1

Introduction

1.1 Radio Frequency Systems

Radio frequency (RF) systems are an essential part of our everyday life. They provide wireless connectivity for diversified applications, such as short-range car/door openers and wireless earphones, medium-range digital systems such as routers for computer data links, and remote-piloted vehicle controls, or long-distance communication systems such as cellular phones, and satellite networks. The required characteristics of wireless transceivers, however, are strongly dependent on the nature of the target system in which the equipment is intended to operate. In this introductory chapter, we provide a detailed overview of several important RF systems, with the purpose to provide the reader with a basic background on the different architectural and operational requirements, which directly dictate the various transceiver design strategies discussed in the chapters to follow.

1.1.1 Conceptual RF system

An RF system consists essentially of five major components, as shown in Figure 1.1.

Transmitter: Accepts at its input the information to be transmitted. Generates an RF signal embedding the input information. "Boosts" the RF signal to a suitable power level. The RF signal is routed to the antenna port.

Transmit antenna: Serves as the mediator between the transmitter and the transmission medium. Its purpose is to make sure that all the RF signal power present at the antenna port, leaves the transmitter, enters the transmission medium, and propagates in the desired direction.

Transmission channel: Is the medium separating the transmitter from the receiver. The RF signal must cross it in order to reach the receiving antenna. Usually the transmission medium consists of air or vacuum, but it may be solid or liquid as well. While propagating through the transmission medium, the RF signal loses its strength, and becomes weaker and weaker as it proceeds through the medium.

Receive antenna: Serves as the mediator between the transmission medium and the receiver. Its purpose is to capture as much as possible of the incident (weak) RF signal power remaining after crossing the medium, and convey it to the input of the receiver.
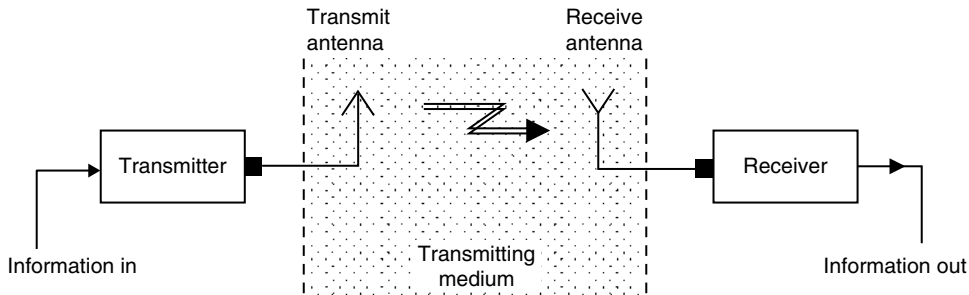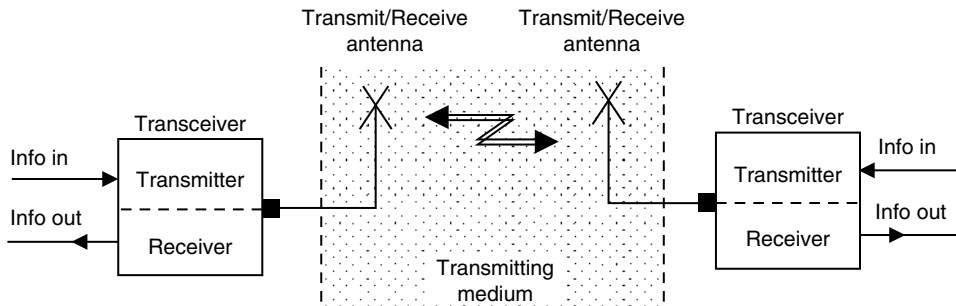
Figure 1.1 One-way RF system.

Figure 1.2 Two-way RF system.

Receiver: Accepts the RF signal captured by the antenna. Extracts the information embedded in it. The information is routed to the receiver output.

The system of Figure 1.1 is one-way. However, adding an identical RF system in the opposite direction yields a two-way RF system, as shown in Figure 1.2. The transmitter/receiver combination is termed a "transceiver". The antenna may transmit and receive simultaneously, while the transmitter and receiver are operating independently from each other.

1.1.2 The frequency spectrum

For various reasons, not all RF frequencies are equally well-fit for implementing different RF systems. For instance, since the optimum physical dimensions of transmit and receive antennas are directly related to the frequency and must be made larger as the frequency becomes lower, it follows that at low frequencies the antenna size becomes impractical for use in mobile systems such as cellular. In contrast, as the frequency becomes higher, the antennas may be made smaller, but the power losses and Doppler fading through the medium increase, which limits the transmission range and the travelling speed. It follows that choice of the RF frequency range is application dependent and the number of useful RF channels is limited. Several RF system architectures, such as the cellular architecture, have been developed in order to overcome the frequency shortage.
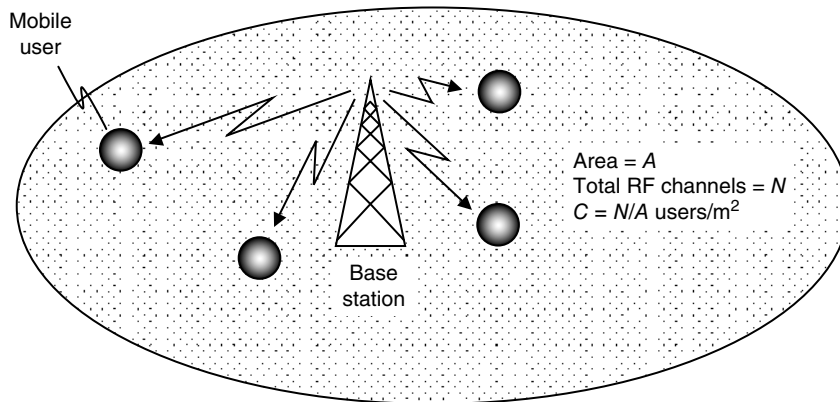
Figure 1.3 Limited capacity RF system.

1.1.3 Cellular concept

The cellular concept is of great importance. Many modern RF system architectures are based on it, thus we find it appropriate to discuss it briefly here. As pointed out in the previous section, the number of available frequencies for mobile applications is limited. With reference to Figure 1.3, assume that a multitude of mobile users are found simultaneously in the region of area A. Further assume that there are N available RF channels and all the users connect to each other through a central base station that is located at a favorably high spot to provide appropriate geographical coverage. It follows that the system capacity is limited to $C = N/A$ simultaneous users per square meter. Clearly such an architecture is limited and cannot support large communication systems in large coverage areas.

Now, with reference to Figure 1.4, assume that we divide the same area A into separate sub-areas, named "cells". At the center of each cell we place a base station that transmits with power sufficient to cover its own cell, but low enough so that it cannot be received in the adjacent cells. The base stations are all connected to each other by physical lines interconnected by a central computer that acts as a switch. Now, assume that we arrange the cells in regular patterns of cells, called clusters, each consisting of K adjacent cells.

Since, there is virtually no interference between cells belonging to different clusters, we can use all the N frequencies within each cluster. If the whole coverage area consists of M clusters, it follows that now the system capacity increases to $C = N/(A/M) = MN/A$, a factor of M. However, the problem remaining is how to prevent the mobile users from losing communication when passing from cell to cell. To see how the issue is solved, assume that the base stations in the various cells continuously report to the central computer how well they receive the mobile subscribers passing nearby. Assume now that a mobile subscriber is connected to the base station of cell #1 and is approaching cell #2, while travelling away from cell #1. At a certain point the user will begin to lose communication with cell #1, while the link with cell #2 becomes stronger. Since the central computer is aware of the scenario, at a certain point it will instruct the mobile user to leave the channel of cell #1 and connect to a free channel of cell #2. This process is called a "handoff" and allows the mobile subscribers to pass from cell to cell without losing
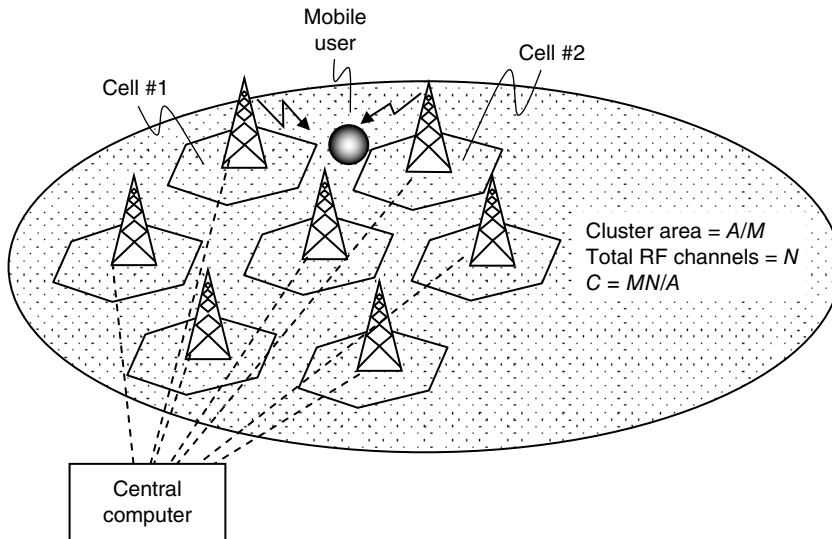
Figure 1.4 The cellular principle.

communication. The cellular architecture was made possible by the advent of micro-processor components, which allowed introducing enough intelligence within the mobile equipment so to be able to instruct it how to handle the handoff process.

