Cellular Communication Networks

by Gerald Williams

in partial fulfillment of the term project requirements for

ECE 404, Computer Networks, at Lehigh University

12/8/95

Table of Contents

Abstract

Cellular phones have revolutionized communication. With one, you never have to worry about being stranded on the side of the road. You can conduct business on the way to work. You can call your spouse to say you're stuck in traffic and will be late. And these are just the benefits of *car* phones. Portable hand-held units are quickly replacing car phones as the cellular phones of choice, and many have the goal of replacing telephones entirely with individual *personal communicators*. This would enable people to have their own personal phones with them at all times and could eliminate the distinction between work, home, and car phones (for those that want the distinction eliminated, at least!).

Cellular networks are a relatively new form of communication, and are rapidly evolving, as coverage is expanded both in terms of network area (reachability) and number of users (capacity), new services are added, and existing analog cellular systems are replaced by digital ones. Several divergent types of cellular networks have developed over time. The basic operations performed by all cellular systems are the same however, and they all face the same challenges, so many of the same or similar implementation methods are used in all cellular systems.

There are a number of standards in cellular communication: some compete with each other, others work together. Standards are important to allow ubiquitous service, although the choice of standards is often made in the political (as opposed to the technical) arena. Standards define the current state-of-the-art in cellular communication, and must adapt to changing needs and technology in order to survive.

The current trend in cellular networks is to provide smaller phones with longer battery lives while cellular providers increase their overall coverage (in terms of both area and users). Despite the fact that it is sometimes at cross-purposes both to decreasing battery life and to increasing capacity, there is growing support for making substantial service improvements that may radically alter the nature of cellular service in the future. *Personal Communications Services*, or *PCS*, will likely be a driving force behind many of these changes.

Overview

The purpose of this report is to summarize the current state of cellular communication networks. It is intended for a reader that understands the basics of communications (such as the notions of time-division and frequency-division multiplexing). Such knowledge should not be needed to gain some understanding about cellular networks by reading this report, however.

The report starts by providing some background about what comprises a cellular network and how cellular networks fundamentally operate. It then details some of the challenges facing designers of cellular systems and describes what some of the important standards do to overcome them, before returning to cellular operation to discuss the operational domains of cellular networks and some of the details of how they are implemented. Finally, it summarizes some of the current trends in the cellular communication industry.

Introduction to Cellular Networks

Cellular networks got their name because of the way they divide service areas into *cells*. A cell is a relatively small area that is serviced by a single transmitter/receiver unit (often called a *cell site*). Mobile phones operating within this area use that cell site to communicate with the rest of the cellular network (and with the public phone network).

The basic premise of a cellular network is that you can have a communication device that you can take with you, starting with car phones which have evolved into hand-held phones. Over time, hand-held phones have been getting smaller, gaining longer battery life, and getting new features like paging. Network coverage and capacity have also increased to the point where cellular service is available almost anywhere and at any time to those that want to use it.

Cellular service has seen tremendous acceptance, especially in the last few years, with millions of new subscribers each year and the new subscriber rate growing. Conservative estimates predict that half a billion cellular phones will be in service by the end of the next decade, although the number may be well over a billion if recent estimates by European cellular providers are correct.

History of Cellular Service

Cellular service was invented by Bell Laboratories and introduced around 1980, based on radio-telephone systems that dated back to the 1940's. The Bell Labs offering became the basis for the *Advanced Mobile Phone System* (*AMPS*), which is the current standard for U.S. cellular service. It is the least common denominator of U.S. cellular service, and the FCC has mandated that all U.S. cellular phones must fall back to AMPS service at least until the year 2002.

Many other nations adopted variants of AMPS service, such as *Nordic Mobile Telephone* (*NMT*), first introduced in Scandinavia, *Total Access Communication System* (*TACS*), first introduced in Britain, and other systems introduced in France, Italy, and Germany. The protocols and communications standards used by each of these varied slightly, so that the various European analog systems were not compatible with each other.

The Evolution of Cellular Service

Most U.S. cellular service still uses the same AMPS analog technology that was used in the earliest mobile telephones, although digital cellular service is rapidly gaining popularity. The key motivator for this is that digital cellular networks can offer more subscriber channels over the same radio bandwidth, although digital networks can offer additional services as well.

Unlike ISDN, ATM, and other innovations in regular telephony, cellular systems have less infrastructure to be replaced when new ideas are developed. Coupled with the rapid growth of cellular service, it is possible to make sweeping changes in the basic nature of cellular service. In fact, it is perhaps too easy to change, causing much debate over what the cellular network of the future should look like. A large division is over whether to use *time division multiple access* (*TDMA*) methods over existing analog frequencies or to use spread-spectrum *code division multiple access* (*CDMA*) methods. One thing that is certain, however, is that cellular service is quickly going from analog systems to digital systems.

Digital Cellular Service

Europe was the first to embrace digital service with the *Global System for Mobile communication* (*GSM*). The incompatible existing analog systems in the 1980's made it impossible to use a single mobile phone in several European countries. With the European Union and increased trade and commerce throughout Europe, a need was seen for a single European standard. To choose one of the existing standards would have given an unfair advantage to those that already provided that service, so it made sense to create an entirely new service that could take advantage of technological advances since the advent of cellular service. Thus, the Groupe Speciale Mobile, a CCITT/ETSI committee, was formed. It established the GSM standard in the 1980's; GSM was first implemented in 1992-1993. This all-digital standard became the least common denominator of service in Europe, and is quickly replacing the analog systems currently in place.

U.S. digital systems have also recently emerged, with IS-54 (also called D-AMPS or U.S. TDMA) systems already in place, soon to be replaced by IS-136 systems (the successor to IS-54). There is also one major cellular service provider that is putting a competing system in place called IS-95 (or U.S. CDMA). There are also two important Japanese digital standards, the *Personal Handiphone System* (*PHS*) and *Personal Digital Cellular* (*PDC*), which both use TDMA like IS-54/136 and GSM.

