Wireless and Mobile Networks

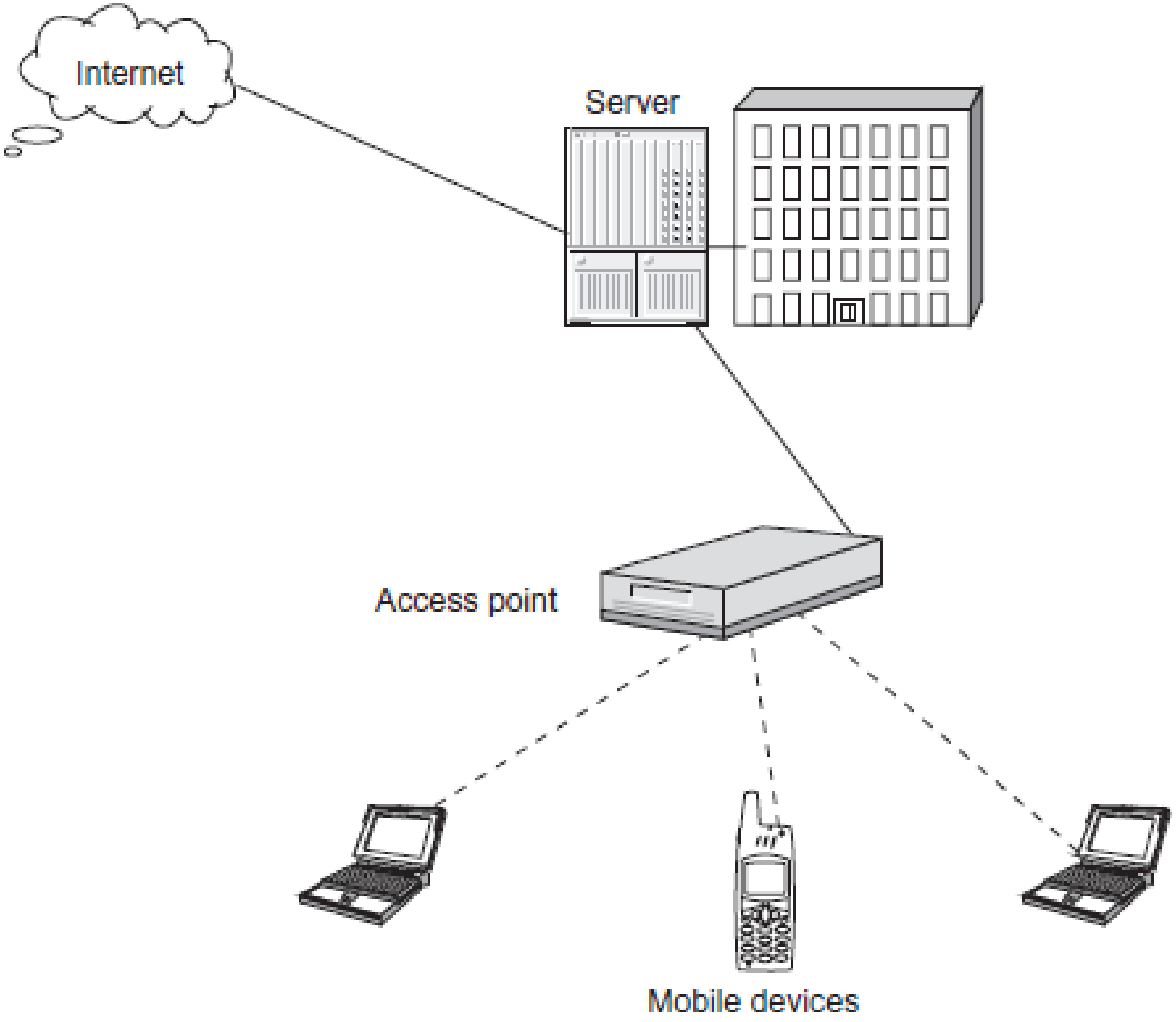
Dr./ Ahmed Mohamed Rabie

Chapter 1

Basics of Wireless Networks

Classification of Wireless Networks

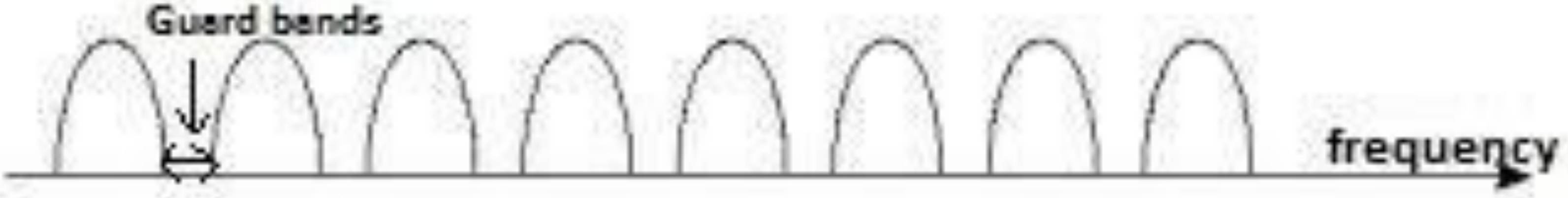
This group is called Wireless Local Area Networks (WLANs) and its signal range is approximately 30 m indoors and 100–200 m outdoors. The WLANs have come to be generally called the wireless fidelity (Wi-Fi or IEEE 802.11). WLAN is a wireless local area network, which is the linking of two or more computers without using wires in a building or a small campus.