1.2 Detailed Overview of Wireless Systems and Technologies

1.2.1 System types

Wireless communications using electromagnetic waves began at the end of the nineteenth century with Tesla, Popov, and Marconi. Marconi sent the first wireless signals (Morse code). In his first experiments, Marconi used a wavelength (λ) much longer than 1 km, and it was in 1920 that he discovered short waves with $\lambda \approx 100$ m.

World War 2 gave rise to many advances in development of wireless communication systems, especially in the fields of RADAR (*RA*dio *D*etecting *A*nd *R*anging), wireless data transmission, and remote sensing. Since then, wireless communication has been evolving continuously, significantly affecting many different aspects of our life. Standardization of the communication technologies, an important step in development of communication systems and services, started with the advent of commercial TV in the 1940s, when the first TV standards were introduced. The development of mobile communications was rather slow till the 1970s, when enabling technologies were developed for reliable, compact RF circuits and modules.

Today, wireless communication systems are very ubiquitous, providing a wide variety of highly reliable services. A broad range of systems and services have been developed, paving the way for implementation of wireless communication systems: satellite

communications, radio and TV broadcasting systems, mobile phones, wireless LANs, wireless sensor networks, and so on.

The rapid growth of wireless systems implies an increased demand for spectrum, making spectrum allocation a key issue for the further extension of existing communication services and the development of new ones.

The challenge in the design of communication systems is the efficient use of the allocated resources, that is, power budget and available bandwidth, to provide high-quality communications in terms of bit error rate (BER) and data rate (measured in bits per second, bps). In the case of wireless communications, the design of such systems is even more challenging due to the fact that wireless channels are subject to dynamic fast environmental changes.

No single technology can provide a proper and optimal solution for all desired wireless applications. Wireless communication systems/networks can be generally divided into three main categories, where each category aims to address specific needs. The division is based on the coverage range: wireless personal area network (WPAN), wireless local area network (WLAN), and wireless wide area network (WWAN). The system's range determines its latency.

WPANs, such as Bluetooth, provide wireless communication in short ranges of a few centimeters up to several meters. In these systems, the communication is mostly a point to point communication. Point to multipoint communication is also possible, for example PicoNET (a network generated by two or more Bluetooth enabled devices). The data rate in WPAN is rather low, limited to a few 100s of kbps.

WLAN is a medium-range wireless network covering areas up to 100s of meters. Examples include Wi-Fi and DECT (*D*igital *E*nhanced *C*ordless *T*elecommunications). The data rate is high, that is up to 20 Mbps.

WWANs are aimed at providing high speed long-distance links extending to several thousand kilometers. Examples include cellular phones, satellite communications, and WiMAX. Beside the geographical scope, the wireless networks WLAN and WWAN differ in data delivery scheme, data rate limitations, and spectrum regulation.

One important distinction between small and large networks corresponds to the ownership of the networks. Small networks are owned and operated by the users. Large networks are owned and operated by service providers that are not necessarily the main users of the network.

The IEEE 802 family of standards governs the physical layer (PHY) specifications and datalink aspects of networking (both wired and wireless networks). Among other IEEE 802 standards, the most widely used standard for wired LANs are IEEE 802.3 (called Ethernet) and 802.5 (Token Ring). The popular standards for wireless networks are 802.15 (Wireless PAN), 802.11 (Wireless LAN), and 802.16 (WiMAX).

A detailed description of these systems is given in the following sections.

1.2.2 Wireless network architectures

1.2.2.1 Wireless Personal Area Network

WPANs are small-scale wireless networks providing low-cost, power-efficient connectivity between a small group of private devices located in proximity to a person, and between these devices and the external world. A WPAN covers the personal space surrounding a person in the range of 10s of meters and can be thought of as a

complementary communication capability for longer range networks, such as WLANs and cellular networks. WPANs allow removing the need for fixed cabled connections. They need no infrastructure or direct connectivity to external world, and hence help to increase the mobility. Personal devices that can be networked by WPANs include: laptops, handheld computers, personal digital assistants, tablets, and cameras.

WPANs are standardized by the IEEE 802.15 group that focuses on standards governing short-distance wireless networks. The IEEE 802.15 standard group is divided into four main task groups:

1) Task Group 1 (TG1) is devoted to standards for Bluetooth operating in the 2.4 GHz unlicensed ISM (*I*ndustrial, *S*cientific, and *M*edical) band.
2) Task Group 1 (TG2) is devoted to the coexistence of devices that operate in unlicensed spectra.
3) Task Group 3 (TG3) is devoted to high data rate WPAN standards, that is UWB (*U*ltra *W*ide *B*and) WPAN.
4) Task Group 4 (TG4) is devoted to a low data rate, low power WPAN standards.

Here we will describe three standards implemented by IEEE 802.15: Bluetooth (IEEE 802.15.1), UWB (IEEE 802.15.3), and ZigBee (IEEE 802.15.4). The standards are to create harmony in technologies from different industrial manufacturers.

Bluetooth (IEEE 802.15.1)

Bluetooth is a widely used WPAN technology that provides ad hoc wireless networking in short-distance stationary and/or mobile environments. It is intended to convey both voice and data using inexpensive and low-power devices. It was proposed by Ericsson in 1994 and originally aimed at eliminating the need for cabling between PCs and their peripherals, such as printers and keyboards.

In 1998, the Bluetooth special interest group (SIG) was established to foster further development of the Bluetooth concept and applications. The SIG was first formed by five companies (Ericsson, Intel, IBM, Nokia, and Toshiba) and later thousands of companies joined this group. The SIG focused on three applications of Bluetooth: (i) cable replacement, (ii) formation of ad hoc networks in a small area called piconet, and (iii) providing voice and data access point to wide-area networks, both wired and wireless. The first Bluetooth standard was released in 1999, and in 2000 there were mobile phones with Bluetooth capabilities.

The Bluetooth topology is based on the Piconet/Scatternet scheme. Piconets are the basic networking units formed by ad hoc detection of nearby (Bluetooth enabled) devices. The Bluetooth Scatternets are extended networks allowing the participation and coexistence of multiple piconets.

A piconet is a small cell consisting of two or more Bluetooth devices that share the same medium using a master-slave mechanism. In other words, a piconet is a WPAN, in which one device acts as a master, that is it initiates and manages the communication with the other (slave) devices. A master device can communicate with the slaves either in point to point or point to multipoint modes. But, slaves are restricted to point to point communication with the master. A master device of one piconet can be slave of other piconets. Each device may belong to a number of piconets at the same time, thus allowing for data to flow beyond the range of a piconet. Over the time, the roles of master and slave

devices can change, from master to slave and vice versa. All devices in a piconet are synchronized by the master's clock.

In order to allow for power conservation, each slave device can work in either one of the following modes: active, sniff, hold, park, and standby. A slave device can communicate with the master only in the active mode. The number of active slaves is limited to seven. In the other three modes, the "listening" time of the slave is reduced to different degrees. Master devices are always active. Each piconet can accommodate one master, up to seven active slaves, and up to 255 standby slaves.

Bluetooth uses the FHSS (*F*requency *H*opping *S*pread *S*pectrum) modulation method to combat interference from other sources, either narrow or wide band, such as other Bluetooth devices, hence allowing for concurrent communication between several Bluetooth devices located in close vicinity of each other. As shown later in this Chapter, in the FHSS technique, the carrier frequency hops from one frequency to another following a certain pseudo-random sequence, to produce a spread spectrum signal, with a small power spectral density. Using FHSS, tens of piconets can overlap in the same coverage space, so that the throughput can be very high (exceeding 1 Mbps). Data is transmitted in packets.

In Bluetooth, each piconet is assigned a unique pseudo-random hopping sequence determined by the master's identity. The hopping phase is determined by the master's system clock. Bluetooth uses 79 RF channels covering the whole bandwidth of 83.5 MHz from 2400.0 MHz to 2483.5 MHz. The RF channels are 1 MHz apart, the hopping rate is 1600 hops per second, and the hop dwell time is 0.625 ms. The 79 hops are arranged in even and odd numbered slots. The master transmits over the even slots and the slaves use the odd slots.

One drawback of using FHSS is the relatively long time (up to 5s) needed to set the Bluetooth connections.

Standard Bluetooth uses digital communication with a GFSK (*G*aussian binary *F*requency *S*hift *K*eying) modulation scheme. The Gaussian shape of the FSK signals produces signals with a narrow power spectrum and hence decreases high power consumption. Recently, other modulation schemes besides GFSK have been also adopted.