Personal Communications Services

There is a great deal of talk about *Personal Communications Services*, or *PCS*, which are being developed now. The FCC recently auctioned off 160 MHz of radio spectrum for PCS services, which it defined as *a broad range of radio communication services freeing users from the limitations of wired phone networks*. These are essentially cellular phone systems, although the intent of PCS systems is not to *supplement* the existing phone system but rather to *become an integral part of it*. PCS systems do not exist yet, so they cannot be defined, although they are likely to make use of one or more of the existing digital cellular standards (GSM, IS-54, IS-95, PHS, or PDC) for wireless access.

The first specification for a "Personal Communication Network" was actually made in 1990 based on the GSM cellular standard at the request of the United Kingdom. It became part of the GSM standard, which includes GSM-900 (the cellular standard) and DCS-1800 (the PCN standard). A variant, PCS-1900, is one of the contending standards for PCS service in the United States. There is still some work needed to create a viable PCS standard, however. Sound quality needs to be improved in order for people to consider switching, and perhaps new services are needed to lure customers as well.

Basic Network Operations

Traditional mobile phone service has used only terrestrial radio. In other words, it relies on ground-based cell sites, which are usually small towers with three antennae arranged in a triangle. Satellite implementations are possible, although they cannot use radio bandwidth as efficiently. Thus, they are used commercially primarily for pager, broadcast, and some specific site-to-site links.

A cellular network is designed to connect to the existing phone system (also called the *Public Switched Telephone Network* or *PSTN*) or potentially to a data network (called a *Public Data Network* or *PDN*). The connection to the PSTN is not much different than the connection of other telephone switching equipment such as a *Public Branch Exchange* (*PBX*).

Cellular networks are comprised of terminals and base stations. Terminals are the end-user equipment, usually phones, and are often called *Mobile Stations*. Everything else in a cellular network is considered to be *base station* equipment.

Terminals

There are three types of cellular terminals. Each type has different output power restrictions, based on how near the antenna is to people when it is in operation. They are summarized in the following table.

Type	Output Power
Portable (hand-held)	less than 0.6 Watts
Mobile (car or "bag" phones)	less than 3 Watts
Fixed	no fixed limit

Table 1: Types of Terminals

Fixed installations might be used in dwellings that cannot be reached via land lines or where land lines would be impractical. These are not too power-constrained, although the vast majority of terminals face strict power constraints. In addition, portable phones and many "bag" phones are usually running on very limited battery power. Therefore, it is important that most terminals use power, especially transmit power, very efficiently.

Most terminals are extremely cost-constrained as well. The sheer number of consumers and competitors in the market is the primary reason for this (many cellular providers give away terminals free in order to attract subscribers). When the basic requirements for the GSM standard were written in 1985, there was even a specific requirement that "the system parameters shall be chosen with a view to limit the cost of the complete system, in particular the mobile units."

Thus, the design of cellular terminals is a difficult challenge. Although they must be able to deal with almost all aspects of cellular communication (for a single consumer), they must do so in a single small, cheap, low-power box.

Base Stations

There are three components of base stations. The *cell sites*, which are often referred to as *base transceiver stations* or *BTSs*, communicate directly with the end-user terminals. *Base station controllers* or *BSCs* control the base transceiver stations either over land links (typically) or over radio links. *Mobile switching centers* or *MSCs*, often called *mobile telephone switching offices*, control the base station controllers, usually over land links. There is no fixed ratio of BTS to BSC to MSC, although there are typically about five to ten BTSs per BSC and anywhere from one to ten BSCs per MSC, depending on the capacity needs and geographic distribution of an area. In fact, base station functions may be combined into a single site, especially in the more remote areas where a single site might serve as BTS, BSC, and MSC.

The following figure demonstrates six cell sites communicating over radio links to two base station controllers, which in turn communicate with a single mobile switching center that is connected to the public switched telephone network (the "regular" phone company).

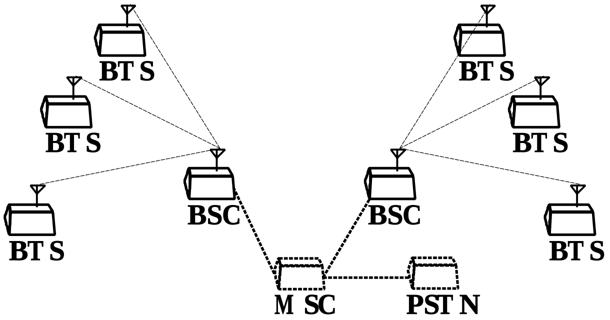

Figure 1: Base Station Organization

Cell sites have one antenna up for transmitting to the terminals and two down for receiving from the terminals: the two down antennas allow it to work like a bigger antenna and help counter multipath effects (which are described later). They generally operate around 900MHz, though other frequencies are also used (especially for PCS). BSC-BTS communication uses a low-speed link (which is why it may be a radio link). MSC-BSC and PSTN-MSC communication is at a much higher rate (and use land-lines).

One reason the link rates are higher closer to the PSTN is that each level of communication may deal with more customers than the next lower one. However, the link rates are also higher because of the nature of the channels. When communicating with the "regular" phone company, telephony signaling mechanisms are used. This includes 64 kbps pulse code modulated channels and additional signaling mechanisms like SS-7 and IS-41. These are beyond the scope of this report, although they use a much higher bit rate than the rest of the cellular network. MSC-BSC communication uses lower bit-rate but still uncompressed data channels (which simplifies the design of the MSC), while BSC-BTS communication uses compressed data channels (which simplifies the design of the BTS).

As can be seen by examining the type of data carried between them, the three types of base stations each perform different types of operations. Rather than performing all cellular operations in a single unit, base stations divide the operations and perform them where they make the most sense. The cell sites perform operations that need to be done independently on each channel while the base station controllers and mobile switching centers can perform certain operations on multiple channels simultaneously.

Cell Organization

Cellular communication got its name because of the "cell" structure of the base transceiver station service areas. For convenience, a service area is often subdivided into an array of hexagonal cells, each containing a single BTS. As the industry is maturing, the service areas of individual BTSs are being calculated more precisely (including such considerations as reflections off buildings) and they are being placed where they can be the most effective rather than in traditional "cells", although the term "cellular" is still used.

The arrangement of the cells is basically a form of *space division multiple access*, since frequencies can be reused by other cells that are far enough away not to interfere with the current cell. The degree of reuse (determined by how far apart cells must be to reuse the same frequency) is dependent upon the actual implementation of the radio link.

