CHAPTER 4

Wireless Network Architecture and Operation

Upon completion of this chapter, the student should be able to:

- Discuss the cellular concept and explain the advantages of frequency reuse.
- Draw a diagram of a typical cellular cluster and explain the meaning of frequency reuse number.
- Discuss how the capacity of a cellular system may be expanded.
- Explain the difference between cell splitting and sectoring.
- Discuss the use of backhaul networks for cellular systems.
- Explain the concept of mobility management and discuss the operations it supports.
- Discuss the concepts of power management and network security.

The cellular concept and its potential for increasing the number of wireless users in a certain geographic area had been proposed many years before it was ever put into practical use. The analog technology used by the first cellular systems dictated a certain type of cellular architecture. As time has past, newer digital technologies and the public's very rapid acceptance of cellular telephones has caused the architectures of today's cellular systems to change in an effort to adjust to the new technologies and the added demand for capacity.

Capacity expansion techniques include the splitting or sectoring of cells and the overlay of smaller cell clusters over larger clusters as demand and technology changes warrant. As demand for newer data services has increased, cellular operators have turned toward the development of their own private data networks to backhaul traffic from their cell sites to a common point of presence where a connection can be made to the PSTN or the PDN.

As cellular systems have matured and become nationwide wireless networks, mobility management has taken on an even more important role in the operation of wireless cellular networks. Mobility management is used to keep track of the current location of a cellular subscriber and to assist in the implementation of cellular handoff. Although not as glamorous as mobility management, power management and wireless network security have become more important issues as the cellular industry heads into its third decade of operation and wireless system engineers fine-tune their designs to build more secure systems and achieve even greater efficiencies of operation.

This chapter will examine all of the abovementioned issues and present several examples of typical cellular architectures and network operations.

4.1 THE CELLULAR CONCEPT

As briefly outlined in Chapter 2, the concept of cellular telephone service was first proposed in the 1940s. The cellular concept would provide a method by which frequency reuse could be maximized thus in essence multiplying the number of available channels in a particular geographic location. The concept of frequency reuse itself was not new at the time for it had been the guiding principle of the licensing of AM commercial broadcasting stations for years and is still used today to determine the granting of licenses for new stations in the broadcasting bands (AM, FM, and TV) and other radio services. However, in broadcasting (a **simplex** or single-direction transmission operation) the goal is to reach as many receivers as possible with a single broadcasting transmitter. This usually entails the use of a high-power transmitter to provide coverage of some particular geographic or trading area. However, there is nothing to prevent the same frequency assignment or cochannel from being used in another area of the country where the signals from distant cochannel stations do not extend to it. Since most users of the radio frequency spectrum recognize it as a limited resource, attempts are usually made to use it as efficiently as possible.

For **duplex** or two-way radio operation, where a system design goal is to allow as many simultaneous users of the available radio spectrum as possible, the reuse of that spectrum is crucial to maximizing the number of potential users. The cellular concept provides a means of maximizing radio spectrum usage. Another benefit of cellular radio systems is that the amount of mobile output power required is not as large due to the smaller cells used and therefore the power requirements for the mobile are reduced, which allows for longer battery life and smaller mobile station form factors.

Introduction

The first mobile telephone service, offered by AT&T and the Bell Southwestern Telephone Company in St. Louis, Missouri, consisted of several colocated transmitters on the top of Southwestern Bell's headquarters. A 250-watt FM transmitter paged mobiles when there was an incoming call for the mobile. This system's high-powered base station transmitters and elevated antennas provided a large coverage area and enough signal power to penetrate the urban canyons of the city. At the same time, however, the frequencies used by the system could not be used by any other services or similar systems for approximately a seventy-five-mile radius around the base station.

The first proposed cellular system would use many low-power transmitters with antennas mounted on shorter towers, to provide a much shorter frequency reuse distance. The area served by each transmitter would be considered a cell. The first cellular systems used omnidirectional antennas and therefore produced cells that tended to be circular in shape. As the technology used to create more efficient cellular mobile systems has evolved, so has the design and implementation of the cellular concept. These changes will be outlined in this chapter.

