tr>
<tr>
<td>5.</td>
<td>802.11a/b/g Access Point (Indoor)</td>
</tr>
<tr>
<td>6.</td>
<td>802.11a/b/g Access Point (Outdoor)</td>
</tr>
<tr>
<td>7.</td>
<td>802.11a/b/g Wireless Switch</td>
</tr>
<tr>
<td>8.</td>
<td>802.11a/b/g Dongle USB Port</td>
</tr>
<tr>
<td>9.</td>
<td>Wireless Media Player</td>
</tr>
<tr>
<td>10.</td>
<td>Wireless Gateway</td>
</tr>
<tr>
<td>11.</td>
<td>Antenna Indoor and Antenna Outdoor</td>
</tr>
<tr>
<td>12.</td>
<td>Wireless Bridge</td>
</tr>
<tr>
<td>13.</td>
<td>Wireless Camera</td>
</tr>
<tr>
<td>14.</td>
<td>Range Booster</td>
</tr>
</tbody>
</table>

C- Existing Use of WiFi

i- A person with a WiFi enabled device such as a computer, cell phone or PDA can connect to the Internet when in proximity of an access point.

ii- WiFi can also be used to create a mesh network.

iii- WiFi also allows connectivity in peer-to-peer (Wireless Adhoc network) mode, which enables devices to connect directly with each other.

iv- WiFi devices are often used in home or consumer-type environments in the following manner: Termination of a broadband connection into a single router, which services both wired and Wireless clients, ad-hoc mode for client-to-client connections, built into non-computer devices to enable simple Wireless connectivity to other devices or the Internet.

v- Outdoor applications utilizing true mesh topologies, a proactive, self-managed network that functions as a security gateway, firewall, DHCP server, intrusion detection system, and a myriad of other features not previously considered relevant to a Wireless network.
D- Use of Standard Devices in WiFi

1- Wireless Access Point (WAP)
A Wireless access point connects a group of Wireless devices to an adjacent wired LAN. An access point is similar to an Ethernet hub, relaying data between connected Wireless devices in addition to a (usually) single connected wired device, and most often an Ethernet hub or switch, allowing Wireless devices to communicate with other wired devices.

2- Wireless Adapter
A Wireless adapter allows a device to connect to a Wireless network. These adapters connect to devices using various interconnects such as PCI, USB, and PCMCIA.

3- Wireless Router
A Wireless router integrates a Wireless Active Protocol (WAP, Ethernet switch, and internal Router firmware application that provides IP Routing. The DNS forwarding through an integrated WAN interface.
A Wireless router allows all three devices (mainly the access point and router) to be configured through one central utility. This utility is most usually an integrated web server which serves web pages to wired and Wireless LAN clients and often optionally to WAN clients. This utility may also be an application that is run on a desktop computer such as Apple’s airport.

4- Wireless Ethernet Bridge
A Wireless Ethernet bridge connects a wired network to a Wireless network. This is different from an access point in the sense that an access point connects Wireless devices to a wired network at the data-link layer. Two Wireless bridges may be used to connect two wired networks over a Wireless link.

5- Range Extender
A Wireless range extender or Wireless repeater can extend the range of an existing Wireless network. Range extenders can be strategically placed to extend a signal area or allow the signal area to reach around every corner of the building. Wireless devices connected through repeaters will suffer from an increased latency for each hop. Additionally, a Wireless device at the end of chain of Wireless repeaters will have a throughput that is limited by the weakest link within the repeater chain.

V- WiMAX
The development of IEEE 802.16 was started by the IEEE in 2001. After that it was revised several times and ended in the final standard IEEE 802.16-2004 which is often called Fixed WiMAX [11]. This standard defines Wireless Metropolitan Broadband access for stationary and nomadic use. This means end devices can not move between base stations (BS) but they can enter the network at different locations. This specification was extended by the development of IEEE 802.16e which is known as Mobile WiMAX [12]. This standard supports mobility so that mobile stations (MS) can handover between BS while communicating. On the link layer, Mobile WiMAX introduces new features like different handover types, power saving methods and multicast and broadcast support. Furthermore IEEE 802.16e eliminates most of the security vulnerabilities discovered in its predecessors [13].

A- Initial network entry procedure
For initial network entry, a MS has to pass some steps. The first step is to search for a downlink map message of the BS which is broadcasted periodically. This frame includes information about the initial ranging connection identifier (CID) which is associated with a timeslot in where the initial ranging process can be performed. Access to this common used timeslot is by standard random access channel. The MS then increases its transmission power with each ranging request it sends on the initial ranging slot until it receives a response from BS.

B- Key management:
In the 3-way TEK-exchange processed at initial network entry, the MS sets up a security association (SA) for each data communication it may wants to establish. Such a security association manages the keys for data encryption (TEKs), their lifetimes and other security related parameters of this connection. It also includes a TEK state machine which has the task to periodically refresh keying material when the lifetime of a TEK is going to expire. To prevent communication disruption each SA simultaneously holds two TEKs. When one TEK expires the second one is used for traffic encryption and a new one is requested [13].