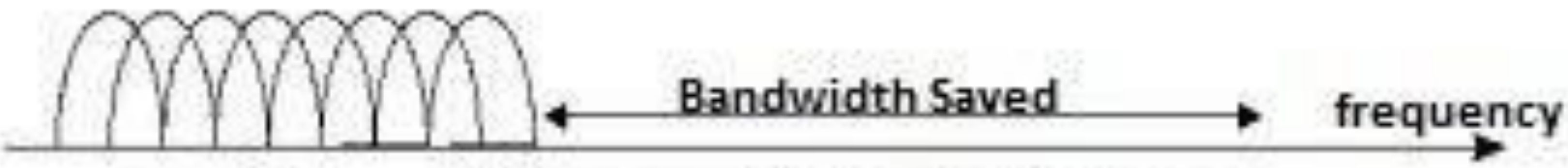
Wireless local area network scenario.

WLAN uses spread spectrum or orthogonal frequency-division multiplexing (OFDM) modulation technology based on radio waves to enable communication between devices in a limited area.

Wi-Fi is the most common used technology for WLANs. IEEE 802.11 is the Wi-Fi standard that denotes a set of WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).

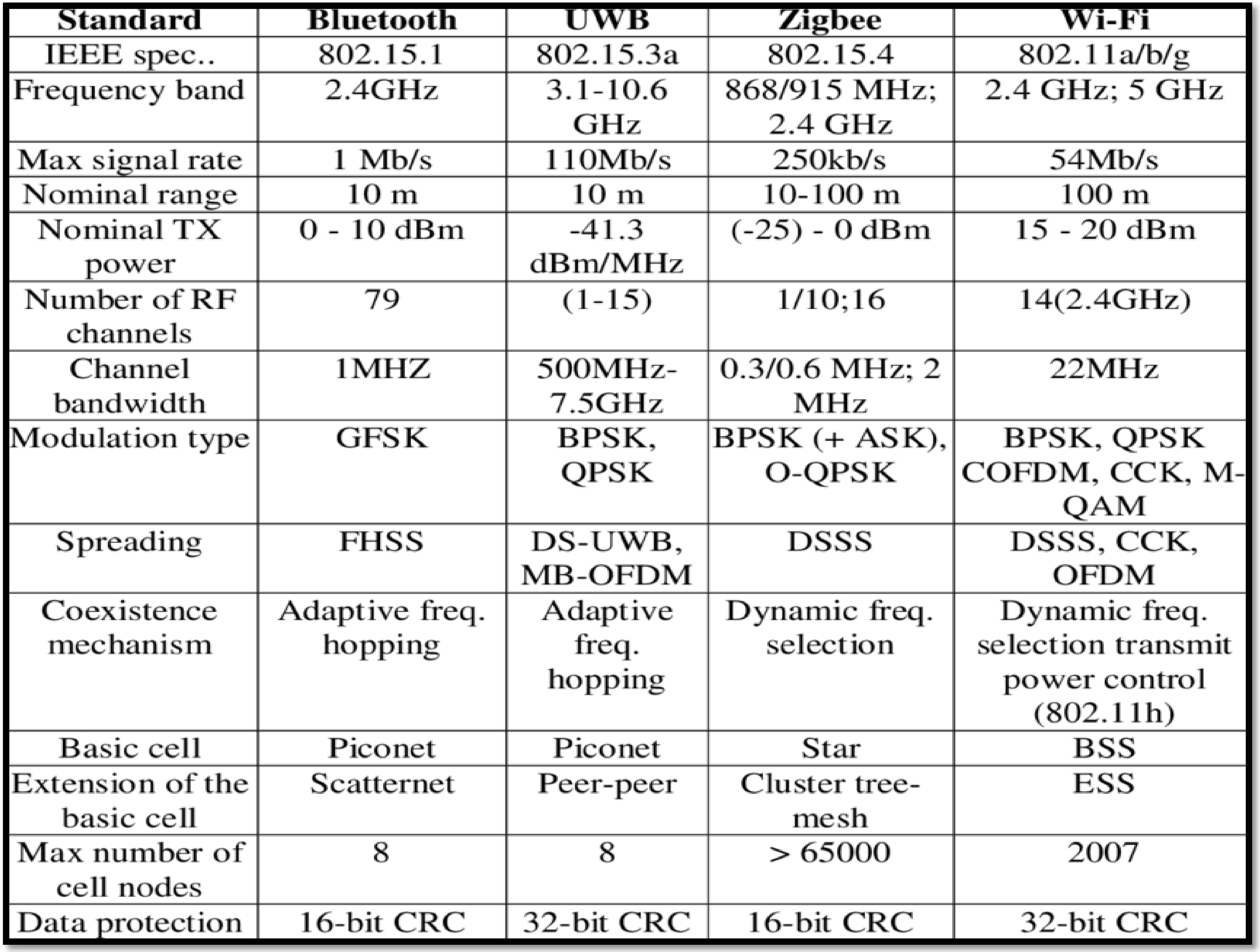