Traditional AMPS-type cell sites are called *macrocells*. These are spaced anywhere from 3 to 60 km apart (averaging around 6 km), depending on population density, terrain, or other factors. Newer networks are adding *microcells*, which are smaller cells (perhaps as close as a few hundred feet apart) that can be used for spot coverage (e.g., near a tunnel) or to increase the level of SDMA, thus adding capacity. Both macrocells and microcells are part of a service provider's network.

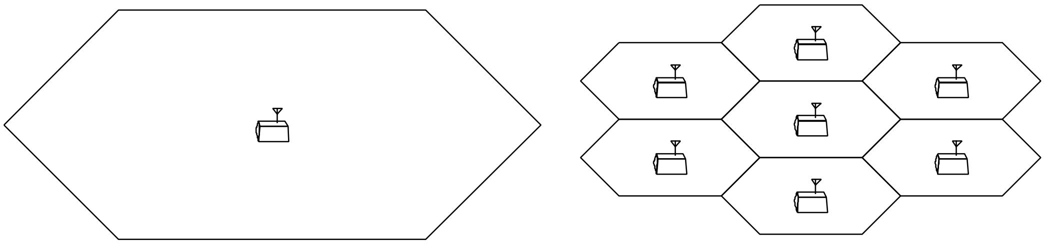

Figure 2: Macro-cells versus Micro-cells

Another type of cell is a *picocell*. Picocells are just small microcells, although they need not be part of a service provider's network. Individual buildings or even floors within a building can use picocells to have their own cellular service. For example, a company could provide local cellular service to its employees without paying per-minute airtime charges to a service provider.

It is also possible to have hybrid arrangements, with microcells and picocells existing inside of macrocells, as is shown in the following figure.

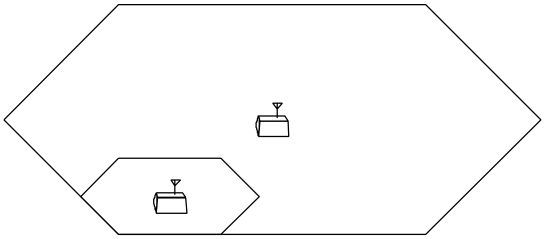

Figure 3: A Micro-cell within a Macro-cell

Challenges of Cellular Communication

Cellular networks must deal with all of the challenges of traditional telephony, such as call setup, switching, and so on. However, cellular networks must face additional challenges due to the mobile, wireless nature of the terminals. They also have to deal with many types of signal corruption caused by sending the signals through the air.

Network Routing

Many of the cellular network routing issues can be attributed to the multiple access methods that are used, although cellular networks also have to deal with discontinuous communication and may have special issues regarding billing, tariffs, and the like.

All cellular networks use two or more multiple access methods to send multiple signals over a single broadcast medium. The reuse of given frequencies in different cells is a form of *space division multiple access*, and it requires that the location of each terminal be known. This is provided through a service known as *location management* (or *mobility management*), which is not simple since terminals may move from cell to cell during a single call (this is called *handover*) and may even operate in an area covered by a different service provider (this is called *roaming*). Calls should not be dropped during *handover*, even when changing service providers, and *soft handover* should be used versus *hard handover* if possible (in *soft handover*, the terminal can continue to use the same channel when communicating with both cell sites rather than having to quickly switch to an entirely different communication channel).

All cellular networks also make use of *frequency division multiple access*. Radio frequency is usually assigned to cellular communication in 50 MHz (or sometimes 70 MHz) blocks. These are divided into an equal number of uplink (terminal to base station) and downlink (base station to terminal) bands. There can be anywhere from 10 to 900 pairs of bands, and each band pair carries one or more bidirectional channels (it is easiest to consider both the uplink and downlink as a single channel; that convention is used in this report).

The digital networks additionally make use of either *time division multiple access* or *code division multiple access* methods to place additional channels over the limited radio bandwidth. Time division multiple access systems put several lower-speed channels into a faster channel by dividing the faster channel in time into multiple frames. Code division multiple access systems encode or *spread* multiple channels in such a way that they appear as noise to the other channels but can be clearly distinguished from the others when properly decoded (or *despread*).

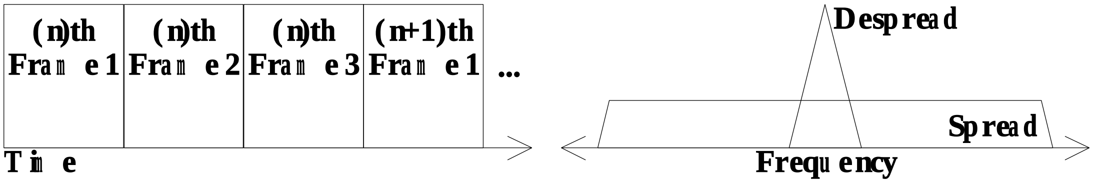

Figure 4: Time Division Multiple Access versus Code Division Multiple Access

The code division multiple access cellular networks being designed today use *direct sequencing* to spread channels. They essentially multiply the data in a channel by a polynomial expression to produce the chips in the signal that is broadcast. Another spreading method is *fast frequency hopping*, where the actual carrier frequency used is changed at a rate much greater than the signaling rate. This is not currently used in cellular communication, although *slow frequency hopping*, in which frequencies may change after each frame, is used in the GSM standard. This helps overcome certain forms of signal corruption although it complicates network routing.

Cellular networks must also deal with gaps in the communication between terminals and base stations. In addition to occasional signal dropouts due to obstacles and such, suppression of the terminal’s radio signal when there is no voice activity is often used to reduce power requirements and signal noise caused by the transmitter, typically by half. This is called *discontinuous transmission*, or *DTX*, and is a form of *power control*. Cellular networks often have complicated power control procedures which use location management as well as transmitted power level information to more finely control the output power of terminals. This is especially important for CDMA networks in order to prevent the signals from nearby terminals from blanking out the signals of further ones.

Cellular networks have additional routing concerns regarding billing, especially when terminals are *roaming* and billing must go through another service provider. Ironically, billing issues can be even worse when calls are made between two terminals using the same cell site (especially when one is roaming). Cellular networks may have additional billing concerns due to tariffs, especially in places like Europe where international roaming is permitted.

