SUBJECT

WIRELESS NETWORKS

SESSION 3 Getting to Know Wireless Networks and Technology

Case study

Getting to Know Wireless Networks and Technology

- By Lachu Aravamudhan, Stefano Faccin, Risto Mononen, Basavaraj Patil, Yousuf Saifullah, Sarvesh Sharma, Srinivas Sreemanthula
- Jul 4, 2003

Get a brief introduction to wireless networks and technology. You will see where this technology has been, where it is now, and where it is expected to go in the future.

Wireless networks have been an essential part of communication in the last century. Early adopters of wireless technology primarily have been the military, emergency services, and law enforcement organizations. Scenes from World War II movies, for example, show soldiers equipped with wireless communication equipment being carried in backpacks and vehicles.

As society moves toward information centricity, the need to have information accessible at any time and anywhere (as well as being reachable anywhere) takes on a new dimension. With the rapid growth of mobile telephony and networks, the vision of a mobile information society (introduced by Nokia) is slowly becoming a reality. It is common to see people communicating via their mobile phones and devices. The era of the pay phones is past, and pay phones stand witness as a symbol of the way things were. With today's networks and coverage, it is possible for a user to have connectivity almost anywhere.

Growth in commercial wireless networks occurred primarily in the late 1980s and 1990s, and continues into the 2000s. The competitive nature of the wireless industry and the mass acceptance of wireless devices have caused costs associated with terminals and air time to come down significantly in the last 10 years. As a result, we now have penetration rates of mobile users reaching almost 100% in countries like Taiwan, Italy, and Finland. Subscriber growth has been increasing by leaps and bounds; by mid-2002, the number of subscribers already exceeded 1 billion. The exponential growth of mobile subscribers is shown in Figure 3–1.

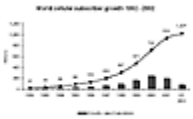

Figure 3–1 Subscriber statistics source: EMC World Cellular

The service offered on wireless networks today is primarily voice. However, the growth of data via short message services (over 24 billion messages per month, as per data in the Groupe Special Mobile [GSM] World Congress) in the last few years has been increasing rapidly. Wireless networks have evolved to the point today wherein there are two major technologies deployed today: the TDM-based GSM networks, and the CDMA-based networks. GSM networks account for about 70% of the wireless networks today. CDMA accounts for about 25% of the networks, and the other 5% are networks of other types, such as the PDC network in Japan. Many of the TDM-based IS-136 networks that were prevalent in the Americas are now transitioning to either GSM or CDMA. An example of this is the AT&T Wireless network in the U.S., which is currently rolling out a GSM/GPRS network to replace the IS-136 network; the same is the case with Cingular wireless.

The growth of wireless networks is expected to continue well into the first decade of the twenty-first century, and the number of wireless subscribers is expected to overtake the number of fixed lines within the next three years (by 2006).

3.1 Brief History

At the beginning of the 1950s, the Bell telephone company in the United States introduced a radio telephone service for its customers. This was the first instance of a radio telephony network for commercial use. However, this network was small and could accommodate very few subscribers. As the demand for radio telephony service slowly grew, it forced engineers to come up with better ways to use the radio spectrum to enhance capacity and serve more subscribers. In 1964 the concept of shared resources was introduced. This innovation allowed networks to allocate radio resources on a dynamic basis. As a result, more subscribers could be served by the radio networks.

Spectrum for radio telephony was a scarce resource (and still is), and the need to optimize the available resources to increase utilization has always been a driver in radio networks. In 1971 the FCC (Federal Communications Commission) in the United States allocated a frequency band for radio telephony. The Bell telephone company introduced the AMPS (Advanced Mobile Phone Service) radio network, thereby deploying the first cellular network. In 1982 the United

States standardized the AMPS system specification, and this became the radio telephony standard for North America.

In the 1980s several cellular radio networks were deployed around the world. In Europe each country chose its own technology for analog cellular telephony. The UK and Italy chose the American system under the name TACS (Total Access Cellular System). The Scandinavian countries and France chose the NMT (Nordic Mobile Telephone) standard. Germany chose the C-Net standard. All these were analog systems and hence considered as first-generation systems.