Conventional Frequency Division Multiplexing

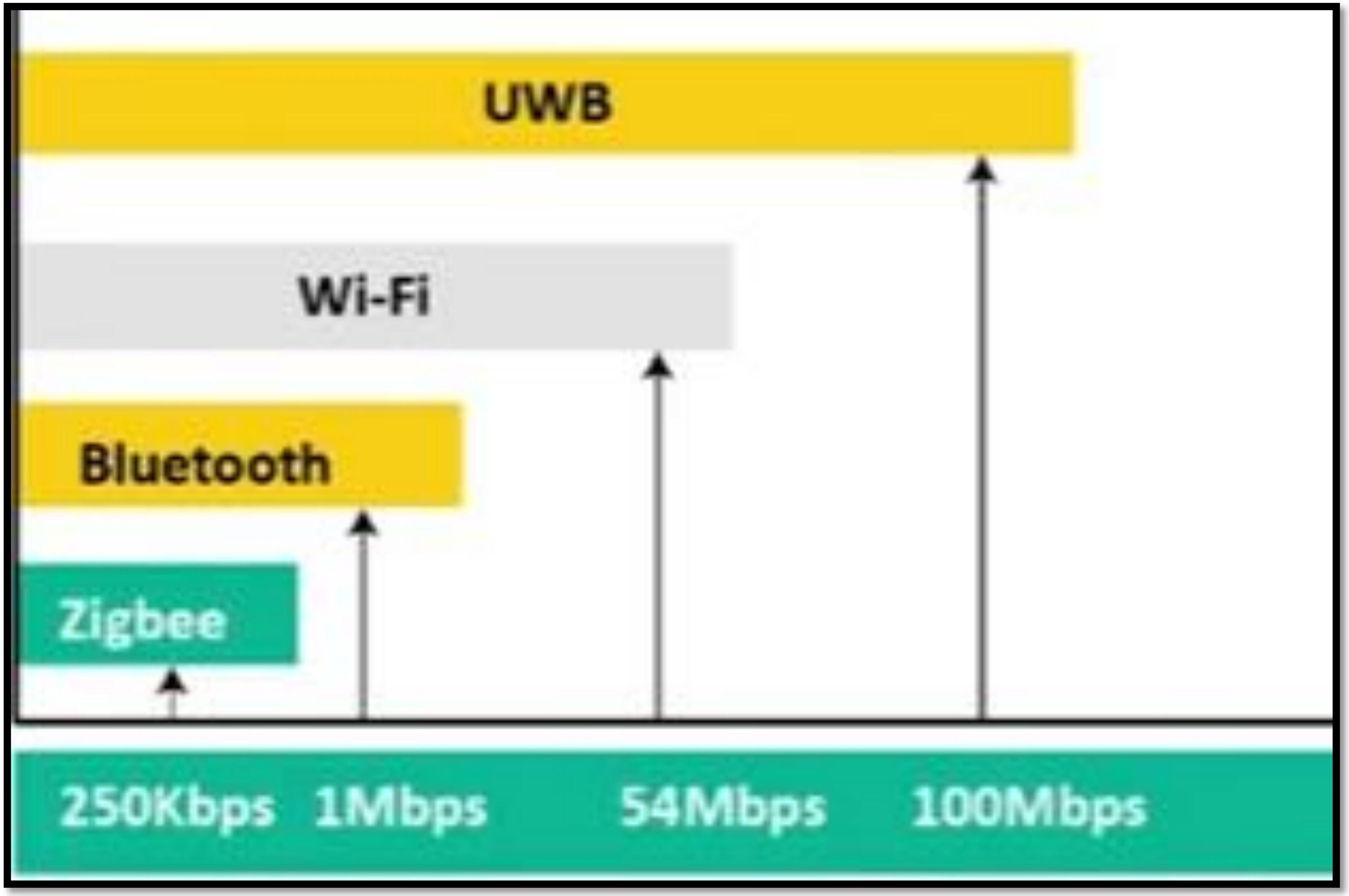


Orthogonal Frequency Division Multiplexing

Here, mobile devices such as laptop, mobile phones, etc. are connected to the access point using IEEE 802.11 standard. All the access points are connected to the server (may be academic campus, organization) with wires. In turn, the server is connected to the Internet. In this way, the Internet is accessed by the mobile devices in WLAN.