Signal Corruption

There are six major types of signal corruption that are individually addressed by most cellular networks. Multipath effects (signal reflections) cause two of them: *Ricean fading* and *Rayleigh fading*. *Doppler effects* are caused by the mobility of terminals. *Blocking* is caused by the fact that terminals may be at different distances from the cell sites. *Signal loss* can be caused by a variety of things, usually physical barriers. All other types of signal corruption can be classified as *noise*.

Ricean Fading

Ricean fading, the most general multipath effect, results when a transmitted signal follows multiple paths to the receiver. After the direct transmission is received, echoes of the signal reach the receiver. These can cause transmitted symbols to interfere with future symbols. In the following figure, the direct transmission would reach the car first, followed by an echo off of the building.

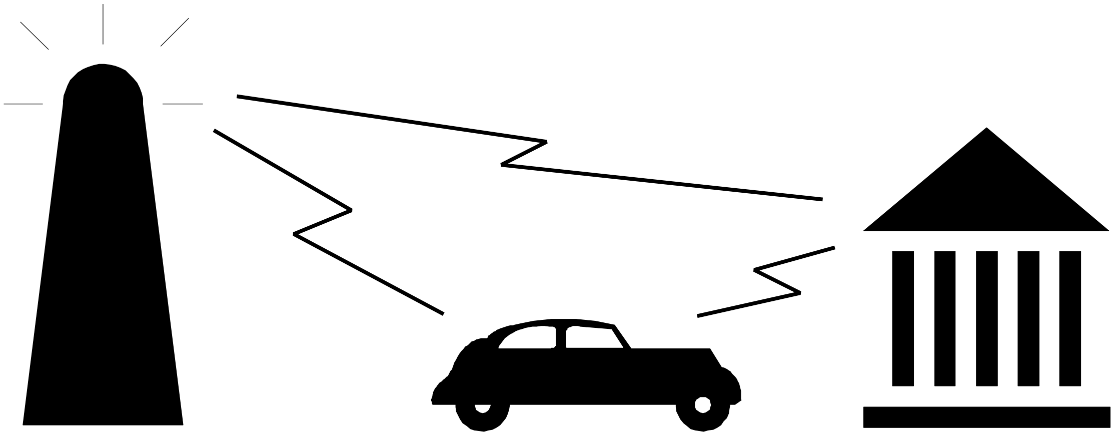

Figure 5: Ricean Fading (Multipath Effect)

Rayleigh Fading

Rayleigh fading is a very similar multipath effect, except it results when obstacles block the direct path from the transmitter to the receiver. Since the direct transmission is blocked, the reflected signals are not echoes, but the first signals received. Deconstructive interference (anti-nodes) can cause short-term amplitude dips, or even complete loss, in the received signal.

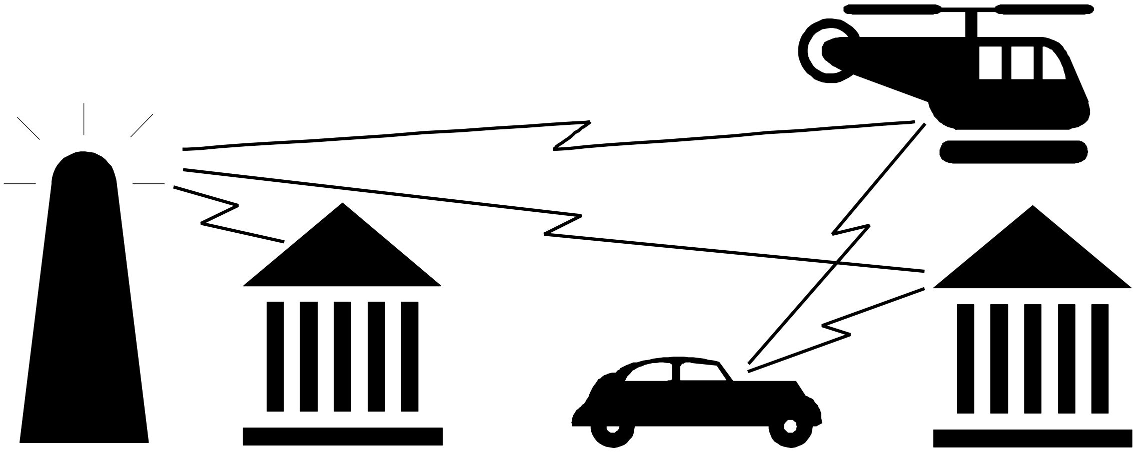

Figure 6: Rayleigh fading (Multipath Effect)

Doppler Effects

Doppler effects are caused by mobile receivers or transmitters, and affect the frequency of the received signal. If the receiver and transmitter are moving towards each other, the frequency of the received signal is shifted up. If they are moving away, it is shifted down. In the following example, the wavefront on the left is what is being transmitted from a stationary receiver. The wavefront on the right is what would be seen by a receiver moving in the direction of the arrow.

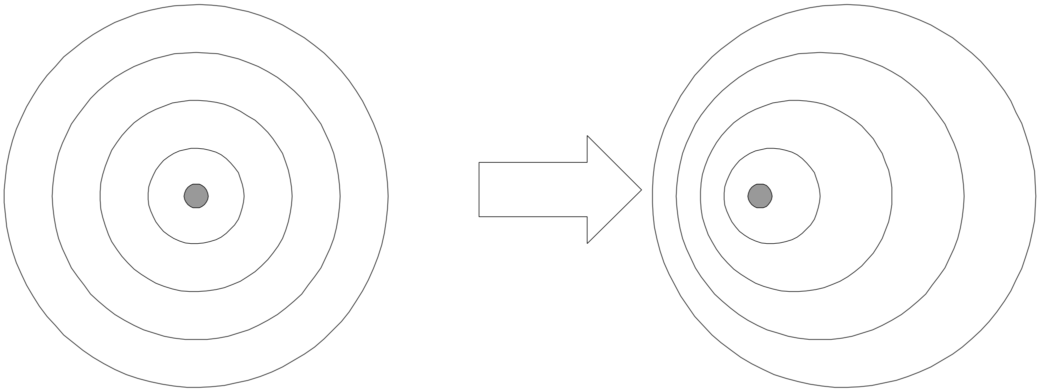

Figure 7: Doppler Effects: Wavefront as seen by Stationary and Mobile Receiver

Blocking

Blocking results when a nearby high-power transmitter blocks out whole range of channels. It is similar to driving by a radio station which can block out other stations on nearby frequencies. One example of how this can happen is when one cell is carrying too many calls and another cell is "covering" for it. If a terminal is too close to the nearby (overloaded) cell, it may lose the signal from the cell with which it is communicating. In the following example, the transmission from the cell on the left is blocked by the more powerful signal from the cell on the right.