In 1982 the Conference of European Posts and Telecommunications (CEPT) created the Groupe Special Mobile (now known as GSM) and mandated the creation of a European standard for mobile radio telecommunications in the frequency band reserved for this purpose. This group produced the GSM standard that is widely deployed today. It also introduced digital radio telephony. Hence the second generation of mobile systems was created. In the United States, the Telecommunication Industry Association has developed two interim standards—the IS-54 standard in 1990, which is based on TDMA, and the IS-95 standard in 1993, which is based on CDMA.

Getting to Know Wireless Networks and Technology

3.2 Cellular Fundamentals

Some of the basic concepts of cellular telephony include frequency reuse, multiple access techniques, speech coding, mobility, ciphering and authentication and network planning. Cellular networks can also be considered from the perspective of being divided into the radio access network (RAN) and the core network (CN). These are discussed in the following sections.

3.2.1 Radio Access Network

The radio access network comprises of the base transceiver stations (BTSs) and the controller element, which is called the base station controller (BSC). The BTSs are basically the radio elements (RF equipment) on the network side. Mobile terminals connect to the network via the BTSs. The BTS transmits system information over channels defined for broadcastting network specific information, and mobile stations tune in to these channels before performing access functions. A BTS is connected to a cell site, which hosts antennas atop towers or buildings. Cell sites can be of type macro, micro, or pico depending

on the coverage radius. The size of a cell site is dependent on the transmit power level of the BTS. Figure 3–2 shows a generic radio access network.

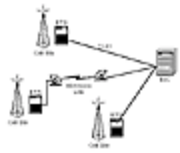

Figure 3–2 Radio access network.

The radio access network is the largest component of the mobile network, and a large number of base stations and cell sites are provisioned in order to provide coverage. Nationwide coverage of mobile networks requires the deployment of thousands of BTSs (coverage of the United States for example). The BTSs provide the channels for use on a dynamic basis to subscribers. Traffic and control channels are defined for the air interfaces depending on the type of technology used. The BTSs are controlled by the base station controller. So from a relationship perspective, a single BSC controls many BTSs. The BSC is responsible for managing the radio resources at the BTSs. The BSC assigns channels to subscribers on a need basis. In addition, it is constantly aware of a mobile station's location and the state that it is in. It measures the signal strength (with the assistance of the BTS and the MS) and makes handoff decisions. In the case of CDMA networks, BSCs are also responsible for performing the macro-diversity-combining function required in spread spectrum systems. In addition, the speech coding function may be incorporated into the BSC in some cases.

BSCs are connected to the BTSs over a wireline network using T1s and E1s. T1s and E1s are physical layer transmission technologies that are widely deployed by telecom operators. T1 is able to multiplex voice and data together in 24 user slots within a frame, as compared to E1, which has 30 user slots within each frame. Microwave links are also used for these connections. BTSs are normally deployed at the cell sites itself and hence are spread out geographically. The network connecting the BTSs to the BSC is referred to as a backhaul network. The BSC is normally at a central location such as a central office. The cost of connecting a large number of BTSs to the BSC is a major expense in radio networks.

3.2.2 Core Network

The core network consists of the mobile switching centers (MSCs), the home location register (HLR), visitor location register (VLR), authentication center

(AUC), billing servers, operation and support systems (OSS), short message service centers (SMSC), and many other elements. The interface to the public switched telephony network (PSTN) and the packet data network (PDN) is from the MSC in the core network.

The subscriber profile and the services that the subscriber is allowed to access are inserted in the HLR. The HLR is also aware of the mobile station's current location. The BSC interfaces to the core network via the MSC. A single MSC can be serving more than one BSC. Mobility management as well as communication with the HLR, VLR, and authentication centers is done via mobility application protocols such as GSM MAP or IS-41. The core network elements are connected to each other via a signaling system 7 (SS7) network, which provides the transport for signaling messages. The MSC also provides call control and switching functionality. Supplementary services, such as three-way calling and call barring, are also supported by the MSC.

For data services the core network hosts the SMSC as well as modem pools for circuit switched data. The core network is also responsible for authenticating the subscribers before allowing access to the network or access to services. Figure 3–3 shows an example core network.

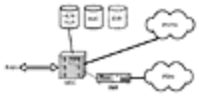

Figure 3–3 Core network.

The Interworking Function (IWF) enables circuit-switched data services in wireless networks. It consists of a modem pool and interfaces to the packet data network such as an ISP. Circuit-switched data in GSM networks is explained in further detail in Chapter 4.