Bluetooth MAC (*M*edium *A*ccess *C*ontrol) is based on TDD (*T*ime *D*ivision *D*uplex) to allow for full duplex transmission and elimination of crosstalk between the transmitter and receiver. In this scheme the time is divided into slots where the duration of each slot is 0.625 ms. As mentioned above, data is transmitted through packets carrying either synchronous information (voice) or asynchronous information (data). The packets are transmitted over different hop frequencies (subcarriers). The data rate in the voice channels is 64 kbps, and in the asynchronous data channels data rates can reach 723.2 kbps asymmetric and 433.9 kbps symmetric.

Simultaneous participation of a Bluetooth device in multiple piconets is enabled by TDM (*T*ime *D*ivision *M*ultiplexing) and allows multiple voice and data stations to participate in a piconet.

Bluetooth uses low-power signals of 1 mW (0 dBm) for ranges up to 10 m. The transmitting power can be increased to up to 100 mW (20 dBm) in order to extend the coverage range up to 100 m. The Bluetooth standard specifies three classes of transmitting power levels: 100 mW (class 1), 2.5 mW (class 2), and 1 mW (class 3). Bluetooth receivers are required to have a sensitivity of −70 dBm or better.

New releases of Bluetooth foster further developments of this technology. In particular the Bluetooth technology is used to explore the growing field of Internet of Things.

UWB (IEEE 802.15.3)

Bluetooth's data rate is not high enough to support the high data rates required in multimedia applications. UWB WPAN technology has been developed to address the ever-growing demand for high data rate WPANs, with higher capacity, high quality of service (QoS), low power consumption, and low cost. Thanks to its great bandwidth, UWB WPAN can provide data rates over 110 Mbps, sufficiently high for audio and video delivery in small areas.

USB is well suited for home multimedia wireless networks, as it can provide more than 110 Mbps for distances up to 10 m, and 480 Mbps for a distance of 2 m. UWB WPAN can also replace high speed cables such as USB 2.0.

The UWB WPAN technology has been standardized by the IEEE 802.15.3 standard group. It is intended to interconnect devices confined to a small coverage area of up to 10 m (e.g. home or office) for streaming high data rate multimedia, such as high-definition video. However, unlike the 802.15.1 standard that completely governs Bluetooth technology for short-range communications, the UWB standard pertains only to a certain part of such communication standard.

UWB is not a new technology, as it has been used in different applications such as sensing and localization. In recent years, UWB was applied to wireless data transmission.

According to the FCC, any signal with a relative (fractional) bandwidth exceeding 20% or an absolute bandwidth greater than 500 MHz is considered a UWB signal.

UWB (absolute) bandwidth is commonly defined as the frequency band bounded by points 10 dB below the peak emission. The UWB signals' relative bandwidth is the ratio between the absolute bandwidth and the center frequency.

The Shannon capacity formula for an AWGN channel, showing the direct proportion of the channel capacity and the signal bandwidth, reflects the potential for high data rates in UWB-WPANs.

UWB signals are characterized by very high bandwidth, very low power spectral density, and low transmitting power (less than 1 mW). It uses low energy RF pulses of different shapes of extremely short duration, with no specific carrier frequency. There are different UWB pulse shapes, such as Gaussian, chirp, wavelet, and Hermite-based short-duration pulses.

The low power and broadband features of the UWB signals result in important advantages, including high throughput, jamming mitigation, and coexistence with other radio links. It can provide data rates up to 480 Mbps. The low energy density property minimizes interference to other services. It also enables the usage of a spectrum being used by other services, hence increasing the spectral efficiency. Other advantages include multipath immunity, low cost, and all digital architecture.

UWB radios must allow for co-existence with narrow-band licensed signals, such as GSM (*G*lobal *S*ystem for *M*obile communications) and GPS (*G*lobal *P*ositioning *S*ystem) that use the same spectrum, without causing intolerable interferences.

In 2002, the Federal Communications Commission (FCC) approved, for the first time, the unlicensed deployment of UWB under a strict spectral mask for indoor and outdoor applications in the United States. The low transmitting power levels (−41.3 dBm/MHz) are meant to ensure that UWB coexists with existing (licensed) communication links,

with minimal interference. The allocated band is the 3.1–10.6 GHz frequency band, that is a bandwidth of 7.5 GHz.

The first UWB communication systems were implemented using very short pulses, which is a carrier-less modulation scheme, and can be considered as a baseband signal. This is a single-band modulation technique that is known also as an impulse radio (IR) modulation. The short duration impulses (less than 1 ns) have a very wide spectrum and very low power spectral density levels.

Since the allocation of the 3.1–10.6 GHz frequency band by FCC in 2002, some other wireless communication technologies have been proposed for UWB transmission. These include multiband (MB) techniques such as multiband orthogonal frequency division multiplexing (MB-OFDM) in which the UWB frequency band is divided into multiple sub-bands, and data is independently encoded in different bands. MB-OFDM was supported by the WiMedia Alliance and considered by IEEE 802.15 task group 3a. In addition to MB-OFDM, the IEEE 802.15.3a standard group considered the direct sequence UWB (DS-UWB) that was developed by the UWB Forum. In DS-UWB, a single pulse of short duration is used that occupies the whole bandwidth of 7.5 GHz. The DS-UWB uses DSSS (*D*irect *S*equence *S*pread *S*pectrum) techniques with variable-length spreading codes and either BPSK (*B*inary *P*hase *S*hift *K*eying) or quadrature biorthogonal keying (4-BOK) signals. This technique can reach high data rates up to 1.32 Gbps.

In the MB-OFDM approach the spectrum is divided into 14 bands of bandwidth 528 MHz, whereby in each band a 128-point OFDM signal using QPSK (*Q*uadrature *P*hase *S*hift *K*eying) modulation is implemented.

UWB WPANs use a topology based on small networks called piconets, like in the case of Bluetooth. However, in 802.15.3 networks piconets are controlled by a dedicated device called the PicoNet coordinator. The network is formed in an ad hoc manner, where devices may dynamically join and leave the network. Unlike Bluetooth (and other WPANs) UWB allows for direct link between devices in a piconet.

UWB uses ARQ (*A*utomatic *R*epeat *Q*uery, or automatic repeat request) aimed at improving the data transmission reliability. ARQ is an error control method, in which the receiver can detect an error in a certain packet. It automatically informs the transmitter to retransmit the corrupted packet, hence reducing the error rate significantly.

ZigBee (IEEE 802.15.4)

Bluetooth and UWB WPANs provide short-range device connectivity and wire replacement. The former has a moderate data rate (up to 1 Mbps), and the latter provides high data rates (110 Mbps). With the availability of these WPANs, a question may arise as what would be the drive to develop ZigBee as another WPAN standard? What added value does it have?

ZigBee, based on the IEEE 802.15.4 standard, has gained its popularity mainly due to its low power consumption and low cost. The nominal transmitting power is from –25 dBm to 0 dBm. Other advantages include ease of installation (joining time for a new slave is typically 30 ms), reliability (mesh networking architecture), greater range (using multi-hop and mesh networking), and a simple and flexible protocol.

The long battery life (typically measured in years, while operating by an AA cell) implies almost no constant maintenance. The low power consumption is a key feature of ZigBee, and this comes at the price of a low data rate (about one-fourth of Bluetooth's 1 Mbps data rate). However, there are many applications in which the advantages of

ZigBee, especially the extremely low power consumption, are more important than the data rate capabilities. Thus, ZigBee is better suited for applications that need only small data packets to be transmitted over large networks (mostly static ones) consisting of a large number of devices. Each ZigBee network has the capacity to support more than 65 000 active devices (compared to eight devices in Bluetooth). ZigBee can be embedded in many applications, such as remote controls, sensors, monitoring services, home automation, and toys. Using a ZigBee network of embedded nodes it is possible to tie together a whole factory, office, or home for safety, automation, and security.

The ZigBee standard for PHY specifies three license-free bands: the 2.4 GHz band, the 915 MHz band, and the European 868 MHz band. The 2.4 GHz band uses the 2.4–2.4835 GHz spectrum with 16 channels and maximum (ideal) data rate of 250 kbps. It can be used worldwide. The 915 MHz refers to the 902–928 MHz band with 10 channels for North America. The data rate is 40 kbps. The 868 MHz band refers to the 868–870 MHz band with one channel for Europe. The data rate is 20 kbps. DSSS techniques are used in all bands.

The 915 and 868 MHz bands use BPSK modulation, and the 2.4 GHz band uses offset QPSK.

Each ZigBee network's node (or device) consists of a transceiver, a microcontroller, and an antenna.

The devices are classified into three categories: PAN coordinator, router, and end device. They are further distinguished as either a full-function device (FFD) or a reduced-function device (RFD). Any FFD can act as either of three device (node) types: a PAN coordinator, a router, or an end device. An RFD can operate merely as an end device. FFDs can communicate with both RFDs and other FFDs.