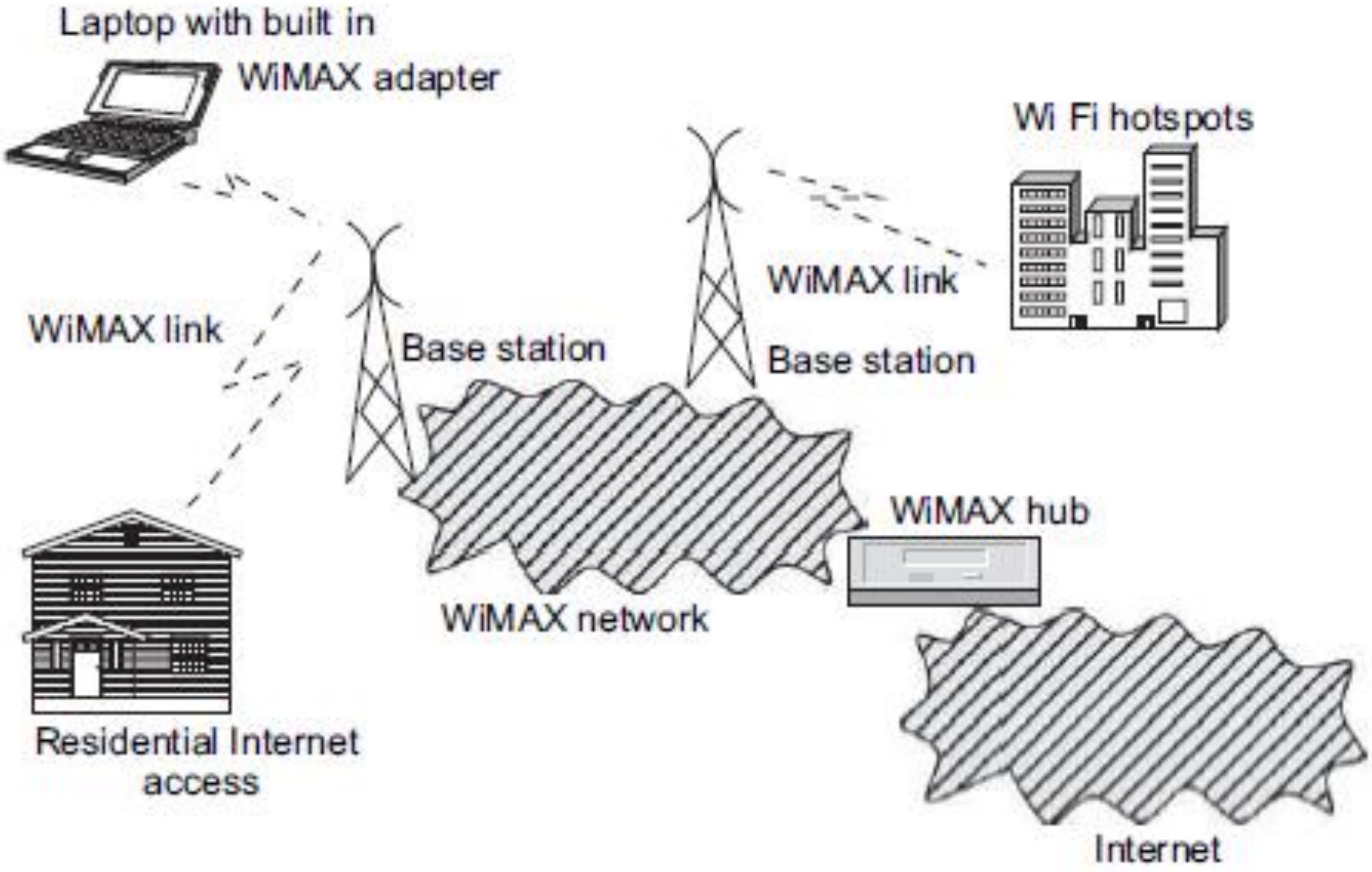


Standard	Bluetooth	UWB	Zigbee	Wi-Fi
IEEE spec..	802.15.1	802.15.3a	802.15.4	802.11a/b/g
Frequency band	2.4GHz	3.1-10.6 GHz	868/915 MHz; 2.4 GHz	2.4 GHz; 5 GHz
Max signal rate	1 Mb/s	110Mb/s	250kb/s	54Mb/s
Nominal range	10 m	10 m	10-100 m	100 m
Nominal TX power	0 - 10 dBm	-41.3 dBm/MHz	(-25) - 0 dBm	15 - 20 dBm
Number of RF channels	79	(1-15)	1/10;16	14(2.4GHz)
Channel bandwidth	1MHZ	500MHz-7.5GHz	0.3/0.6 MHz; 2 MHz	22MHz
Modulation type	GFSK	BPSK, QPSK	BPSK (+ ASK), O-QPSK	BPSK, QPSK COFDM, CCK, M-QAM
Spreading	FHSS	DS-UWB, MB-OFDM	DSSS	DSSS, CCK, OFDM
Coexistence mechanism	Adaptive freq. hopping	Adaptive freq. hopping	Dynamic freq. selection	Dynamic freq. selection transmit power control (802.11h)
Basic cell	Piconet	Piconet	Star	BSS
Extension of the basic cell	Scatternet	Peer-peer	Cluster tree-mesh	ESS
Max number of cell nodes	8	8	> 65000	2007
Data protection	16-bit CRC	32-bit CRC	16-bit CRC	32-bit CRC


UWB
Wi-Fi
Bluetooth
Zigbee
250Kbps
1Mbps
54Mbps
100Mbps

The Wireless Metropolitan Area Networks WMAN **is the fourth group** of the wireless networks. The networks working in accordance with this standard have a signal range of approximately 5–20 km; they are used to connect the user to the Internet. This standard is often called worldwide interoperability for microwave access (WiMAX or IEEE 802.16).

This is a good alternative to fixed line networks; it is simple to build and is relatively inexpensive. WiMAX is a worldwide interoperability for microwave access by the WiMAX Forum to promote conformance and interoperability of the IEEE 802.16 standard, officially known as WMAN. The Forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and digital subscriber line (DSL)."



Wireless metropolitan area network scenario.