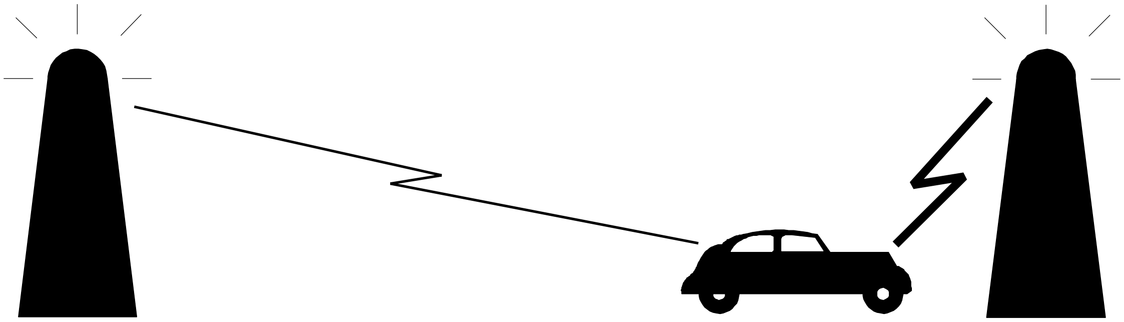

Figure 8: Blocking

Loss of Signal

There are several possible causes for loss of signal, including over-aggressive power management, although the most likely cause is simply due to obstacles. If the direct transmission blocked and there are no reflected signals to receive, the signal is lost and must be renegotiated.

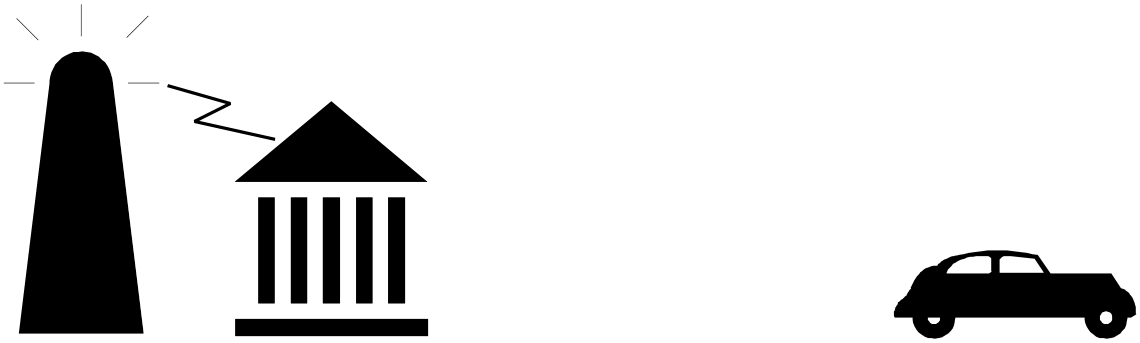

Figure 9: Loss of Signal

Noise

There are many types of noise, although the most common noise is “general background” noise, which is additive white Gaussian noise that is dependent only on temperature and cannot be avoided. The cellular network also introduces its own noise. For example, the *blocking* effect can be felt on a smaller scale, when a cell that has greater power (i.e., is closer) than the cell with which a terminal is communicating is using a nearby frequency, only causing noise rather then blanking out the other signal. This is called *cell-to-cell adjacent channel* noise. *Co-channel* noise is also present, and is caused by the reuse of frequencies. There can be additional noise problems when two terminals are using the same cell to communicate with each other (a type of crosstalk problem). Cellular networks usually deal with all types of noise by simply protecting the data with error correction techniques, although a major effect of the different types of noise is the limits that they place upon cellular networks (e.g., number of terminals per cell, frequency reuse factors, *etc.*).

Cellular Communication Standards

When Bell Laboratories first invented cellular service, the FCC actually considered granting a monopoly on cellular service to AT&T. Part of their reason for considering this was likely to prevent a proliferation of different incompatible cellular standards, as eventually happened in Europe. Instead, it decided to adopt the AMPS standard and promote competition.

Although the AMPS standard is now becoming outdated, it is still very important to have minimum standards for access. Besides allowing for universal coverage independent of service provider, standards promote competition among both service and equipment providers, which means lower cost and higher quality for consumers. Currently, GSM is the “least common denominator” standard for Europe. It has the advantage of a much higher capacity than AMPS and of being an all-digital standard. Many are looking to replace AMPS with a new “least common denominator” service in the United States.

The Advanced Mobile Phone System (AMPS) standard is the still most important cellular standard, since it was the basis for all future cellular standards and is still the least common denominator of service in the United States. It may eventually be phased out, however, if a digital standard emerges as a clear victor in the battle to become the cellular standard of the future.

There are four important TDMA standards in the world today. *IS-54* stands for *Interim Standard-54*, and is the only digital cellular network in commercial operation in the United States. IS-54 and its successor, *IS-136*, are usually treated as a single standard. *GSM* stands for *Global System for Mobile communication*, and is the preeminent European cellular standard. *PDC* (*Personal Digital Cellular*, also called *Japanese*

Digital Cellular or *JDC*) and *PHS* (*Personal Handiphone System*) are two Japanese standards that are in many ways superior to both GSM and IS-136, although they rely heavily on very small cell sizes. They are not really expected to displace any of the existing U.S. or European standards, although some of the services they provide might find their way into future PCS standards.

The only existing CDMA cellular standard is *IS-95* (*Interim Standard-95*), which is not in commercial service yet. It has many theoretical benefits over any of the TDMA standards (as its supporters will quickly point out), although it has yet to be successfully implemented, and IS-95 networks are unlikely to realize any of these benefits for a few years. CDMA may also play a part in the emerging PCS market, and the GSM committee has even been discussing implementing a CDMA system with a GSM protocol.