The PAN coordinator is a smart FFD that initiates the formation of a new PAN, and serves as a bridge to other networks. There is only one coordinator in each ZigBee network. The coordinator should find a suitable RF channel to avoid interfering with WLAN channels operating in the same frequency bands (2.4 GHz bands). After formation of a network by the coordinator, other ZigBee devices can join it.

A router is an FFD that links devices and groups together and allows for multi-hopping from a source device to a destination device.

The ZigBee end devices are either an FFD or RFD that can communicate with the coordinator and routers, but are not involved in the routing process.

Unlike coordinators and routers, the end devices are battery powered and can be in sleep mode in order to minimize battery consumption. These devices have 64 bit addresses. If necessary, the address size can be shortened to 16 bits in order to reduce packet size.

ZigBee supports three network topologies: star, tree, and mesh. Star network is the simplest topology in which messages are exchanged between end devices in two hops. In this configuration, devices communicate via a central node, called the PAN coordinator, through which all messages are passed. The reliability of the star topology is relatively low as there is only one path between each node pair.

A tree network starts with a top node (root tree) below which branches evolve via a net of routers to the end devices. The routers extend the network coverage area. The tree network is a multi-hop network in which messages travel up and down the tree to reach destination. One drawback of the tree topology is its low reliability due to lack of alternative paths if a router is disabled.

A mesh (or peer to peer) topology is a multi-hop network with a structure similar to a tree topology, in which there is a direct path between some branches. Data packets are routed to their destination across the tree through an available route.

The mesh topology is characterized with high reliability, as there exist different routes between each device pair. This topology allows for network extension by amending new devices and routers to the network.

There exist other topologies, such as the cluster tree or clustered star networks that are based on a combination of the above-mentioned topologies.

The ZigBee technology is based on a standardized set of layers. IEEE 802.15.4 standard defines only the characteristics of the PHY and MAC layers, and the ZigBee Alliance specifies network and application layers.

The functions provided by the PHY layer are the modulation and transmission of the signal at source, and the reception and demodulation of the received signals at the destination.

The MAC layer accesses the network and provides synchronization and coding to increase reliability of data exchange. Access to the network is based on carrier sense multiple access with collision avoidance (CSMA-CA).

The network layer performs the functions of network initiation, detection of neighbor devices, adding/dropping of devices to the network, and route discovery.

A ZigBee network can operate in either the beacon mode, or the nonbeacon mode of communication to enable data exchange between devices. The beacon mode is employed in battery activated coordinators in order to minimize power consumption. The nonbeacon mode is preferable when the coordinator is operated by mains.

In the beacon mode, devices become active when a beacon is transmitted, so they all know when to communicate with each other. In this mode a coordinator periodically sends beacons to the routers in the network. Upon receiving a beacon, devices "wake up" and look for incoming messages. After a message is completely transmitted to a certain device, the coordinator sets a time for the next beacon, and the device and the coordinator enter the sleep mode till the next beacon.

In the nonbeacon mode, the coordinator and routers are always active. In this mode every device must know the schedule for communication. This requires a precise timing system in each device, increasing its power consumption level. It should be noted that, even though the power consumption level in the nonbeacon mode is higher than its level in the case of beacon mode, the power consumption in the former mode is also low since devices are mostly in inactive "sleep" mode.

1.2.3 Wireless local area network

Local area networks (LANs) emerged during the 1970s out of a desire to share resources such as printers and storage devices, at first as a wired means to connect computers located in a small area such as an office. The networking between PCs allowed each user to access resources (data and services) residing on other computers. LANs have a limited geographic extent in a fixed location, for example an office building or a university campus. The physical reach of LANs is between a few 100s of meters to a few kilometers. LANs provide reliable, high speed, secure, and low-cost connectivity between users, who are usually the owner of the network. In the first LANs of the 1970s, computers were interconnected by coaxial cables or shielded twisted-pair lines. Unshielded twisted-pair

and optical fibers were used in later stages. The structure and protocols of LANs are based on packet communication. Since the 1970s, LANs have evolved in line with the growing demand for high speed and low-cost communication between PCs. Ethernet, invented in 1973, has become the predominant wired LAN. Ethernet is an asynchronous technology, that is no system level timing is required. The Ethernet standard was developed by the IEEE 802.3 working group in the 1970s. It is a CSMA/CD protocol based on carrier sensing, collision detection, and random time delay before resending a packet corrupted upon collision with another packet.

Wireless LAN (WLAN) technology was envisioned as an extension of wired LAN technology: users are able to move around in the coverage area with their laptop (or other portable devices) with no need to deal with cabling. In 1971, a packet-switched wireless communication network called Alohanet was developed. This pioneer WLAN provided communication between seven computers at the University of Hawaii.

The first WLANs were deployed in 1990s and as expected had lower performance than wired LANs. For example data rates of only a few Mbps, compared to data rates of 100 Mbps in wired LANs. Since then, much effort has been devoted to improve the WLANs' performance, functionality, and compatibility to a level similar to wired LANs.

WLANs mark the beginning of the era in which the dream of connectivity at anytime and anywhere became reality. Many WLANs are deployed as an extension to existing wired LANs, increasing the users' capabilities for mobility and Internet access.

The WLAN has good flexibility, that is it allows adding many different devices very easily, and facilitates the deployment of hot spot-like and ad hoc networks (e.g. mesh networks), otherwise requiring costly and complicated cable installation. WLANs are now well established and almost all laptops, smartphones, tablet computers have built-in capability for wireless networking.

WLANs use the unlicensed ISM bands. This fact had a great impact on the successful development of WLANs, and is considered as a great strength of this technology as it removes the need for any regulation and restrictions.

The first wireless standards were based on the Ethernet standard (IEEE 802.3), even though the performance of WLANs was not up to the level of Ethernet at that time. All WLANs are governed by the IEEE 802.11 standards family developed since 1997. The first standard was IEEE 802.11a issued in 1997. It specified a center frequency of 5 GHz, and a maximum (raw) data rate of 54 Mbps, with ranges of 35 m indoors and 115 m outdoors. This standard uses the OFDM (*O*rthogonal *F*requency *D*ivision *M*ultiplexing) modulation method. IEEE 802.11a was not as widely accepted as IEEE 802.11b, apparently due to the use of the rather incompatible 5 GHz band, as compared to the 2.4 GHz band of the IEEE 802.11b standard.

IEEE 802.11b was the first WLAN standard widely used. Its range is 38 m indoors, and 125 m outdoors. IEEE 802.11b uses a modulation technique called Complimentary Code Keying (CCK) with a center frequency of 2.4 GHz. The maximum data rate is 11 Mbps, much lower than that of IEEE 802.11a.

In 2003, the IEEE 802.11g standard was introduced, based on the 2.4 GHz band (like IEEE 802.11b) and offering a bit rate of 11 Mbps (like IEEE 802.11b). The coverage range of this standard is 38 m indoors and 125 m outdoors.

In 2009, two versions of the IEEE 802.11n standard were developed, one operating in the 2.4 GHz band and the other in the 5 GHz band. This standard offers high data rates

up to about 150 Mbps, an indoor range of 70 m and outdoor range of 1125 m. IEEE 802.11b and IEEE 802.11n are the most popular standards.

In the standards using the 2.4 GHz band, there are two power limits. For IEEE 802.11b using CCK modulation the maximum EIRP is 18 dBm (63 mW) set by the spectral power mask of 10 dBm/MHz (10 mW/MHz). For IEEE 802.11 g and IEEE 802.11n standards that use OFDM modulation, the limit is 20 dBm (100 mW). Since the 5 GHz band is divided into two bands, namely 5150–5350 MHz and 5470–5725 MHz, each band can have different power limits.

WLANs use spread spectrum and OFDM, in which the available spectrum is divided into many small bands, and each band uses a different subcarrier.

The very first WLANs operated in the unlicensed frequency band of 902–928 MHz. Over time, the interference level in this band grew as many other unlicensed devices started using this band. To mitigate the interference, spread spectrum techniques were used. The data rate with the spread spectrum was 500 kpbs.

The next generations of WLANs used the 2.4–2.483 GHz ISM band. However, the potential of interference from nearby systems such as MW ovens, cordless telephones, garage door openers operating in the 2.4 GHz ISM band led to using spread spectrum techniques that are less sensitive to such interference and noise sources. The data rate was increased to 2 Mbps, that is four times faster than the first generation.

The more recent WLANs allow for data rates up to 10 Mbps, operating at 5 GHz ISM band of 5.775–8.85 GHz, and an additional frequency band around 5.2 GHz.

1.2.3.1 Wi-Fi

Wi-Fi refers to WLAN devices based on the IEEE 802.11 standards and approved by the Wi-Fi Alliance. The term Wi-Fi was originally used for the 802.11b standard, considered as a fast standard (11 Mbps). Later, the Wi-Fi Alliance extended Wi-Fi to include other standards as well.

The main application of Wi-Fi is to enable mobile users to access Internet easily. Users of portable devices, such as a cellular phone or a laptop, with Wi-Fi capability, can access the Internet when being within the coverage range of a Wi-Fi access point.