A network operations center (NOC) manages the RAN and the core. An operations support system (OSS) is an element of a telecommunications network that supports the daily operation of the infrastructure. The OSS includes network management equipment, which monitors the state of the network. It also includes billing systems that are responsible for capturing the network usage by subscribers. Call data records (CDRs), which are used to bill the subscriber, are generated based on information received from the MSC by the billing systems.

Core network functionality is an involved topic; for details, please refer to texts that discuss this in detail.

3.2.3 Multiple Access

Any scarce resource that is to be used simultaneously by more than one user needs to be divided into subportions in order to prevent interference in each user's usage of that resource. In telecommunications that resource is a transmission medium and is divided into channels in order to allow multiple users to access the same transmission medium simultaneously. This simultaneous use of channels is called multiple access. A channel can be defined as an individually assigned, dedicated pathway through a transmission medium for a single user's information. The physical medium of transmission, which in our case is the wireless spectrum, can be divided into individual channels based on a set of criteria. These criteria depend on the technology that is utilized to make the distinction between channels.

The three primary technologies used in wireless cellular communication in order to separate the user channels are

- Frequency division multiple access (FDMA)
- Time division multiple access (TDMA)
- Code division multiple access (CDMA)

Figure 3–4 uses the analogy of a room as a transmission resource to illustrate these technologies.

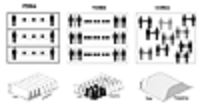

Figure 3–4 FDMA, TDMA, and CDMA techniques.

In FDMA, the channel is a specific frequency, and each user is assigned a different frequency for the duration of the call. In our room analogy, this is equivalent to partitioning the room and placing users who wish to communicate in each partition. However, due to human speech characteristics, a significant portion of the time that resource is not utilized. In other words, no information is being transmitted. This exclusive allocation results in poor resource utilization.

In TDMA, the channel is a time slot on a specific frequency, and each user is assigned a different time slot on a specific frequency. In our room analogy, this is equivalent to allowing more than one pair of uses who wish to communicate in

each partition and limit the time a pair of users can communicate without interruption. Each pair then takes turns to communicate within their allocated time period and then waits till their next turn. In TDMA, this switching between users happens so quickly that the users never perceive that they are sharing their assigned frequency with others.

In CDMA, the channel is a unique code, and each user is assigned a different code. In the room analogy, this is equivalent to breaking down the partitions and allowing all users who wish to communicate to have a conversation simultaneously. However, there is a caveat; each one of these users has to use a different language and each user has highly evolved ears that can tune out conversations that are in a language other than the one that the user understands. Thus each pair of users is able to use the room simultaneously to have a conversation without interrupting other users.

3.2.4 Frequency Reuse

Cellular systems utilize the concept of frequency reuse to provide higher capacity. The core concept of cellular systems is to reuse the same frequency in a network many times over. The ability to reuse the same radio frequency many times is a result of managing the carrier to interference signal levels (C/I). A specific radio frequency is transmitted from one base station at a power level that supports communication within a moderate cell radius. Since the power limit is controlled to serve a limited range, the same frequency can be transmitted simultaneously or reused by another base station as long as there is no interference between it and any other base station using the same frequency.

Several frequency reuse patterns are currently in use in the cellular industry. Each has its own pros and cons. The most commonly used patterns in cellular are the N = 4 and N = 7 patterns. The frequency repeat pattern determines the maximum number of radios that can be assigned to a single cell site. The N = 4 pattern can deploy cell sites with six sectors, whereas the N = 7 pattern uses a three-sector cell. Figure 3–5 shows the N = 7 pattern reuse.

Figure 3–5 N = 7 frequency reuse pat

3.2.5 Speech and Channel Coding

Speech coding is critical to digital transmission systems, and the main use for speech coding has been in wireless networks. The wireline network uses digital pulse code modulation (PCM) at 64 Kbps for voice transmission. Speech synthesis systems such as linear predictive coding (LPC) predict the current sample from a linear combination of past samples. At the expense of poor tone quality, they do achieve high efficiency. The adaptive differential PCM (ADPCM) technique is an alternate method of predicting a speech waveform from past samples.

Another class of speech coding is via algorithms termed vocoders. Vocoders are relatively complex systems and operate at low bit rates (normally 2.4 Kbps). Residual excited linear coding (RELP) is a hybrid coding scheme for wireline quality speech with a few integrated digital speech processors. CDMA uses a variation of RELP called code-excited linear prediction (CELP). The GSM speech coding scheme is based on regular pulse excitation–long-term prediction (RPE–LTP) at 13 Kbps. Enhanced variable-rate codec (EVRC) is yet another coding scheme that has higher voice quality.