The Cellular Advantage

The deployment of a large number of low-power base stations to create an effective cellular mobile system is a large and expensive task. The acquisition of land for cell sites; the associated hardware; radio base station transceivers and controllers; antennas and towers; the communications links between the base stations, base station controllers, and mobile switching centers; and finally, the cost of the radio frequency spectrum needed to implement the system can be enormous. Mobile service providers can only recover their costs and make a profit if they can support a sufficient number of mobile subscribers. The cellular concept allows a large enough increase in capacity to make these operations economically feasible.

The implementation of the basic cellular architecture consists of dividing up the coverage area into a number of smaller areas or cells that will be served by their own base stations. The radio channels must be allocated to these smaller cells in such a way as to minimize interference but at the same time provide the necessary system performance to handle the traffic load within the cells. Cells are grouped into **clusters**

hat make use of all the available radio spectrum. Since adjacent cells cannot use the same frequency chan-
ıels, the total frequency allocation is divided up over the cluster and then repeated for other clusters in the
ystem. The number of cells in a cluster is known as the cluster size or the **frequency reuse** factor.

For cellular architecture planning one must be concerned with interference from radio transmitters in
ɔther cells using the same radio channel and from interference from other transmitters on nearby channels.
The first type of interference is known as cochannel and the latter is known as first-adjacent channel, sec-
ɔnd-adjacent channel, and so on. Using the cellular concept and careful design techniques can increase the
maximum number of system users substantially. The following example will illustrate this point.

Example 4–1

Consider the following case: a service provider wants to provide cellular communications to a particular geographic area. The total bandwidth the service provider is licensed for is 5 MHz. Each system subscriber requires 10 kHz of bandwidth when using the system. If the service provider was to provide coverage from only one transmitter site, the total theoretical number of possible simultaneous users is 500 (5 MHz/10 kHz/user = 500 users). If, however, the service provider implements a cellular system with thirty-five transmitter sites, located to minimize interference and provide total coverage of the area, determine the new system capacity.

Solution: Using a cluster size of 7, the total system bandwidth is divided by 7 yielding approximately 714 kHz of bandwidth per cell (5000 kHz/ 7 = 714 kHz), and this is repeated over the 5 clusters (35/7 = 5). Now each cell has a capacity of 71 simultaneous users (714 kHz/10 kHz/user = 71 users) or a total system capacity of 2485 users (35 cells × 71 users/cell = 2485 users). This is a system capacity increase of approximately 5 times.

Cellular Hierarchy

Before examining the technical characteristics of frequency reuse and reuse number, it is helpful to define the hierarchical structure of today's cell sizes. The wireless industry has more or less settled on some particular names to indicate the size of a cell. Going from the smallest to the largest, cells that are less than 100 meters in diameter are known as **picocells,** cells with a diameter between 100 meters and 1000 meters (1 km) are known as **microcells,** and cells greater than 1000 meters in diameter are known as **macrocells.** These definitions are also related to the various possible operating environments that one might find oneself in. Picocells are usually found in the indoor environment (e.g., inside of buildings), microcells are found in the outdoor-to-indoor and pedestrian environment (urban), and macrocells are found in the vehicular and high- antenna environment (suburban). Each of these particular environments presents a different type of radio link propagation scenario that affects the required equipment and other technical aspects of the hardware used to implement the particular type of cell.

Newer technologies have expanded our concept of cells to include the global environment served by a variety of satellite systems and smaller cells for personal area networks (PANs) usually considered being less than ten meters in diameter. Although the terms have not become universal yet, cells with global coverage have been referred to as **megacells** and very small cells have been referred to as **femtocells.** Figure 4–1 illustrates the relative coverage areas of the various cell sizes. It is entirely possible to have mixed environments that are served by several different types of cell structures simultaneously.