Originally, the main idea behind Wi-Fi was to connect between PCs and peripheral devices located in proximity, for example an office environment. Nowadays, it has many more applications, including emailing, access to the Internet, and downloading music and videos.

The coverage area of a Wi-Fi network is called a Wi-Fi hotspot. For example, public areas such as university campuses, airports, lobbies (hotels and others) that have an accessible wireless network are Wi-Fi hotspots providing Internet access. When in a hotspot, a user can connect to the Wi-Fi network from his laptop, cellular phone, or any other device with Wi-Fi capability. It is also possible to set a hotspot (at home, for instance) using a mobile phone connected to a cellular network.

Wi-Fi allows for two operation modes: peer to peer communications between users (ad hoc mode), or communication through a central access point. In the latter case, the access point is usually connected to a wired LAN through which the users can access the Internet. The access point consists of a wireless router operating according to IEEE 802.11 standards.

Wi-Fi uses frequency bands within an unlicensed ISM spectrum. However, as the ISM spectrum is shared by many other systems the interference level increases, leading to

degradation of the QoS. The main ISM bands used in Wi-Fi are the 2.4 GHz band, used in IEEE 802.11b, g, and n versions. The 5.8 GHz band, that is the 5725–5875 MHz bandwidth, provides additional bandwidth. Wi-Fi has 14 channels in the 2.4 GHz ISM band, supported in most countries.

1.2.3.2 Wi-Fi Direct
Wi-Fi Direct provides direct connectivity between clients without any access point. It is based on the IEEE 802.11 standard. The idea behind Wi-Fi Direct is to produce groups in which one node is chosen as the host (access point; AP) and manages the communication between the group's nodes. For this purpose Wi-Fi Direct uses a soft AP (a software-defined AP) to provide peer to peer communication.

1.2.4 Wireless wide area network

Wireless Wide Area Networks (WWANs) are wireless networks that span over large areas such as cities and countries, far beyond the coverage area of WLANs, namely a single building (residential, office, etc.). WWANs are supported by wireless service providers. Cellular phone networks are the largest WWAN.

As long-distance wireless networks, WWANs are more vulnerable to security problems, so they should incorporate some kinds of sophisticated encryption and authentication methods to provide security.

1.2.4.1 Cellular Systems
The introduction of the cellular communication technology is one of the most successful and important developments the last decades. With billions of mobile phones in use today, this technology has a great impact on our everyday life, well beyond merely increasing mobility in telephone services. It provides the users with ubiquitous global connectivity and access to information.

Cellular networks are based on a wired infrastructure, which consists of multiple base stations (called access points) spanning a large coverage area. The base stations play a central role in the cellular networks, their main functions being: network control, dynamic resource allocation, handoff, and power control.

1.2.4.2 The Concept of Frequency Reuse
The main idea lying at the very heart of the cellular communication systems is to reuse the (limited) available frequencies many times over, hence increasing the spectral efficiency. In this manner, one can achieve a high system capacity, in terms of number of accommodated users, using a limited amount of spectrum and provide coverage over a large area.

To allow frequency reuse, the entire coverage area (e.g. a city) is divided into many spatially separated cells. Each cell has one base station (BS) of its own and a set of frequency channels. A cell's BS transmitter provides coverage to the cell area. Beyond the cell border the signal power must be low enough to avoid significant interference. Cells using omnidirectional antennas in their BS have a circular coverage area. However, circular areas are not tessellating, and hexagonal cells are usually used to model cellular networks.

Cellular architectures suffer mostly from two types of interference: intra-cell interference and inter-cell interference (ICI). The latter interference stems from cells using the

same set of frequency channels, called co-channel cells. For this reason ICI is called co-channel interference. Both intra- and inter-cell interference power levels are reduced by the use of high gain spreading codes.

The intra-cell interference is caused by imperfect multi-user transmission, such as multi-path, and power leakage between adjacent frequency channels, inside the same cell.

ICI, on the other hand, occurs between RF channels of identical frequency used in separated but closely located cells. In order to minimize ICI, cells using the same set of RF channels are separated by a minimum distance, called the reuse distance. To reduce ICI, cells are grouped in cluster patterns, in which adjacent cells are accommodated with different sets of frequency bands (RF channels). Cluster patterns are regularly repeated to cover the whole service area of the cellular network. The available spectrum of the whole cellular system is allocated, as sets of frequency bands (RF channels), to the cells in each cluster. In other words, each cluster uses the complete number of RF channels available to the whole cellular system.

Generally, cells are classified in three major types according to their size:

Macro cells: These are large cells with a radius of 5 km and more, used in sparsely populated areas.

Micro cells: These cells are limited to a radius of 500 m and are used in densely populated urban areas.

Pico cells: These are small cells used for covering small areas not easily covered by large cells. For example indoor open spaces, and tunnels. Due to their small size, the transmitting power levels are low, hence causing little interference to adjacent cells.

How to design the cluster size?

On the one hand, increasing the number of cells in a cluster (increasing the cluster area) increases the distance between co-channels and leads to lower ICI. On the other hand, a large cluster means that each cell is allocated with a smaller set of frequency channels (due to the limited number of available channels for the whole system), and hence the system capacity decreases. One way to enhance the capacity of a cellular system is to use small cells. But, in this case it will be necessary to increase the number of BSs (and additional interfaces for access to a public switched telephone network), increasing the system deployment cost. In addition, handoff from one cell to another during a conversation will be required more often.

The received signal is subject to power variations due to both large- and small-scale fading effects. The large-scale fading depends on the distance between the mobile unit and the base station. A simple model for large-scale signal propagation in a wireless channel states that the received power decays as $1/R^n$, where R is the distance between the transmitter and the receiver and n is the power path-loss exponent. In dense urban areas n may be higher than six.

The cellular systems have evolved from what is now referred to as the first generation (1G): a mobile wireless phone system based on analog signaling methods, developed in the 1980s. Since then, many improvements have been introduced, leading to sophisticated systems and the ubiquitous use of mobile phones and smartphones. The early mobile systems were independently developed without following a common standard, so that a mobile phone from one country could not be used in other countries. Cellular

standards, which emerged in the last decades, play a very important role on the development of cellular systems.

We will now proceed with a brief description of different cellular generations, and through this, introduce and discuss various concepts and characteristics of cellular systems.

First generation

The first operational cellular systems making mobile phones practical to masses were launched in early 1980s. First generation (1G) systems are voice-oriented systems based on analog modulation methods designed for voice calls only, as data services were not envisioned at the time of their emergence. 1G standards use frequency modulation (FM), FDD (*F*requency *D*ivision *D*uplex), and FDMA (*F*requency *D*ivision *M*ultiple *A*ccess). The (analog) voice signals are directly transmitted over the frequency channel allocated to each user. Channel bandwidth is 25 or 30 kHz, center frequency around 900 MHz, and data rate is rather low (e.g. up to 14.4 kbps in AMPS). AMPS (*A*dvanced *M*obile *P*hone *S*ystem) was one of the first and most common 1G systems in North America. As an analog system, 1G does not allow for data encryption (no security) and has poor sound quality.

Second generation

Second generation (2G) cellular networks were commercially launched in the early 1990s, about one decade after the emergence of the 1G systems. 2G networks are based on fully digital modulation, that is the voice is digitized and encoded to digital codes. This enabled improvements over the 1G networks: digital encryption of phone conversations (better data security), higher spectral efficiency and system capacity, and better sound quality. The development of 2G standards was motivated by two different needs in Europe and in the United States. In Europe, it was desired to enable roaming between different European Union countries, whereas in the United States the capacity of 1G systems was not sufficiently high to meet the demand in large cities. The 2G technology removed many compatibility problems and became an international standard.

GSM (Europe), TDMA (IS 136 or D-AMPS, USA), and CDMA (IS 95, USA) are the main 2G mobile technologies, where the first two are narrowband TDMA standards, and the third is a CDMA standard. Among the 2G standards, GSM was the dominant 2G technology worldwide. CDMA uses spread spectrum technology and provides better sound quality, lower outage probability, and better security.

Beside voice transmission, the 2G technologies have some limited data capabilities such as short message service (SMS) that established a new messaging platform. However, the data services in 2G are based on circuit switching data (CSD) and the data rate is rather low (up to 9.6 kbps), so that it is not suitable for web browsing and multimedia applications.

Second and half generation

The so-called "second and a half generation, 2.5G" or advanced 2G is an informal term referring to the intermediate step in the evolution of cellular technology from 2G to 3G networks. Basically, 2.5G adds packet-switching and IP support to the existing 2G cellular systems to offer increased mobile data transmission capabilities. In a packet-switching

system, the transmitted data is divided into a sequence of packets, that travel separately through the network to the destination, the path being optimized dynamically.

Packet switching allows users to share the radio resources much more efficiently because in this scheme resources are used only during data transmission and reception.