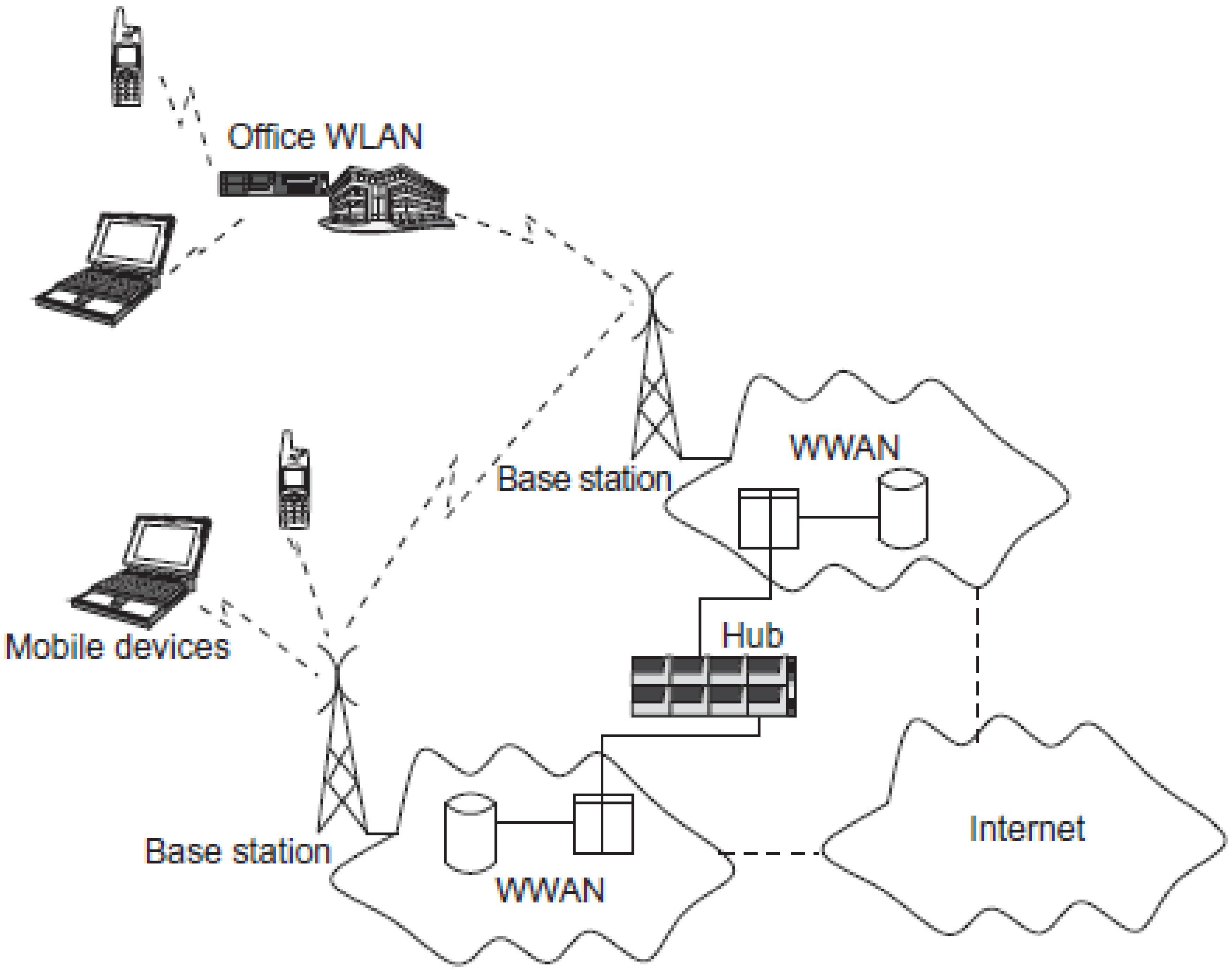
Mobile devices or residential Internet access are connected to the WiMAX base stations. The mobile devices may have built-in WiMAX adapter (or may be externally plugged) to access the WiMAX links. The users access the network resources or Internet by using WiMAX base stations. WiMAX base stations are connected to the WiMAX network.

With the help of WiMAX hub, WiMAX network is connected to the Internet. Wi-Fi users may also be connected to the WiMAX network for accessing the remote resources. A WMAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. WMANs might also be owned and operated as public utilities. They will often provide means for internetworking of local networks. WMANs can span up to 50 km.

The last group Wireless Wide Area Networks (WWANs). WWANs (GSM- and CDMA-based networks) employ the network infrastructure of mobile operators by means of which they provide wireless connection covering an area much wider than the group. A WWAN is a computer network covering a broad geographical area. The largest and most well-known example of a WWAN is the Internet.

WWANs are used to connect WLANs together, so that users and computers in one location can communicate with users and computers in other locations. Many WWANs are built for one particular organization and are private. Others, built by Internet service providers, provide connections from an organization's LAN to the Internet. WWANs facilitate connectivity for mobile users such as the traveling businessman.

In general, WWANs allow users to maintain access to work-related applications and information while away from their office. WWAN connectivity requires wireless modems and a wireless network infrastructure, provided as a fee-for-service by a wireless service carrier. Portable devices receive communications as the connected wireless modems and wireless networks interact via radio waves.