C- Optional sleep mode:
To save stations battery capacity and reduce the load on the channel, an optional sleep mode was defined in Mobile WiMAX. It allows the MS to be absent from the serving BS for certain time periods and may power down its transmitter. Therefore IEEE 802.16e specifies three different sets of power saving classes. Services with common demand properties should be mapped to the same set of power saving class. However, an MS is able to execute all other processes like ranging or neighbor measurements which do not require a communication with the serving BS. When the BS receives data destined to a sleeping MS, this data is buffered and the MS is waked up with a broadcasted Traffic Indication message.

D- Multicast and Broadcast Service (MBS): IEEE 802.16e also introduces a service for Multicast and Broadcast communications. This enables the BS to distribute data simultaneously to multiple MSs. To secure the broadcast communications,
A comparative study of Technical aspect of WiMAX & WiFi Networks Technology

the IEEE 802.16e uses a common group traffic-encryption key (GTEK) for traffic encryption/decryption. Every group member must know this key. To share the GTEK between MS and BS, two algorithms are used: The mandatory key request/reply mechanism and the optional Multicast and Broadcast rekeying Algorithm E-(MBRA). In the standard request/reply mechanism a MS has to manage the GTEK update by itself. This means it has to request new keying material if the current key is going to expire. Such a key request triggers a unicast key response from the BS which includes a new key. To ensure an ongoing communication the MS simultaneously holds two keys similar to the TEK key management described above. An optional alternative to distribute keying material is the Multicast and Broadcast rekeying algorithm (MBRA).

F- Technical Information for WiMAX

WiMAX is a term coined to describe standard, interoperable implementations of IEEE 802.16 Wireless networks, in a rather similar way to WiFi being interoperable implementations of the IEEE 802.11 Wireless LAN standard. However, WiMAX is very different from WiFi in the way it works.

Table 4. Devices requirement for WiMAX

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Requirement for WiMAX technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>License for particular frequency 3.5GHz/5.8GHz</td>
</tr>
<tr>
<td>2</td>
<td>802.16 Adapter for Desktop/Laptop</td>
</tr>
<tr>
<td>3</td>
<td>Wireless Gateway and Wireless Bridge</td>
</tr>
<tr>
<td>4</td>
<td>Antenna Indoor and Antenna Outdoor</td>
</tr>
<tr>
<td>5</td>
<td>Laptop/Desktop</td>
</tr>
</tbody>
</table>

E-IEEE 802.16 PROTOCOL LAYER-
IEEE 802.16 WiMAX standard consists of a protocol stack with well-defined interfaces. The WiMAX protocol layer contains MAC layer and PHY layer. MAC layer includes three sub-layers shown in Figure 3: The Service Specific Convergence Sub-layer (MAC CS), the MAC Common Part Sub-layer (MAC CPS) and the Security Sub-layer or Privacy Sub-layer.

WiMAX security process is divided into three steps:
01. Authentication
02. Data Key exchange.
03. Data Encryption.

The PKM protocol uses, RSA public key algorithm, X.509 digital certificates, and strong encryption algorithm to carry out key exchanges between SS and BS [14]. This Privacy protocol has been enhanced to accommodate stronger cryptographic methods such as AES to fit into the IEEE 802.16 MAC [15].
The main objective of the privacy sub layer is to protect service providers against theft of service, rather than guarding network users. Privacy sub layer is above the physical layer, so it only guards data at the data link layer but does not protect physical layer from intercepted. It is necessary to include technologies to secure physical layer.

VI- Comparison of Wireless technologies

The use of Wireless technologies is beginning to appear similar to the initial development of the railways. Each technology seems to have a different “gauge” and compatibility issues seem to confuse the novice. The main points of comparison of the three technologies that have been discussed in this paper are listed in table 4.

![Table 4. Comparison of emerging Wireless technologies](image)

VII- Conclusion

This paper proposed an overview of Technical aspect for WiMAX & WiFi networks technology by focusing on the basic overview and architecture design. The WiMAX and WiFi will play equally important roles in the future of wireless networks. WiMAX is very important as it represents a whole new dimension of market opportunities. WiMAX is a promising wireless communication technology for wireless MANs. WiFi decreases cost of operation and deployment and opens new business opportunities in local area deployments. The robustness and effectiveness of end-to-end security approaches in WiMAX and WiFi will become clear only after deployment. Therefore it is easy to predict that WiFi and WiMAX are the mainstream technology for mobile broadband evolution.

WiMAX is not expected to completely eliminate the WiFi technology in the near future, but will be a complement to WiFi as its primary backhaul service of choice. WiMAX promises to help corporations expand business, drive down costs, increase overall profitability, increase the quality of service, and increase the number of users that connect to the Internet. Moreover, the mobile WiMAX technology is designed to provide high-quality, mobile broadband multimedia services; however, it presents challenges that operators need to consider before setting up their networks.
A comparative study of Technical aspect of WiMAX & WiFi Networks Technology

References


[4] WiMAX Forum: “Network Architecture Stage 2 and 3 - Release 1.0 (Revision 1.2)”


A comparative study of Technical aspect of WiMAX & WiFi Networks Technology