2.5G data rates are far higher than 2G networks, designed to address the demand when users started using email frequently. Although 2G systems supported text messaging (i.e. SMS), they could not provide data services as an intrinsic integrated feature.

GPRS (*G*eneral *P*acket *R*adio *S*ervice), EDGE (*E*nhanced *D*ata rates for *G*SM *E*volution), and WAP (*W*ireless *A*pplication *P*rotocol) are examples of 2.5G technologies. GPRS uses the same air interface as 2G GSM networks and provides packet-switching by adding some hardware and software upgrades.

Beside GSM, GPRS was adopted also by the IS-136 TDMA standard. It should be noted that, although GPRS was not defined as a new standard (i.e. 3G), it was a rather revolutionary step in the evolution of cellular communication networks. It was the first major step in the evolution of 2G networks to 3G, as it made data services readily available on mobile phones.

The "gap" between GPRS and 3G was mainly due to the low data rate of GPRS compared to that of the 3G systems that had been specified by the International Telecommunication Union's (ITU's) IMT-2000 by the time GPRS emerged. IMT-2000 is a set of worldwide harmonized standards for the third generation of mobile communications, initiated by ITU. IMT-2000 requires a data rate of 2 Mbps in stationary conditions and 384 kbps in a moving vehicle, whereas the theoretical maximum data rate of GPRS is 171.2 kbps.

Third generation

Third generation (3G) systems started the shift of the cellular standards to a new paradigm in which the focus is on providing an ubiquitous communication network with a wide set of data services. In other words, 3G is not merely an improvement of the voice communication, but provides data-oriented services at substantially higher data rates in a mobile environment. 3G uses packet-switching for both voice and data. It is based on ITU standards. It was also designed as an open architecture, allowing easy and quick addition of new services and technologies.

As mentioned above, the first steps for this paradigm shift were taken by 2.5G, which let users access to data networks (e.g. Internet access).

The primary goals of the 3G mobile phone standards and technologies were: increasing the network capacity by increasing the spectral efficiency, enabling high quality images and video communications, developing a variety of high-speed data services including high-speed Internet access, and providing a single global standard for all mobile networks. In addition, it allowed for new features such as symmetrical and asymmetrical data traffic, high sound quality (comparable to that of wired telephony), and the possibility to multiplex different services on a single connection. 3G mobile phones are defined by the third generation partnership project (3GPP) and are based on ITU-T standards.

3G technologies include UMTS (*U*niversal *M*obile *T*elecommunication *S*ystem), GSM WCDMA (*w*ideband CDMA), CDMA-2000, EV-DO, and HSPA. UMTS is based on GSM and proved to be the most popular 3G standard. UMTS uses WCDMA with a bandwidth of 5 MHz and can provide data rates up to 2 Mbps. CDMA2000 systems,

deployed by Qualcomm, are considered as the successor of IS-95. They use a bandwidth of 1.25 MHz and their maximum data rate is 2 Mbps.

WCDMA is based on DSSS. Its chip rate of 3.84 Mcps is higher than that of the 2G CDMA networks (called CDMAone or IS-95), that is 1.2288 Mcps, hence the notation of WCDMA. The wider bandwidth of WCDMA allows improving system performance in certain terms such as supporting higher data rates.

WCDMA supports both FDD and TDD modes.

Fourth generation

As the demand for bandwidth and higher data speeds increased beyond the 3G capabilities, a new generation became necessary, that is the fourth generation (4G), with enhanced data rate and improved QoS. 4G standards focus on providing increased system throughput, increased mobility, lower latency, and providing an Internet protocol (IP) architecture. According to some definitions, 4G will also unify cellular and wireless local area networks.

A 4G system must have a peak speed around 100 Mbps for high mobility communication, and around 1 Gbps for fixed and/or low mobility wireless access, all with premium quality and security.

To achieve high data rates, 4G uses two advanced techniques that were not used in previous generations. These are the OFDM (*O*rthogonal *F*requency *D*ivision *M*ultiplexing) multicarrier technique, and multiple input multiple output (MIMO) antenna systems.

To implement the 4G standard, two paths somewhat competing with each other were pursued in parallel: WiMAX and LTE (*L*ong *T*erm *E*volution). WiMAX is based on IEEE standards (IEEE 802.16e for WiMAX R1.0, IEEE 802.m for WiMAX R2.0), whereas LTE is based on 3GPP standards (3GPP release 8 for LTE, 3GPP release 10 for advanced LTE). These technologies are not yet capable to fulfill the high data rate requirements for 4G, and hence they are considered as pre-4G technologies. However, since the required data rates specified by 4G standards are very challenging, there is a tendency to refer them (commercially) as 4G technologies, as they present a substantial enhancement over the 3G technology. For example, LTE can theoretically reach a data rate 10 times higher than in 3G. LTE and WiMAX are both flat-IP, all packet-switching technologies, and use OFDM modulation schemes.

WiMAX is an IP-based telecommunications standard for providing fixed and mobile broadband radio access for large scale wireless networking, that is beyond offices and houses. It is a scalable platform for Wireless Metropolitan Area Networks (WMANs) offering an alternative to wired systems such as DSL (*D*igital *S*ubscriber *L*ine) and cable modems. It can support broadband real-time applications over long distances. Applications include voice over IP and wireless multimedia streaming. WiMAX combines the networking performance of Wi-Fi (IEEE 802.11 standard) with the QoS and long distance coverage of cellular systems.

Besides addressing the upsurge in the demand for broadband wireless access, WiMAX can accommodate other applications such as: (i) deploying new high speed data networks in remote areas where wired solutions are not viable, due to lack of a wired infrastructure for networks, and (ii) providing Internet services to a larger area where it can serve residential areas, mobile phones, and even Wi-Fi spots.

A WiMAX network consists of a base station (BS) or tower, and WiMAX receivers. A BS is either wire connected to the Internet, or alternatively, to another BS through a LOS MW link.

A single BS can theoretically provide coverage up to 50 km (30 miles) with line of sight (LOS) and data rates up to 70 Mbps. The frequency band 2–11 GHz is for non-line of sight (NLOS) with a range of up to 6–10 km (4–6 miles) with a fixed connection. Both the fixed and mobile standards include the licensed (2.5, 3.5, and 10.5 GHz) and unlicensed (2.4 and 5.8 GHz) frequency spectra. However, the frequency range for the fixed standard covers 2–11 GHz while the mobile standard covers below 6 GHz. Depending on the frequency band, it can be a Frequency Division Duplex (FDD) or Time Division Duplex (TDD) configuration. The data rates for the fixed standard will support up to 75 Mbps per subscriber in 20 MHz of spectrum, but typical data rates will be 20–30 Mbps. The mobile applications will support 30 Mbps per subscriber, in 10 MHz of spectrum, but typical data rates will be 3–5 Mbps.

Unlike WiMAX, LTE is backward compatible to older 3GPP standards (GSM, GPRS, WCDMA, EDGE, etc.). Advanced LTE (A-LTE) uses a relatively large bandwidth of 100 MHz and enables high mobility speeds of up to 450 km/h.

For different reasons, especially compatibility to previous standards, and including nontechnical reasons, LTE is very popular, taking the role of the dominant technology for 4G cellular networks, putting WiMAX behind, at least in Europe and North American countries.

Another candidate technology for 4G worth mentioning is the High Speed Packet Access (HSPA) that is a new version of the 3G GSM network providing data rates higher than a 3G network.

A new technology for implementing 4G that seems promising is VSF-OFCDM (*V*ariable *S*preading *F*actor – *O*rthogonal *F*requency and *C*ode *D*ivision *M*ultiplexing), that is based on multi-carrier CDMA techniques, in which the spreading code is dynamically changed in order to enhance the system capacity.

Global system for mobile communications

GSM was designed as a second generation (2G) cellular phone technology deployed in Europe since 1991. GSM was aimed at providing greater capacity compared to 1G analog systems, good sound quality, low cost, and seamless roaming within Europe. Although it was originally designed for use in Europe, it was later deployed worldwide and became a global system, as it provided the ability for worldwide roaming in a rather easy and simple fashion. GSM is a fully digital system, in which voice is digitally encoded using a vocoder.

The first GSM systems used a bandwidth of 25 MHz in the 900 MHz band: the 890–915 MHz band for the uplink (from BS to mobile), and 935–960 MHz band for the downlink. It used the Gaussian minimum shift keying (GMSK) modulation scheme, along with FDD, and a combination of TDMA and FDMA. The FDMA process consists of dividing the total bandwidth (25 MHz in each direction) into 124 RF channels of 200 kHz bandwidth. TDMA is employed to divide each RF channel into eight time slots. The time slots are allocated to multiple voice or data streams. In this manner a high capacity is achieved.

New GSM systems operate in the 900 MHz and 1.8 GHz bands in most countries (except North America). Within North America the operating frequency is 1.9 GHz.

Beside voice services, GSM supports some data services whose performance is far lower than that of 3G systems. Nevertheless, such data services were very useful at the time of the 2G era. These services were offered with the rather low user data rates of maximum 9.6 kbps, and included SMS and facsimile. SMS was developed as part of GSM standard and recorded a fast growth.