Channel coding is a technique that aims to improve transmission quality when the signal encounters disturbances for reasons such as noise when the reception level is low, intereference, and multipath propogation. The side effect of this is that there is an increase in the number of bits transmitted to compensate for errors. Coding consists of adding some redundant data, which is calculated from the source information. The decoding function makes use of this redundancy to detect the presence of errors or estimate the most probable emitted bits given the received ones.

Channel coding can be classified into block codes and convolutional codes. The codes used in GSM are block convolutional codes; a fire code, which is a conventional linear binary block code; and parity codes, which are linear block codes. CDMA IS-95 systems use convolutional code based on the Viterbi algorithm.

3.2.6 Mobility

Mobility is one of the key factors of wireless networks. It allows users freedom of movement. Depending on the radio technology, mobility can be either limited

to pedestrian speeds only or can support communication even at speeds up to 120 Kmph. However, mobility places a few requirements on the network:

- They must have the ability to locate subscribers.
- They must monitor the movement of the subscribers.
- They must enable handoffs seamlessly as the user moves across cells while sessions are kept alive.

The two key concepts of mobility are roaming and handovers.

Roaming can be defined as the movement of the mobile terminal from one network to another. Network operators have coverage that is either limited in scope or is limited to a country. In order to support global mobility, network operators agree to allow subscribers from other networks to roam into their networks and access services. Roaming agreements between operators enable subscribers to roam on a global basis while being reachable all the time.

Handover is the process of switching a call or session that is in progress from one physical channel to another. Handovers can be classified into intracell and intercell. Intracell handover is the transfer of a call in progress from a channel in one cell to another channel in the same cell. Intercell handover is the transfer of the call or session to another cell.

CDMA systems are considered as make-before-break systems since the characteristics of spread spectrum allow the system to be connected simultaneously to two or more base stations. In contrast, TDMA systems from a handover perspective are termed break-before-make networks. CDMA also classifies handoffs into soft handoffs, softer handoffs, and hard handoffs.

3.3 First-Generation Mobile Networks

3.3.1 AMPS

First-generation mobile networks are analog systems. Some of the more widely deployed first-generation networks include AMPS and NMT. In this section we focus the discussion on AMPS.

The Advanced Mobile Phone Service (AMPS) is in wide use even today, almost 25 years after it was introduced. AMPS was conceived by Bell Labs in the 1970s,

and improvements in the form of digital AMPS (D-AMPS) were made in the late 1980s. The AMPS air interface is specified in EIA/TIA-553. AMPS is based on FDMA.

The FCC allocated a total of 50 MHz (25 MHz on the A side and B side) in the 800-MHz spectrum for AMPS. Each voice channel is allocated a 30-KHz portion of the bandwidth within the AMPS frequency allocations. Because each carrier has 25 MHz of spectrum, this provides a total of 832 (25 MHz/30 KHz) cellular channels (forward and reverse). However, since the same frequency cannot be used in adjacent cells, the 416 duplex channels are a theoretical maximum (actual number of valid voice channels equals 312). AMPS uses the seven-cell frequency reuse method. Control channels are used to set up and clear calls as well as other control messages. Each band (25 MHz) contains 21 control channels. When a mobile station is not in session, it must monitor designated control channels. It tunes and locks into the strongest channel to receive system information. The forward control channel (FOCC) is a data stream from the base station to the mobile, and the reverse control channel (RECC) is from the mobile to the base station. Voice conversation is carried over the forward voice channel (FVC) and the reverse voice channel (RVC).

The identifiers used in AMPS are as follows:

- The mobile station's electronic serial number (ESN)
- The mobile operator's system identification (SID)
- The mobile station's mobile identification number (MIN)

The ESN for a mobile is a 32-bit number that uniquely identifies a mobile and is set up by the mobile manufacturer. System IDs (SIDs) are 15-bit binary numbers that are assigned to cellular systems. One of the uses of the SID is to determine a home network from a roaming network. The MIN is a 34-bit number that is derived from the mobile terminal's 10-digit telephone number.

The network utilizes the IS-41 protocol for mobility and authentication procedures. The MSC provides the capability for call processing, and the HLR and VLRs keep track of the mobile as it moves. The mobile terminal is responsible for updating its location as it moves in the cellular network.