PCS (Personal Communication Systems) standards could be based on any TDMA or CDMA standard, although in Europe they will probably be based on the GSM standard. PCS systems tend to be smaller, use less power, operate at higher frequencies, and rely more on microcells than traditional cellular systems, although they are not substantially different. They are really just state-of-the-art cellular systems. The fundamental difference is the “universal telephone number” concept of PCS, which extends beyond cellular networking, but could be considered a natural evolutionary concept for telephony in general.

These standards come from many places. AMPS came directly from the early research done at Bell Labs. The GSM standard, on the other hand, was designed by an international committee. IS-54 was designed by a consortium, and IS-95 was designed primarily by QUALCOMM. In the end, the existence and acceptance of standards is what is important though, not how they were generated.

AMPS

AMPS, along with all U.S. cellular standards, is specified by the *Telecommunications Industry Association* in association with the *Electronics Industry Association* (*TIA/EIA*). The AMPS standard uses an “analog” control channel, which carries binary frequency shift keyed (BFSK) control information (this is the same modulation technique used in low speed modems). The control channel uplink, like all cellular control channels, uses a simple Aloha mechanism for multiple access, meaning that terminals simply send requests whenever they want access, retrying if they are not acknowledged. The control channel down-link acknowledges call setups and sends the terminals to the appropriate analog traffic channels. Traffic channels also contain embedded BFSK control information, which are simply filtered out as “noise” before being sent to the speaker or PSTN.

Like the other standards, 50 MHz of radio frequency is usually allocated per AMPS service provider, half of which are used for the up-link, half for the down-link. It is divided into 833 pairs of 30 kHz bands, each of which can carry a single AMPS traffic channel. Every cell cannot use all frequencies, however. In order to meet the required Carrier to Interference (C/I) ratio of 18 dB, cells reusing the same frequencies must be 3 cells apart. This yields a reuse factor of 7, meaning that one in 7 cells can use any given frequency, resulting in a maximum of 119 usable channels per cell on average.

IS-54/136

IS-54 and IS-136 are based on AMPS, and replace individual AMPS traffic channels with 3-way or 6-way multiplexed TDMA channels. They are often called *D-AMPS* for that reason, and have also been referred to as *American Digital Cellular* (*ADC*). IS-54 uses the same “analog” control channel as AMPS, although traffic bands are 3-way multiplexed. IS-136 add support for an all-digital control channel as well as for half-rate voice coding which allows traffic bands to carry 6 channels. Both standards are capable of supporting AMPS traffic channels as well.

IS-54/136 digital signaling, like that of all of the digital standards, is built based on the OSI reference model. The physical layer is divided into 40 ms frames, with a fixed time-slot allocation per channel. Digital control channels also specify 16-frame superframes and 2-superframe hyperframes. The type of modulation used is $\pi/4$-shifted *differential quadrature phase-shift keying* (*DQPSK*).

Both digital control channels and traffic channels add *Service Access Points* (*SAPs*) on top of the physical channel. Service Access Points are logical channels built on top of the channels (these are OSI layer 2 services). These provide random access control, paging, and other services as well as traffic data. In the traffic channels, there are embedded slow control service access points, although a fast control service access point can preempt the traffic data for high-priority information (e.g., notification that a call is being dropped). The IS-136 digital control channel also adds additional broadcast and short message services.

The gross bit rate carried over a 30 kHz IS-54 band is 48.6 kbps, yielding 16.2 kbps per channel. Of this, 8 kbps is voice traffic (which is compressed), 5 kbps is error protection for the speech, and the remaining 3.2 kbps are used for embedded signaling, guard time, and so on. IS-136 supports this type of channel as well as *half-rate* channels, which compress the voice traffic to half the size (with correspondingly lower error protection/guard time needs) and get 6 channels in the same 48.6 kbps.

IS-54/136 can thus get 2500 full rate or 5000 half-rate digital traffic channels in the 50 MHz allocated per service provider, although the reuse factor of 7 (the same as AMPS) reduces this to at most an average of 357 full-rate or 714 half-rate channels per cell.

GSM

GSM is very similar to IS-136, except that it is not tied to the 30 kHz AMPS bands. It uses 200 kHz bands which carry 8 channels each (or 16 with half-rate speech coding) and has a slightly more complicated digital control channel.

GSM uses very short (4.615 ms) frames, with 51-frame multiframes comprising the control channel and 26-frame multiframes comprising the traffic channels. It also has 1326-frame superframes and 2048-superframe (extremely long) hyperframes. Like IS-54/136, it uses fixed time-slot allocation per channel and provides Service Access Points as a layer 2 service; it also provides some additional synchronization SAPs. The type of modulation used is *Gaussian minimum-shift keying* (*GMSK*).

The gross bit rate carried over a 200 kHz GSM band is 270.8 kbps, yielding 33.85 kbps per channel. Of this, 13 kbps is voice traffic (which is compressed), 9.8 kbps is error protection for the speech, and the remaining 11.05 kbps are used for embedded signaling, guard time, and so on. GSM also supports *half-rate* channels, which compress the voice traffic to half the size and get 16 channels in the same band.

GSM can thus get 1000 full rate or 2000 half-rate digital traffic channels in the 50 MHz allocated per service provider (compared to 2500/5000 for IS-136). However, GSM has a much lower reuse factor (3), so the average number of usable channels per cell is 333 (or 666 half-rate) as compared to 357 (or 714) for IS-54/136.

The GSM specification is extremely thorough, including details on cost, security, network control, operations support, and the like. GSM also requires a special Subscriber Identity Module (SIM), which is like a credit card that is required for customers to access to GSM phones.

Two PCS specifications have already been made based on GSM. The cellular specification, GSM-900, calls for cellular service at 900 MHz. DCS-1800 was introduced at the request of the U.K. for “Personal Communication Network” services at 1800 MHz. PCS-1900 is another GSM specification that is vying for a share of the U.S. PCS market at 1900 MHz. One advantage that GSM solutions have for PCS is a higher bit rate assigned to the voice data, because the voice coders that were available when GSM was specified were not as good at compressing voice as voice coders are today. Newer voice coders can take advantage of the extra bandwidth available to provide service that sounds much better, though. This is called *enhanced full-rate* coding, which is finding its way into the IS-54/136 and IS-95 specifications as well.