1.2.5 Access methods

1.2.5.1 Multiple access

Multiple access (MA) techniques aim to maximize the number of users that can simultaneously use a given channel of finite spectrum. In this way, more data is transmitted through the channel, and the system capacity defined as the maximum allowable number of users increases. Each technique defines the diversity scheme by which multiple users can share a communication channel, without degrading the link quality.

Over the years different multiple access techniques have been proposed and employed. The main techniques are FDMA, TDMA, and CDMA.

1.2.5.2 Frequency division multiple access

FDMA is a multiple access technique based on frequency diversity: the total available bandwidth is partitioned into frequency slots, called frequency channels. Each user is assigned a specific frequency channel, the bandwidth of which is determined according to the user's needs (data rate in digital communication, signal bandwidth in analog communication). A user transmits and receives through different channels. FDMA requires high performance filters in each receiver and transmitter. It is widely used with both analog and digital communications.

Channel impairments such as propagation delays and reflections, as well as the effect of nonperfect filtering, may cause interference between adjacent channels. To mitigate these impairments, a guard band of small bandwidth is usually introduced between the channels. Since the available bandwidth is divided to smaller bands, fading effects are lowered and if these sub-divisions are sufficiently narrow (that is smaller than the channel's coherent bandwidth), frequency selective fading can be avoided.

FDMA was used in 1G (analog) cellular systems such as Nordic Mobile Telephone, NMT (Europe) and AMPS (USA). FDMA was also used in satellite circuits to share the transponder bandwidth. FDMA is not efficient for bursty communications, such as data transmission schemes that are based on the IP, commonly used for the compression and transmission of voice, video, and data.

The strengths of FDMA include:

- Unlike TDMA, no need for synchronization in FDMA.
- FDMA algorithms are rather simple and easy to implement.
- Frequency filtering helps to avoid the near–far problem.
- No need for equalization.

Disadvantages of FDMA include:

- Needs high performance filters for channel separation.
- FDMA use is not suitable for signal compression, hence efficiency is low.
- In each sub-band only one user can transmit, not suitable for statistical multiplexing.

Orthogonal frequency division multiplexing (OFDM) and orthogonal frequency division multiple access (OFDMA) are multi-carrier, multiple-access methods that can be considered as a form of FDM. In these techniques, orthogonal subcarriers are used in order to include a large number of subcarriers in the available bandwidth, hence increasing the spectral bandwidth. OFDM uses long-duration symbols so that frequency selective fading and hence ISI problems are greatly avoided.

1.2.5.3 Time division multiple access

In TDMA, multiple access to a single channel is enabled by splitting the channel into time slots. Each user is assigned a different time slot that is cyclically repeated. Slots can be allocated to different users on demand in dynamic TDMA. During the allocated time slot, the user either transmits or receives data using the available bandwidth in its entirety. Since the users do not transmit simultaneously, interference among users is avoided in this technique. Since each transmitter is active only during its time slot, it can power down in other time slots. Thus, TDMA allows for duty cycling at low levels, yielding high power efficiency and longer battery life.

This technique is well suited for the transmission of both voice and data. Using TDMA, cellular 1G analog systems such as AMPS were upgraded to 2G digital technologies (IS-95), with an enhanced data rate.

Besides power efficiency, the strengths of TDMA include:

- More flexibility to achieve asymmetric bandwidth assignments, compared to FDMA.
- No need for frequency guard band (unlike FDMA), hence higher capacity and spectral efficiency.
- Cost-effective technology, no need for high-performing filters.
- No interference in the transmission system due to time diversity.

The weaknesses of TDMA technique include:

- Need for network-wide strict synchronization.
- Subject to multipath distortion.
- Need for guard time between different slots.
- Need for channel equalization in high speed mobile systems to mitigate inter-symbol interference (ISI) caused by frequency selective fading.

TDMA is used in many digital wireless systems such as 2G cellular networks (e.g. GSM), DECT, satellite communications, and personal digital cellular (PDC). Its practical use started in 1970s in satellite communications. In cellular communications, it was first used (and defined as standard) to implement the digital AMPS (known as D-AMPS, or TIA IS-54) in the TIA (*T*elecommunication *I*ndustry *A*ssociation) IS-54 standard, in order to increase its capacity. For this purpose, the AMPS analog channel (bandwidth 30 kHz) was divided into three time slots, yielding three digital TDMA voice channels supporting three users, and the capacity was tripled.

1.2.5.4 Code division multiple access

CDMA is a form of spread spectrum communication used in digital mobile communication systems. In spread spectrum communications the transmission of data signals is accomplished over a bandwidth much wider than the minimum bandwidth normally needed for transmitting the data signal. It should be noted that since many signals share

the same bandwidth, the average bandwidth per signal is approximately the same as in narrowband signals. Bandwidth broadening is accomplished with the same transmitting power as in the case of the narrowband signal, and hence the power spectral density of the signal is significantly decreased so that the resulting signal resembles white noise. In order to allow for extracting a desired signal in a multi-user channel, the spread signals should be uncorrelated with each other.

1.2.5.5 Why to spread?
Here are some advantages of spread spectrum techniques:

- Low power spectral density due to the very large bandwidth of the spread signal. So interference to other communications systems is rather small.
- Interference limited operation. In all situations the whole frequency spectrum is used.
- Good anti-jam performance.
- High data security due use of private distinct codes.
- Efficient mitigation of narrowband interfering signals.
- Allowing random access at any time without setup processes.

Spread spectrum techniques were first employed in military applications, due to their good anti-jamming performance: it is very difficult to jam or detect noise-like spread spectrum signals. In cellular systems, the IS-95 standard (2G) was the first system to utilize CDMA.

In CDMA systems all users can transmit and receive simultaneously, using the whole available bandwidth, without introducing much interference to each other. User separation is obtained by assigning each user a separate and unique pseudo-random code. The code is independent of the transmitted data and is used to spread the transmitted signal (narrowband) into a spread spectrum signal, and hence it is called a spreading code. The spreading codes are an essential feature of CDMA techniques. They are specific to each user and must have high autocorrelation and very low cross-correlation (ideally zero).

A main characteristic of CDMA systems is the spreading factor that is defined as the ratio between the signal's bandwidths after and prior to spreading. It is called also the processing gain, and its value is in the range of 10–1000.

The processing gain determines many parameters of CDMA systems, including the system capacity, the ability to mitigate jamming and other interference effects, and to reduce multi-path fading effects. The benefits of spread spectrum systems are more pronounced for higher values of the processing gain.

CDMA has some advantages over FDMA and TDMA schemes, including mitigation of both narrowband and wideband interferers.

Two different techniques are commonly used to produce spread spectrum signals: direct sequence (DS), and frequency hopping (FH). Combinations of these techniques are also possible.

Turning first to the DS spread spectrum (DSSS) modulation, it uses a spreading code, called the chip sequence, for converting the (narrowband) data signal to a spread spectrum signal. The chip sequence is a polar signal and its rate is much faster than the data bit rate. The codes can be either orthogonal or non-orthogonal.

In the transmitter, the chip sequence (having a very large bandwidth) amplitude modulates (i.e. multiplies) the data signal, yielding a spread spectrum signal whose bandwidth is far wider than the original signal.

In the receiver, a synchronized replica of the spreading code used by the transmitter must be used in order to de-spread the received spread spectrum signal and extract the data signal.

Hence, only a receiver who knows the spreading code of the desired signal/user, and is able to synchronize it with the transmitter's sequence can extract the data signal. The spread signals of all other users (multi-user interference) as well as any jamming signal (narrowband interfering signal) received from the radio channel and multiplied by the spreading code (uncorrelated) will be spread and hence their effects will be significantly reduced.

Hence, DSSS-CDMA mitigates, to a good extent, the effects of both narrowband interference and other users' signals. However, as the number of users increases, the effects of these interferences add up and degrade the link performance, limiting the total number of users that can be serviced.

The performance of CDMA wireless systems depends, to a great extent, on the characteristics of the spreading codes used. The spreading codes used in CDMA systems must exhibit several characteristics, including high autocorrelation and minimum (ideally zero) mutual cross-correlation. These properties are needed in order for the receiver to be able to distinguish the desired user from other users, that is to mitigate multiple access interference due to the simultaneous transmission of many signals occupying the same bandwidth. Another key requirement is to provide a big set of code sequences. The number of code sequences determines the maximum number of users that can be simultaneously serviced. Since (logical) RF channels in these systems are formed by the spreading code of each user, the number of sequences accessible within the code family used determines the total number of available logical channels.

Both orthogonal, and non-orthogonal (quasi-orthogonal) spreading sequences have been used in DSSS CDMA systems.