Data services in AMPS are straightforward and analogous to dial-up networking. Because AMPS is an analog technology, it is possible to make use of standard modems directly with AMPS. Data rates are at a maximum of 14.4 Kbps irrespective of the modem protocol (v.90 or others).

3.3.2 D-AMPS

D-AMPS, or digital AMPS, is a hybrid air interface that uses both first-generation and second-generation technology. The D-AMPS specification is detailed in IS-54-B. The primary reason for introducing D-AMPS in the early 1990s in North America was to overcome some of the shortcomings of AMPS technology. The co-channel interference problem of AMPS limited its capacity significantly, and the 30-KHz channel assigned to each user is excess capacity on a per user basis. The hybrid nature of D-AMPS comes from the fact that second-generation TDMA technology is placed on AMPS traffic channels.

The AMPS channels are still used, but the content and formats of the 30-KHz channels are modified. The channels defined for D-AMPS are as follows:

- FOCC—Forward analog control channel; direction: base station (BS) to mobile station (MS) control channel
- FVC—Forward voice channel; direction: BS to MS voice channel
- FDTC—Forward digital traffic channel; direction: BS to MS digital user and control channel
- RECC—Reverse analog control channel; direction: MS to BS control channel
- RVC—Reverse analog voice channel; direction: MS to BS voice channel
- RDTC—Reverse digital traffic channel; direction: MS to BS digital user and control channel

The FDTC and RDTC can be split up into fast associated control channel (FACCH) and slow associated control channel (SACCH), which are used for signaling. One of the improvements that was made in the handoff process was the involvement of the mobile in the handoff procedure. Mobile assisted handoff was introduced in D-AMPS. The MS keeps measuring the quality of the

forward channel and sends these measurements to the BS to allow the network to make a more informed decision.

First-generation AMPS and D-AMPS mobile networks continue to exist even today, especially in the United States. They complement coverage of second-generation digital networks such as GSM and IS-95. Most mobile terminals are dual mode (i.e., they incorporate a second-generation (2G) digital radio as well as the analog radio). With roaming agreements in place, 2G network operators can claim nationwide coverage. However, it is expected that the lifetime of these analog networks is coming to an end and will be decommisioned slowly in the next few years. One of the reasons for decommissioning these networks is to reclaim the spectrum for other uses.

3.4 Second-Generation Mobile Networks

Second-generation mobile networks are a step up in technology evolution. 2G networks, as they are commonly refered to, are digital networks. There are several 2G technologies that have been deployed across the world. The most widespread deployment is, of course, the TDMA-based GSM system and the CDMA-based IS-95 system. Other 2G technologies that have been deployed include DECT (Digital European Cordless Telephone), IS-136, and the PDC-based personal handyphone system (PHS) in Japan.

The following sections will take a closer look at the GSM and CDMA networks and technology.

3.4.1 -GSM (Global System for Mobile Communication)

GSM is a TDMA-based wireless communications system. Work on the GSM specifications started in the 1980s in Europe as a result of the capacity limits being experienced by analog networks such as NMT.

The GSM 900 system uses two 25-MHz bands for the uplink and downlink, and within this spectrum 200-KHz channels are allocated. The uplink and downlink are separated by a 45-MHz spacing. GSM 1800 uses two 75-MHz bands for the uplink and downlink. Again 200-KHz channels are allocated within those bands and are separated by a 95-MHz spacing. The 1900-MHz systems use two 60-MHz bands for the uplink and downlink using 200-MHz channels within those bands and separated by 80-MHz spacing.

STANDARDS

Europe felt the need for a common mobile telephony standard since different countries had differing analog networks, and as a result roaming of subscribers between these networks was not possible. CEPT (Conference European des Postes et Telecommunications) is a standardization arena in Europe. A new group called GSM (Groupe Special Mobile) was formed within CEPT in 1982 whose task was to specify a unique radio communication system for Europe at 900 MHz. The timeline in Figure 3–6

Figure 3–6 GSM standards timeline.

GSM TOPOLOGY

The topology and network architecture of GSM is shown in Figure 3–7.

Figure 3–7 GSM network architecture.

The mobile station (MS) is the terminal (phone, PDA mobile unit) provided to the subscriber. It is essentially a GSM two-way radio that conforms to the air interface specifications.