IS-95

IS-95 is a direct-sequence CDMA standard that was developed by QUALCOMM and is being put into service primarily by Bell South. It uses pseudonoise, or PN, sequences to encode channels into pairs of 1.23 MHz bands and is fundamentally different from any of the TDMA standards. Unlike the TDMA standards, call quality in an IS-95 system improves when other channels are idle, even if they are being used but have no voice activity in one direction on a channel.

CDMA supporters frequently use theoretical calculations to show a tremendous increase in capacity, but in actuality there can never be more than 63 traffic channels per band, and the realistic limit is 45 (the true numbers will be known when a real system is operational). Thus, 900 IS-95 channels may be carried in the 50 MHz allocated to a service provider.

IS-95 literature is deceptive about reuse factors. Theoretically, IS-95 has a reuse factor of 1, meaning that every cell can use every frequency. However, some of the available PN sequences are not available to all of the cells. For example, if a terminal is directly between two cells, they will both communicate with it using the same PN sequence (channel). This is referred to as part of "loading", and reduces the number of available channels, likely to at most 25 per 1.23 MHz band, or 500 per cell.

Since channels are isolated through a CDMA mechanism, the framing structure under IS-95 is much simpler. The traffic channels are divided into 20 ms frames with no superframes. Two synchronization channels are each also divided into 20 ms frames and use 3-frame superframes. Layer 2 services are provided that split the physical channels into subchannels. The type of modulation used is *quadrature phase-shift keying* (*QPSK*).

The IS-95 down-link encodes 64 chips per bit with a PN sequence to create 64 channels, each with a maximum bit rate of 19.2 kbps. The up-link uses a more complicated encoding method to get 64 channels with a maximum bit rate of 28.8 kbps. Of this, at most 9.6 kbps is used for speech and varying amounts are used for error protection and embedded control (the uplink uses more error protection bits than the downlink). Lower bit rates may also be used to decrease the overall noise in the system.

Operational Domains

There are two major domains of cellular communication processing: radio frequency (R/F) and baseband. R/F processing takes place in the tens of MHz to several GHz frequencies and deals with the signals sent through the air. Baseband processing takes place in the zero to tens of kHz frequencies and is the range in which humans communicate. Sometimes intermediate frequency (I/F) processing is used as well, but only if the hardware is incapable of making the leap from baseband to R/F in one step.

Radio Frequency Domain

The R/F processing includes modulation, demodulation, frequency synthesis, amplification, and analog filtering. Analog cellular phone systems typically stop here and do not do baseband processing (they also typically use more power and consume more radio bandwidth per channel).

Modulation and demodulation deals with putting baseband signals on carrier waves. Digital cellular systems use different forms of frequency or phase-shift keying in their modulation techniques. CDMA systems also use a PN sequence before determining the actual "chips" to send.

Frequency synthesis is the generation of carrier frequencies. This is made a bit more challenging when frequency-hopping is used as in GSM networks (one reason frequency hopping is used is that it helps avoid Rayleigh fading since the interference pattern changes at different frequencies).

Cellular frequencies are allotted by the governing regulatory body (the FCC in the U.S.). They are typically allotted in 50MHz blocks (25 MHz for the base-to-terminal "downlink" or forward channels and 25 MHz for the terminal-to-base "uplink" or reverse channels). Typically, they are allotted at around 900 MHz. Other frequencies that are commonly used are 450, 1800, and 1900 MHz, with PCS systems using the latter two. In all cases, channels operate in pairs (one uplink, one downlink), which can be treated as a single bidirectional channel.

Baseband Domain

Baseband processing in digital cellular systems consists of voice coding and decoding, channel coding and decoding, equalization, timing and control, digital conversion, and encryption. Voice coding is simply compressing speech. Channel coding, or Forward Error Correction (FEC), builds redundancy and structure into messages so digital faults may be corrected, and helps correct for Raleigh fading and noise.

Equalization corrects for analog corruption (including noise, multipath, and Doppler effects) by attempting to reconstruct parts of the message and guess what phenomena affected them. Timing and control coordinates and synchronizes between the R/F and baseband processing and deals with high-level control issues such as protocol handling. Digital conversion is from digital to analog and analog to digital. Encryption is not always supported, but might be used to send subscriber information to the base station, for example.

Voice Coding

Voice coding (or "vocoding") compresses voice data down to anywhere from 4,000bps to 13,000bps. Full-rate speech coding is at 8,000bps to 13,000bps. Anything less is considered half-rate speech coding, and results in a drop in call quality. For reference, uncompressed voice is input at a rate of 8,000 13-bit samples per second (104,000bps), and 64,000bps are carried on regular phone lines.

Some speech quality is sacrificed for the compression, so the call quality of AMPS systems is actually better than *any* of the digital standards when the terminal is close to a cell site. However, call quality decreases under AMPS as the terminals move farther from the cell sites, while digital systems tend to be more all-or-nothing. The GSM specification indicates that GSM call quality must be roughly the same as analog (AMPS) service, which presumably is averaged throughout the service area.

Channel Coding

Channel coding is simply a fancy name for Forward Error Correction. It protects for a whole range of errors by building redundancy into messages. It can correct for *digit faults*, which are where digits are lost (also called *modem faults*). These may be caused by Rayleigh fading, blocking, or simply by noise.

Typically, at least the "important" parts of voice data (where "important" depends on the voice coding method used) are protected via a rate 1/2 algorithm. This means that there are 2 transmitted bits for each data bit. The IS-95 up-link uses a rate 1/3 algorithm. Control data may be protected more, with as many as 6 transmitted bits per data bit.

Equalization

Equalization methods look for known patterns in messages, try to guess what caused any failures, and attempt to compensate for them. Equalization filters out channel faults, especially inter-symbol interference (between one symbol and the next) due to Ricean fading, Doppler, or noise effects. Usually, the known patterns are inserted as close to the middle of the message as possible so that they will probably be affected by the same phenomena as the rest of the message.

Implementation Details

Regardless of the communication standard used, all cellular communication systems have much in common. The basic mechanics of the cell sites and terminals (e.g., handsets) are very similar, and the communication challenges are the same. It is not surprising that even radically different systems often use many the same implementation techniques.