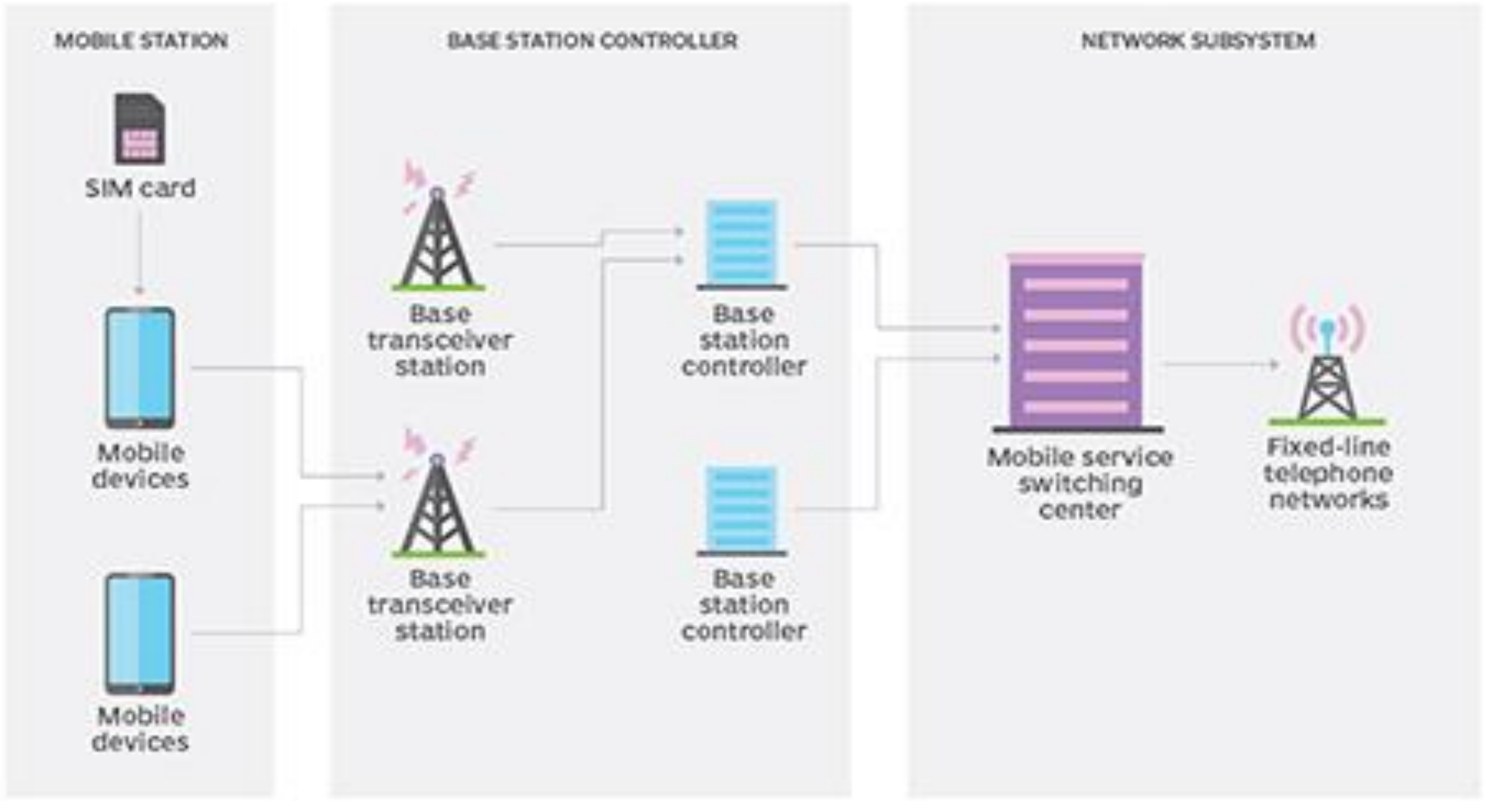


Wireless wide area network scenario.

The modem directly interfaces with radio towers, which carry the signal to a mobile switching center, where the signal is passed on to the appropriate public or private network link (i.e., telephone, other high-speed line, or even the Internet). From here, the signal can be transferred to an organization's existing network.

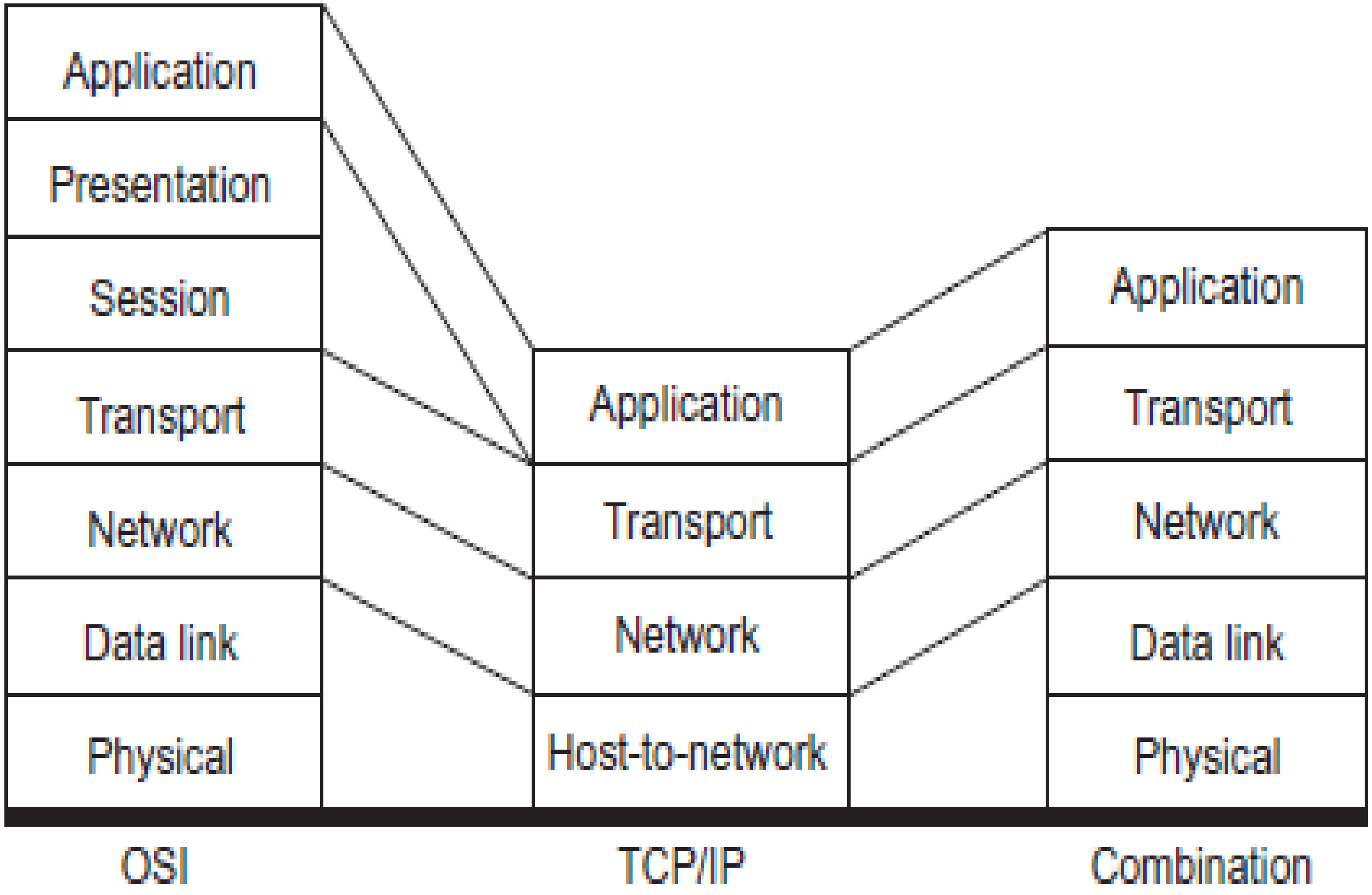
A WWAN uses cellular network technologies such as WiMAX, universal mobile telecommunications system (UMTS), general packet radio service (GPRS), global system for mobile (GSM) communications, cellular digital packet data (CDPD), high-speed downlink packet access (HSDPA), or 3G to transfer data. Each WWAN comprises a set of base stations that are connected by wires. WWANs are connected through a hub by using wires. Mobile devices can access the Internet through the respective base stations where they reside during communication.