The base station subsystem is functionally subdivided into the base station controller (BSC) and the base transceiver station (BTS). A single BSC normally controls a large number of BTSs. BTSs contain the radio equipment and are connected to cell site antennas. The BTS is essentially a layer two bridge if viewed from a high-level perspective. It provides an entry point for the subscribers who are present in the cell, allowing them to make or receive calls. Some of the base station functions are radio transmission in GSM format, use of frequency hopping techniques, coding and decoding of radio channels, and measurement of quality and received power on traffic channels.

The BSC is a much more complex system. It is responsible for managing the radio resources in the network as well as control handovers. So the BSC has functionality of mobility management, radio resource management, call control, management of intercell handovers, and other housekeeping tasks.

Table 3–1 MAPInterfaces

Network Elements Connected	**x**	**Map**
MSC	VLR MAP	B
MSC	HLR MAP	C
HLR	VLR MAP	D
MSC	MSC MAP	E
MSC	EIR MAP	F
VLR	VLR MAP	G
AuC	HLR MAP	H

The mobile switching center (MSC) is the centrallized controller of the network. The MSC is a switch that provides call control capability. It also interfaces to the PSTN. An MSC that interfaces to the PSTN is called a gateway MSC (GMSC). The MSC also is responsible for tracking the user as he or she moves between networks. So it plays a role in mobility management as well.

GSM uses two databases, called the home location register (HLR) and the visitor location register (VLR). The HLR contains the subscriber's profile information (which is static) as well as the current location of the subscriber (i.e., it knows the reachability information of the subscriber). The VLR stores the current location or point of attachment to the network and the state of the mobile terminal. For mobile terminated calls, the HLR is the initial signaling contact point in the

mobile network, whereas the VLR is the initial signaling contact when the call originates from the mobile.

The authentication center (AuC) is a database that stores confidential information, such as keys associated with valid subscribers. The AuC is responsible for authenticating a subscriber. When subscribers attach to the network, the network performs an authentication procedure for the subscriber. The keys associated with the subscriber are utilized in conconjunction with an algorithm to validate the authenticity. The secret key associated with the subscriber is stored on the subscriber identity module (SIM).

Frequency Hopping Spread Spectrum (FHSS)

Frequency hopping is one of the spread spectrum techniques used in the IEEE 802.11 standard. This is one of the transmission mechanisms of the physical layer. The technique involves the breakup of a wide band of frequency into smaller bands. Then the transmitter "hops" in each of the smaller bands, in a predetermined pattern. The receiver knows this hopping sequence and can lock on to the frequency to receive information. The transmitter and the receiver constantly change patterns using the agreed-on hop sequence; thus, interference is avoided as the transmitter and receiver keep hopping around the smaller bands of frequency over a wide range of frequencies. Interference from narrowband applications (such as garage door openers) will occur only in a specific band for a certain period of time.

The 2.4-GHz frequency spectrum that is available for use is divided into several 1-MHz frequency bands. The transmitter and receiver hop from one 1-MHz frequency band to another, in a near-random sequence. The transmitter will send data in each of the 1-MHz frequency bands, and if the receiver is locked onto the appropriate 1-MHz band, it should be able to receive the information from the transmitter.

The amount of time spent by the transmitter or the receiver in a 1-MHz band is referred to as the dwell time. Typically, any narrowband interference is limited to the dwell time in each band.

Direct Sequence Spread Spectrum

In DSSS the transmitter and the receiver agree on a digital code. The transmitter takes the typically narrowband input signal and spreads or transforms it into wideband by applying the selected code. Each input bit is replaced by the code, resulting in wideband. The receiver applies the same digital code to the received signal and, when properly synchronized, retrieves the input bits transmitted.

DSSS systems are complex to build and provide inherent security due to the transformations performed (i.e., codes used). They have the ability to provide higher data rates when compared to FHSS systems, as most of the FHSS systems are required to use around 1-MHz of bandwidth at any time. In the IEEE 802.11 DSSS system, an 11-bit code called a Barker sequence is used to transform the original data bits. The resulting transformed bits are modulated to send over a carrier frequency using one of two modulation techniques: differential binary phase shift keying (DBPSK) or differential quadrature phase shift keying (DQPSK).

INTERFACES

Four main interfaces are defined in GSM networks:

- Um Interface—Between the MS and the BTS
- Abis Interface—Between the BTS and the BSC
- A Interface—Between the BSC and the MSC
- MAP-x—Between the MSCs as well as between MSC and HLR/ VLR/AuC.

The Um interface uses a combination of FDMA and TDMA access techniques. One hundred twenty-four full-duplex channel pairs are defined that operate with different carrier frequencies. Each of these FDM channels uses TDMA slots.