Distribution of Functions

Most cellular communication processing is duplicated in both terminals and base stations. Each terminal must only deal with one channel of communication, although it has very stringent power and cost requirements and must be capable of all of the wireless processing associated with that channel. Base stations must deal with more channels but have less stringent cost and power requirements and can distribute the processing between BTS, BSC, and MSC.

In base stations, the BTS typically handles R/F, digital conversions, channel coding/decoding, and equalization. It then transfers compressed (possibly encrypted) data to and from the BSC. The BSC does voice coding/decoding and sends data at a much higher bit rate to the MSC. The MSC handles higher-level routing, billing, encryption, and interacts with the cellular user at a higher level. It converts cellular traffic into regular PCM and other telephony signaling and sends it to the PSTN.

Operational Components

R/F processing is usually done using fast, dedicated hardware, as is baseband-R/F synchronization and digital conversion. The CDMA encoding in IS-95 also uses dedicated hardware, usually *application-specific integrated circuits* (*ASICs*). As more custom devices are being built for the cellular industry, functions are being integrated onto fewer and fewer chips each year.

Microcontrollers are usually used to manage the cellular protocols and the *HMI* (*Human-Machine Interface*, usually a keypad and display on the terminal). *Digital Signal Processors* (*DSPs*) are often used to implement most of the baseband processing as well as for some filtering and modulation/demodulation functions. Many of the algorithms used in cellular processing, especially in baseband processing (e.g., voice coding) are specified in the applicable standards.

Algorithms

Compression methods for voice coding include *codebook excited linear prediction* (*CELP*, used by JDC and IS-95), *vector-sum excited linear prediction* (*VSELP*, used by IS-54/136), *regular pulse excitation long-term prediction* (*RPELPT*, used by GSM), and others. As new types of service (e.g., enhanced full-rate voice) are added, new compression methods are devised.

Convolutional encoding is a type of Trellis coding and is used for channel encoding. Polynomials are used to generate multiple bits of transmitted data per actual data bit. The *rate* of an encoder is the number of data bits per transmitted bit (e.g., both IS-54 and GSM specify rate 1/2 convolutional encoding for speech data, meaning that each data bit results in two transmitted bits).

Viterbi decoding is a type of Trellis decoding, and is a kind of modified intelligent tree search. It can be used for channel decoding and for certain types of equalization, particularly *maximum likelihood sequence estimation* (*MLSE*) equalization. There are other types of equalization methods that may be used, such as *decision feedback equalization*.

Data Services

Data services can be supported on all cellular systems, whether through cellular modems or through features inherent to the cellular standard being used. Enhanced data services can even be provided over standard AMPS channels using *cellular digital packet data* (*CDPD*), which uses existing AMPS channels to send digital packet data (usually TCP/IP) when they are not being used for voice.

Digital cellular services already send digital data. All you really need to do is skip the voice coding part. Some specifications also support lower-priority messaging data (such as would be received by a pager) without tying up a whole channel.

Current Trends

Personal Communications Services will probably be a driving force in cellular networks. It could be argued that PCS is really just “state of the art” cellular service using smaller low-power terminals, higher frequencies, higher capacity service through microcells, and advanced features (e.g., improved power management and data services). The concept of a *universal telephone number* (*UTN*) is really not particularly new to PCS either. Services such as 500 numbers and call forwarding have been around for some time. But even if PCS systems are viewed as entirely different types of systems, the concepts and technology introduced in PCS will probably have a large effect on cellular networks.

Another trend in cellular communication is towards more integration. Components within phones are being integrated, making phones cheaper, smaller, and less power-hungry. Bell Laboratories has already put a cellular phone on a watch for one of the “You Will” commercials. More features are being added to phones. Although integrated faxes and cellular modems have not really taken off, cellular phones have been integrated with cordless phones. The Japanese *Personal Handiphone System* does this now, allowing calls to be made as cordless calls within the home and automatically become cellular calls outside of the home.

Satellites have been considered as an alternative way to provide cellular service. Besides offering coverage to extremely remote areas, satellites tend to have less problems with signal corruption since they usually have a direct line to the receiver (and if they don't, reflections tend not to be as horizontal and thus do not interfere with each other much). Frequency reuse is definitely an issue though, since satellites cover a much larger area than cell sites. Motorola's proposed *Iridium* network would use Low Earth Orbit satellites (which cannot stay in orbit very long—perhaps a decade or so) to provide this service. Support seems to be lacking for it, though.

There are a number of ways in which data services are currently being improved in cellular networks. At one end is a push for higher-speed data services. This is primarily for land-line quality sound and secondarily for fax/modem applications, although there is also some work underway to make ATM, ISDN, and even video services available to cellular networks. On the other end is a push to let as many users as possible have some form of wireless access through either half-rate voice coding or with messaging (pager) services. All of these data service enhancements require additional support in the cellular protocols, and may require algorithmic support (e.g., improved voice coders). There is also research under way attempting to improve the capacity of cellular networks without changing the data services (e.g., through adaptive TDMA).

Summary

Cellular technology is revolutionizing communication. The recent explosion of cellular technology and number of users indicates that it has definitely been accepted. Although telephone technology has been difficult to change in the past (ISDN, video phones, and many other major service improvements never quite caught on), radical changes in cellular service are already coming. Cellular networks are rapidly evolving from the analog systems of the past into the personal communicators of the future. What exactly will be in that future is hard to tell, although cellular networks are definitely going digital and will definitely add many services not available to regular telephones today.

References

Unfortunately, there don't seem to be many good tutorial-type books on cellular networks, so the information in this paper was culled from many sources, including extensive discussions with cellular designers. The best place to look for general information about cellular networks is in industry and research papers. A few places to look include:

- the IEEE Proceedings on Vehicular Technology,
- IEEE Selected Readings in Cellular Radio and Personal Communications (edited by Theodore S. Rappaport),
- the IEEE Proceedings on Personal Wireless Communications,
- the Wireless Information Network Laboratory (WINLAB) Proceedings, by Kluwer Academic Publishers, and
- the IS-95, IS-136, and GSM specifications (published by the TIA/EIA and CCITT/ETSI).