An orthogonal code consists of a set of mutually uncorrelated sequences, so that the cross-correlation of all pairs of code sequences is zero. Walsh codes are a set of orthonormal codes most commonly used in CDMA applications. A set of Walsh codes consists of the rows of a Walsh matrix, in which each row is orthogonal to any other row and also its logical NOT. Besides the requirement for orthogonality of spreading codes, all the users sharing the same CDMA channel must be synchronized to within a fraction of a chip (less than 1 µs). The main disadvantage of Walsh codes is the limited number of available code sequences. Because the cross-correlation between different shifts of Walsh sequences is not zero, if tight synchronization is not provided its performance will drop.

The IS-95 CDMA (2G) and CDMA-2000 (3G) standards use, respectively, 64 and 256 Walsh codes in their base stations, and hence they can provide 64 or 256 separate channels simultaneously. In practice, the number of users serviced at any given time is less than the number of RF channels because some data bits are devoted to pilot channel, synchronization and paging.

Non-orthogonal spreading codes, on the other hand, have non-zero cross-correlation values so that some amount of (multiple access) interference is produced. This degrades the signal to noise ratio (SNR), hence limiting the number of users. So, the lower the cross-correlation, the higher the number of users in the system (higher capacity). Various pseudo-random (called also pseudo-noise; PN) codes characterized as quasi-orthogonal codes have been proposed and used in wireless systems. It is a periodic binary sequence

generated using linear feedback shift register logic. A pseudo-random binary sequence appears random within the sequence length and fulfills the needs of randomness, but the entire sequence repeats indefinitely. In fact, a PN sequence is a deterministic chip stream of binary digits that appears as a random sequence.

Two types of non-orthogonal PN sequences mostly used are the maximal length sequence and the Gold codes or sequences. The maximal length sequence code, known also as the m-sequence, exhibits excellent autocorrelation properties. In these sequences, the binary digits appear randomly distributed. These codes are easily generated by means of linear feedback shift register logic, and are used in many CDMA systems. Gold codes produce more multiple access interference than m-sequences (lower orthogonality), but are preferable due to the large number of codes (sequences) they can provide. Gold sequences are generated by the sum (modulo-2) of two m-sequences in a similar fashion as m-sequences.

One serious problem with wireless systems based on DSSS is the near–far problem. This problem arises when an interfering source is located very close to a receiver whereas the desired signal comes from a far transmitter. For example in the case of cellular communications, users may be anywhere in a cell, some of them in the vicinity of the base station and others far away, resulting in a large variation in the received field strengths. Due to the non-zero cross-correlation of the spreading code, the desired data signal cannot be properly detected.

This problem is commonly solved by using fast and accurate power control mechanisms aiming to make all the signals in the channel have more or less equal power. However, some data capacity must be sacrificed for the power control mechanism, reducing the system spectral efficiency.

In the frequency hopping form of a spread spectrum, the signal is broadcast over a random series of frequencies. For this purpose, the carrier frequency hops from one frequency to another, following a pre-set sequence of frequencies within the allocated bandwidth. Typically a large number of frequencies are used and several symbols are sent during each hop.

Frequency hopping modulation can be easily implemented using a digitally controlled frequency synthesizer operated with a PN code.

In the receiver, the received signal is "de-hopped" by a PN code generator synchronized to that of the transmitter and fed to the local oscillator frequency synthesizer.

1.2.6 Transmit–receive regimes

1.2.6.1 Wireless transmission regimes (or modes)
Transmission regimes or modes describe the way data flows between nodes. It indicates the direction of information flow. There are three main modes of data transmission:

- Simplex mode
- Half-duplex mode
- Full duplex mode.

1.2.6.2 Simplex mode
Simplex radios are the most ancient type of transceivers, and as suggested by their name, operate on the same channel frequency alternating transmit and receive modes, in a "single channel TDMA" fashion. They have been disregarded for a long time with the

advent of the second and third cellular generations, and they survived mainly in military or marine applications where a central base site cannot be relied upon.

With the advent of broadband wireless systems, simplex radios working in TDD mode are reviving, due to their flexibility in bandwidth allocation and their capability to work efficiently without a supporting wireless infrastructure, which is typically missing when operating in unlicensed bands.

1.2.6.3   Half-duplex mode

In this mode a transceiver works on paired channels. As in the simplex case, receiver and transmitter do not operate simultaneously; however, the transmit and receive frequencies are different, with a large frequency separation. The reason is that, although in many systems the remote units could work in simplex mode, the base station must have full duplex capability in order to be able to effectively control the subscribers.

1.2.6.4   Full duplex mode

In this mode data can flow in both directions simultaneously, that is the channel is bi-directional at all times. This requires separate transmit and receive channel frequencies. Unlike half-duplex channels, in full duplex mode, users are not required to switch between transmit and receive modes. Phone networks (ordinary wired and cellular) operate in full duplex communication mode (simultaneous talking and listening). Full duplex mode is obviously faster than simplex mode, but its implementation is more complex and costly.

There exists also a fourth mode of data communication, the asymmetric duplex. This is a bi-directional data transmission scheme (either half-duplex or full duplex), in which the data rate in one direction is much higher than in the other direction. One example is ADSL (*A*symmetric *D*igital *S*ubscriber *L*ine) in which the data rate in the down link (DL; from the network to the user's terminal) is much higher (from 1.5 to 8.0 Mbps), than in the uplink (UL) direction (from 64 to 384 kbps).

1.2.6.5   Duplexing

In wireless transceivers (transmitter and receiver located in close proximity), the transmitting power is much higher than the receiving power (typically by several orders of magnitude), resulting in receiver blocking. This poses a serious constraint on the implementation of full duplex communication. Wireless transceivers often use a half-duplex scheme to emulate full duplexing communication.

There are two basic duplexing schemes widely used: FDD (*F*requency *D*ivision *D*uplex) that uses two different frequencies for transmit and receive signals, and TDD (*T*ime *D*ivision *D*uplex) that is based on time diversity to send and receive signals on the same frequency channel.

1.2.6.6   Frequency division duplex

In FDD, transmission from the transceiver (upstream or UL) and reception (downstream, or DL) is performed at two different frequencies, with a sufficiently wide spectral separation (a wide guard band) to minimize interference between the transmitter and receiver. Filters of high selectivity (called duplexers) are used for this purpose.

In systems using FDD, the UL and DL channels are symmetric, that is of equal bandwidth. This feature can lead to a waste of unused bandwidth in cases where the traffic is asymmetric, for example Internet access in which the amount of UL data transmission is

only a small fraction of the DL traffic. FDD provides full data capacity in both directions at any time.

1.2.6.7 Time division duplex

TDD is based on time diversity: data transmission and reception are accomplished over the same frequencies, but the transmitter and receiver are switched in time. Since the UL and DL data transfer is accomplished on the same frequency, TDD needs no guard band. In the case of symmetric traffic the spectral efficiency of FDD is superior to that of TDD, due to time wasted switching between transmission to reception periods. TDD lends itself to dynamic allocation by simply changing the number of time slots assigned to each direction. In the case of asymmetric traffic, the dynamic allocation capability of TDD results in a very small wasted bandwidth. The time delay due to switching between transmitter and receiver causes a higher latency than in the case of FDD that requires no switching.

Bibliography

1 Black, B. A.; DiPiazza, P. S.; Ferguson, B. A.; Voltmer, D. R.; Berry, F. C. (2008) *Introduction to Wireless Systems*, Prentice-Hall, New York.
2 Farahani, S. (2008) *ZigBee Wireless Networks and Transceivers*, Elsevier and Newnes, London.
3 Glisic, S. G. (2005) *Advanced Wireless Communications 4G Technologies*, John Wiley & Sons, Ltd, London.
4 Goldsmith, A. (2005) *Wireless Communications*, Cambridge University Press, Cambridge.
5 Ilyas, S. A. M. (2008) *Wimax Standards and Security*, CRC Press, London.
6 Molisch, A. F. (2010) *Wireless Communications*, 2nd edn, John Wiley & Sons, Ltd, London.
7 Mullett, G. J. (2005) *Wireless Telecommunications Systems and Networks*, Thomson Delmar Learning, London.
8 Rackley, S. (2011) *Wireless Networking Technology: From Principles to Successful Implementation*, Elsevier and Newnes, London.
9 Rappaport, T. S. (2002) *Wireless Communications – Principles and Practice*, 2nd edn, Prentice-Hall, New York.
10 Springer, A., Weigel, R. (2002) *UMTS The Universal Mobile Telecommunications Systems*, Springer, Heidelberg.
11 Srinivasa Reddy, K. A (2011) *Textbook on Wireless Communications and Networks*, Laxmi Publications, Chennai.
12 Stallings, W. (2005) *Wireless Communications and Networks*, 2nd edn, Prentice-Hall, New York.
13 Stueber, G. L. (2002) *Principles of Mobile Communication*, 2nd edn, Kluwer Academic, Dordrecht.
14 Viswanath, P. and Tse, D. (2005) *Fundamentals of Wireless Communication*, Cambridge University Press, Cambridge.
15 Viterbi, A. J. (1995) *CDMA: Principles of Spread Spectrum Communication*, Addison-Wesley, Reading, Mass.