The Abis interface connects the BTSs with a BSC. The Abis interface has normally been implemented as a proprietary interface. The physical layer is defined by a 2-Mbps PCM link, and the datalink uses LAPD.

The A interface is an open interface that connects the radio access network (RAN) to the core network. The A interface links multiple BSCs to an MSC. It is the open nature of this interface that makes it possible to connect equipment made

by different vendors. The A interface functions include call control and mobility signaling.

THE SUBSCRIBER IDENTITY MODULE

The SIM is a personalized part of the mobile station and operates along with a memory card. The SIM identifies the subscriber. The mobile station is simply a piece of radio equipment and becomes associated with a subscriber only as a result of the SIM being inserted into the terminal. The SIM provides the security needs of the operator and the subscriber.

With the SIM concept, a subscriber is not tied to any specific mobile terminal. A subscriber can use different terminals. As far as the network operator is concerned, a subscriber is identified by the SIM. It identifies the account owner and can be modified or subscription options changed. The key functionalities afforded by SIM are subscriber authentication, secure location for secret keys at the subscriber end, processing capability for executing the authentication, and ciphering algorithms.

MOBILE APPLICATION PART

MAP is a protocol used in GSM core networks on various interfaces. MAP can be denoted as MAP-x, where x can determines the interface. The interfaces where MAP is used are shown in Table 3–1. Functionalities associated with each of these interfaces are defined in the specifications for MAP in GSM 09.02.

3.4.2 CDMA IS-95

CDMA is a relatively new technology in the mobile cellular industry. Commercial networks were first deployed in the mid-1990s. However, they are growing rapidly and they account for about 25% of the wireless networks globally.

The CDMA standard referred to as IS-95 is specified by TIA/EIA.

SPREAD SPECTRUM

The wireless spectrum is a scarce resource, with tight regulations in terms of usage and power radiated along with licenses required to operate. This is true for most of the wireless systems in place. Interference is an issue that wireless networks must contend with.

Spread spectrum is one of the techniques employed that inherently is less sensitive to interference. Spread spectrum techniques typically use more bandwidth than necessary to transmit and receive bits.

Spread spectrum techniques inherently offer more privacy than narrowband techniques, as they are more difficult to intercept or spy on. They use a code, which is known only to the transmitter and the receiver. Spread spectrum techniques can also coexist with other technologies as the transmitter and receiver can obtain information as long as they are decoding with the same code.

There are two popular spread spectrum techniques. The first is frequency hopping spread spectrum (FHSS), where the transmitter and the receiver hop in a predetermined sequence through a wide band of frequencies.

The second technique is direct sequence spread spectrum (DSSS), a mechanism in which data bits are transformed by codes, which in turn occupy a wide band of frequencies. This technique is already in use in public wireless networks such as IS-95 (or CDMA, as it is popularly known). DSSS is a technique wherein the carrier is modulated by a digital code in which the code bit rate is much larger than the information signal bit rate.

The DSSS system is a wideband system in which the entire bandwidth of the system is available to the user. The user data is spread using a spreading signal refered to as the code signal. The code signal or the spreading signal has a much higher data rate than the user data rates; for example, the 1.2288 MCPS in CDMA vs. user data rates that are much lower. At the receiving end, despreading is accomplished by the cross corelation of the signal with a synchronized replica of the same signal used to spread the data. In CDMA systems pseduorandom noise (PN) sequences are used to spread the bandwidth and distinguish among various users' signals. PN sequences, as the name suggests, are not random but rather deterministic.

ARCHITECTURE AND CHANNELS

The CDMA architecture is based on the reference model from the cellular standards group TR-45. Structure of the standards organization is discussed in Chapter 16. The main elements of the reference architecture are as follows:

- Base station—The base station is the BSS equivalent in GSM networks. The BS consists of the BTS and the BSC. The functionality of the BTS and BSC is similar to the functionality of these elements as described in "GSM Topology" (p. 53).

- Mobile station—The mobile station is the terminal that is a transmitter and receiver.

- Mobile switching center (MSC)—The MSC is the switch that provides call control functionality, mobility, and the trunking interface to the PSTN.

- Home location register (HLR)—The HLR is attached to an MSC and maintains the subscriber's profile information as well as the current location of the user in the network from an attachment perspective.