Global system for mobile (GSM) network



Wireless Network Reference Model

Open systems interconnect (OSI) reference model to allow connectivity (or interworking) between different computer systems. Prior to the OSI reference model, computer systems made by one manufacturer could not easily communicate with computer systems made by other manufacturers.



Wireless network reference model.

The intent of the OSI reference model was to allow computer systems to successfully communicate with each other even though different vendors manufactured them. Transport protocol/Internet protocol (TCP/IP) architecture. It consists of **seven layers**: physical, data link, network, transport, session, presentation, and application.

Wireless Networking Issues

The challenge of a wireless network is to overcome the harsh reality of wireless transmission and to provide mobility and multimedia services. The data link layer of a wireless network has to provide assistance to several basic functions: traffic and resource allocation according to a traffic contract; flow control to avoid buffer overflow and also to discard packets of which the maximum allowed delay is exceeded due to retransmissions.

Error control to overcome the effect of errors on the wireless link; security and privacy for the mobile user, and mobility features to allow handover when a mobile moves to another area; quality of service (QoS) management when a connection is initiated or when the operating conditions have changed.

1- Traffic and Resource Allocation: Each accepted connection has a certain traffic contract that describes the traffic type and resource requirements. A slot scheduler is responsible to assign slots in a transmission frame according to the various traffic contracts. At the same time, it must attain a high utilization of the scarce radio bandwidth and minimize the energy consumption for the mobile devices.

2- Flow Control: A connection involves buffering at several places on the path between the sender and the receiver. Traffic type requirements concerning delay and implementation restrictions on the buffer capacity generally limit the amount of buffer space available to a connection.

Due to the dynamic character of wireless networks and user mobility, the stream of data might be hindered on the way from source to destination. Therefore, flow control mechanisms are needed not only to prevent buffer overflow, but also to discard packets that have exceeded the allowable transfer time.

3- Error Control: Owing to the high bit error rate (BER) that is typical for a wireless link, many packets can be corrupted during transmission. If this rate exceeds the allowable packet loss rate of a connection, an effective and efficient error control scheme must be implemented to handle such situations. At the radio physical level, redundancy for detecting symbols reduces the BER for the first time.

However, it is usually inefficient to provide a very high degree of error correction, and some residual errors pass through. The residual channel characteristic is based on erases, that is, missing packets in a stream. Erasures are easier to deal with than errors, as the exact location of the missing data is known. Then, integrated into the MAC layer (and possibly also into the higher layers), an error control scheme further enhances transmission quality by applying error correction and/or retransmission schemes.

Since different connections do not have the same requirements concerning packet loss rate and packet transfer delay, different error control schemes must be applied for different connection types. The error control scheme can also be adapted to the current error condition of the wireless connection. The error control mechanisms should trade-off complexity, buffering requirements, and energy requirements (taking into account the required energy for both computation and communication) for throughput and delay.

4- Security and Privacy: Network security refers to the protection of information and resources from loss, corruption, and improper use. Eavesdropper may listen to the traffic in real time or record it for future cryptanalysis. This can be done on radio, link layer (MAC), or network (IP) level. As eavesdropping of the data bits is a real threat because they will be transmitted over the wireless air interface, security and privacy are important issues in wireless systems.

These items are important on **two levels**: protection of the data on the wireless link and end-to-end application security. The MAC layer is only capable to provide some basic protection of the data on the wireless link. As it is hard to make this very secure, end-to-end security will be the most attractive and secure solution.

Other problems are denial of service, data integrity, tampering, and unauthorized access and spoofing. In tampering, attacker can modify the content of the intercepted packets from the wireless network and this results in a loss of data integrity. In unauthorized access and spoofing, attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. This kind of attack is known as spoofing. To overcome this attack, proper authentication and access control mechanisms need to be put up in the wireless network.