- Vistied location register (VLR)—The VLR is attached to an MSC and stores the subscriber information that is obtained from the HLR on a dynamic basis or as long as the user remains within the area served by that MSC.

- Authentication center (AC)—The AC is responsible for maintaining the keys associated with a subscriber and performs authentication of subscribers when they register with the network.

- Operations support, billing systems, interworking function—Other elements that have the same functionality as described in Section 3.2.2.

IS-95 channels can be segmented into physical channels and logical channels:

- Physical channels—Physical channels are defined in terms of an RF frequency and a code sequence. There are 64 Walsh codes available for the forward link (BS-MS) providing 64 logical channels. On the reverse link channels are identified by long PN code sequences. In IS-95, CDMA carrier band center frequencies are denoted by AMPS channel numbers. One CDMA carrier requires 41 30-KHz AMPS channels to provide a CDMA carrier bandwidth of 1.23 MHz. The 1.23-MHz bandwidth of a CDMA carrier makes the minimum center frequency separation between two carriers at 1.23 MHz.

- Logical channels—Logical channels can be further subdivided into control and traffic channels. The control channels and traffic channels in IS-95 are as follows:

  Pilot channel (downlink)—The pilot channel is transmitted continuously by the base station on each CDMA frequency and is used to provide a reference to all mobile stations.

  Paging channel (downlink)—The paging channel is used to transmit control information to the mobile station. In order to terminate a call, the network pages the mobiles in an area on the paging channel.

  Sync channel (downlink)—The sync channel is used along with the pilot channel to acquire initial time synchronization.

  Access channel (uplink)—The access channel is used by the mobile to transmit control information to the base station. Many messages can be carried on the access channel. When a mobile originates a call, it uses the access channel to inform the base station. This channel is also used to respond to a page.

  Forward traffic channels—These channels are grouped into rate sets. Rate sets identify the voice coding scheme that can be used on any channel.

  Reverse traffic channels—User traffic on the reverse channel is identified by a user-specific long code sequence based on the user's ESN.

INTERFACES

IS-95 uses the following interfaces:

- A Interface (BSC-MSC)—This interface is between the BSC and the MSC. It supports both the control plane and user plane.
- Abis Intreface (BTS-BSC)—This is the interface between the BSC and the BTS. This is an internal interface and generally proprietary.
- B Interface (MSC-VLR)—This interface is defined in TIA IS-41.
- C Interface (MSC-HLR)—This interface uses IS-41 messaging as well.

- D Interface (HLR-VLR)—HLR-VLR signaling is based on IS-41 as well. It sits on top of SS7.
- E Interface (MSC-MSC)—Inter MSC signaling is defined in IS-41.
- H Interface (HLR-AC)—The interface that is used for authenticating a subscriber is defined in IS-124.
- L Interface (MSC-IWF)—This interface allows the ability for circuit switched data in second generation networks.
- Um Interface (BS-MS)—This is the air interface between the mobile and the network.

IS-41

IS-41 is standardized by the Telecommunications Industry Association (TIA). Revision C is the latest version of the protocol and is called IS-41C. IS-41 is the core networking protocol that supports mobility, authentication, and roaming. IS-41 allows network equipment to be multivendor. Since the equipment has to conform to the standard interface, it is possible to have an environment wherein MSCs are from vendor A and the BSC/radio network is from vendor B.

IS-41C is an application-layer protocol. IS-41 normally is operated over SS7 networks, which provide the reliability required for signaling.

Roaming between networks that use GSM MAP and IS-41 requires the use of gateway functions that convert messages from one protocol to another. Such gateways can be considered protocol translators.

3.4.3 GPRS (2.5G Network)

General Packet Radio Service (GPRS) is an enhancement to GSM networks with support for packet radio. GPRS overlays a packet-based air interface on the existing circuit switched network. It also introduces a packet core aspect primarily for data applications. Packet switching allows radio resources to be shared efficiently by a large number of users since radio resources are allocated if there are data to send or receive. GPRS network architecture as well as the enhancements to the air interface are covered

3.6 Summary

This chapter provided a brief introduction to wireless networks and technology. Wireless networks today are primarily based on either TDMA or CDMA technology. Second-generation networks support voice as the main application. However, in recent years, the use of SMS has taken off on a large scale and hence SMS as a data service is becoming synonymous with these networks. It is expected that third-generation networks will offer even greater bandwdith for data applications. While third-generation networks will enhance the capacity for carrying voice, they will also be driven by the need and support for data applications.