5- Mobility: In a wireless environment, the mobility of the wireless node enforces handover procedures when the node moves from one area to another. As the radius of an area (cell) decreases (because of the higher bandwidth density and lower energy requirements) handover situations will be encountered frequently. The task of the link layer is to provide the higher layers of the mobile with information about which areas (cells) are in range, and provide services to actually handle the handover.

The radio link quality will be the first parameter to be taken into account for the handover initiation procedure. In the new cell, a new connection has to be prepared and the bandwidth reserved. When a mobile is being handovered to a new cell, the connection will be dropped if there is insufficient bandwidth to support the connection.

As dropping connections is more undesirable than blocking new connection requests, some bandwidth can be reserved in neighboring cells in advance, before the mobile reaches that cell. It is possible to provide a general pool of bandwidth that can be used for new connections. If it is possible to predict the movement of wireless nodes, then bandwidth can be saved since not in all neighboring cells bandwidth has to be reserved.

6- Routing: Multihop wireless networks without any infrastructure (without access points or base stations) pose bigger challenges in computing proper and efficient routes for source destination pairs. This is mainly due to node mobility, that is, network topology frequently changes leading to unstable and improper routes. Thus, **dynamic routing protocols** are to be designed to take care of dynamic network configuration of wireless networks. Reachability and path minimization are some of the important features of routing.

Reachability: Any wireless network should have reachable paths from source to destination so that packets are delivered reliably and network performance improves. If the paths are not correct, packets will be dropped causing network throughput degradation, and user’s services will be hampered.

Path minimization: The paths from source to destination should be such that they should increase the throughput, lower the delays, satisfy user's quality requirements, reliability in data delivery, and reduce the computation and space costs. For example, a path with minimum bandwidth overheads.

7- Quality of Service (QoS) Management: To support diverse traffic over a wireless channel, the notion of QoS of a connection is useful. Setting up a connection involves negotiation along a path from sender to receiver to reserve the required resources to fulfill the needed QoS. Due to the dynamic nature of wireless channels and the movement of the mobile, the agreed QoS level in one or more contracts generally cannot be sustained for a longer period.

These situations are not errors, but are modus operandi for mobile computers. Therefore, these situations must be handled efficiently, and QoS renegotiations will occur frequently. Multimedia applications can show a more dynamic range of acceptable performance parameters depending on the user's quality expectations, application usage modes, and application's tolerance to degradation.

8- Radio Access: Frequency division multiple access (FDMA) or time division multiple access (TDMA) resource usage is based on the frequency reuse option concept throughout the cell and the microcell. Frequency reuse implies the distinct terminal use of the same channel in different cells with constraint on meeting a given threshold in interference.

In the spread spectrum multiple access (SSMA) or CDMA, subscriber spreads its transmitted signal over the same frequency. It resources the channel's assignment when network assigns a pseudo-noise sequence. New channel is set up only if interference threshold is below a given level, that is, the channel capacity of each cell depends on the actual status of the network.

9- Channel Allocation Scheme: Channel allocation scheme has an impact on the network performance. There are two categories of channel allocation schemes: fixed channel allocation and dynamic channel allocation schemes.

- **Fixed channel allocation scheme**: The interference constraint is ensured by the frequency plan. Frequency plan is independent of the number and the location of active module in the channel.

Each cell is assigned with a fixed number of carrier where it is dependent on the traffic density and/or the cell size. Frequency plan requires to be reconfigured in medium term or long terms. The interference constraints are ensured by the real-time evaluation of most suitable channel and most suitable one for mobile resource assignment. Currently, it is used by FDMA- and TDMA-based wireless networks.

- **Dynamic Channel Allocation Scheme (DCA):** It behaves dynamically to actual radio link and traffic needs. It allows total decentralized control of channel assignment even for network controller. It continuously monitors signal strength and quality of a broadband channel by using either the identity of transmitting base station or the wireless node.

This allows both wireless node and network to keep track of subscriber movement throughout the service area. The control channel assigns when the wireless terminal tries and eventually proceeds in accessing the network. It allows authentication and ciphering mode establishment. At this point, the terminal knows the servicing call. On this method, radio assignment channel is a responsibility of the network. It falls on the subscriber to cell association while simplifying control function during operation.

There are some concerns about the DCA. There can be uncontrolled situation in using these. The locally selected channel might be very good with specific wireless node whereas very poor to other traffic source. In the next generation system, this is resolved by having a very high-potential efficiency and robustness to traffic heterogeneity throughout the cell.

- **Random allocation schemes** The wireless nodes randomly try to access the broadcast channel whenever they have data to send and thus get the channel allocated to them. The scheme works well with the light loads, but, as the load increases the number of data collisions may increase due to simultaneous access by the users.

10- Power Management: Wireless devices have maximum utility when they can be used anywhere anytime. However, the finite power supplies is one of the limitation to achieve this goal. As batteries provide limited power, a general constraint of wireless communication is the short continuous operation time of wireless terminals. In the infrastructure wireless networks, mostly power management is done at the base station.

The base stations in infrastructure wireless networks have infinite power supplies; therefore, base station can run the centralized algorithms to provide the power-efficient network. In wireless peer-to-peer networks, the non-existence of a centralized authority complicates the problem of medium access control. Therefore, power management is one of the most challenging problems in wireless communication.

11- Pricing: This deals with pricing policies in wireless networks. The service providers should charge the prices based on the QoS requirements and the network situations.