4.2 CELL FUNDAMENTALS

Since the first cellular systems usually employed omnidirectional antennas and thus theoretically produced circular-shaped cells, the reader might be puzzled by the cellular industry's de facto choice of a hexagon as

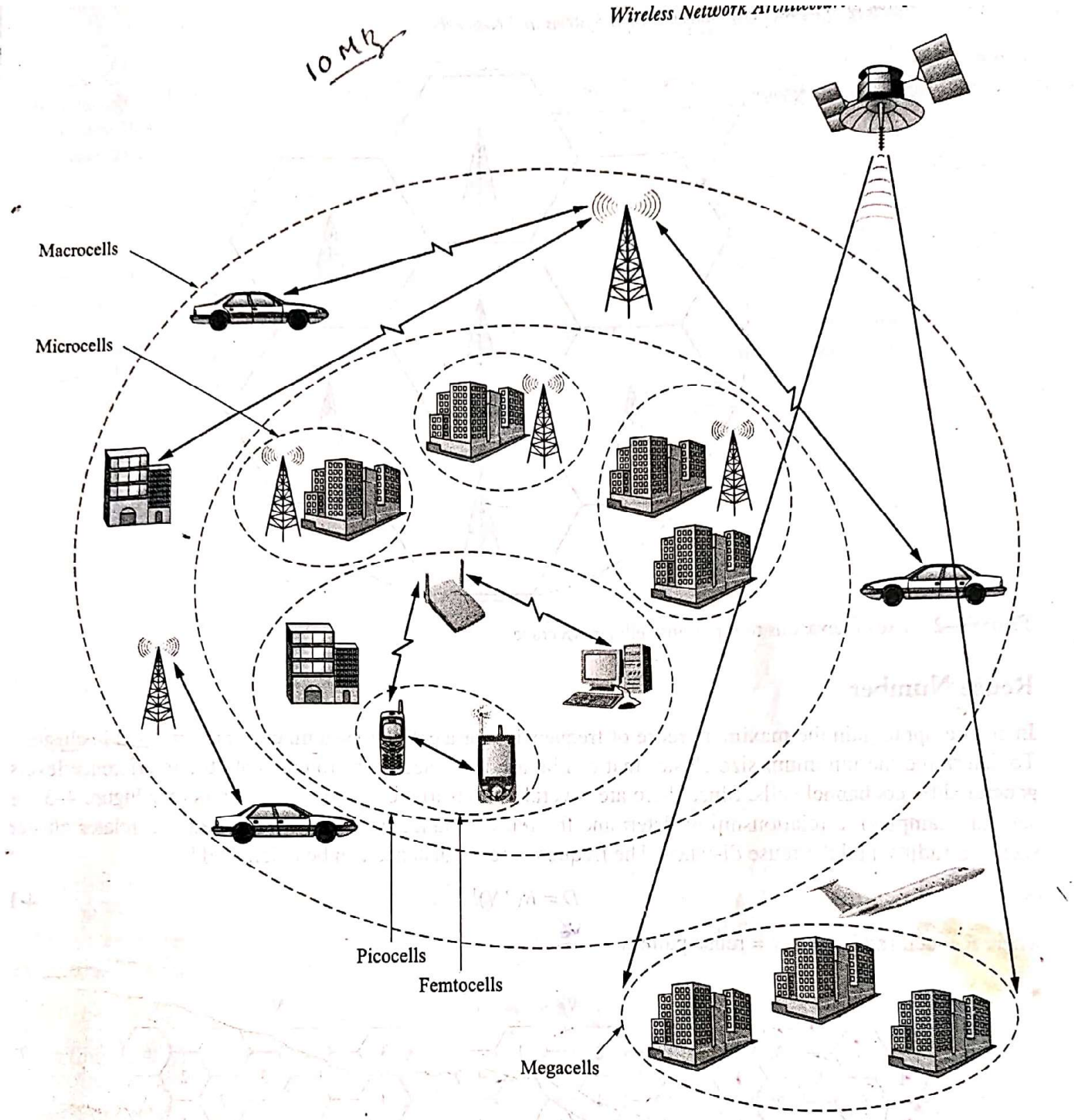

Figure 4–1 Relative coverage areas of different size cells.

shown in Figure 4–2 to represent a typical cell's coverage area in a service provider's network. Any initial consideration of the shape to use for a typical cell must be concerned with the fact that a true circular coverage area is rarely obtained in practice. Propagation conditions, terrain, and the environment (urban, suburban, etc.) all contribute to the distortion of an antenna's radiation pattern and hence coverage area. Furthermore, using circles to lay out a network's coverage area leaves gaps between adjacent tangent circles or ambiguous areas if the circles are overlapped. Referring to Figure 4–2, one can see that the use of a hexagon, however, allows for the complete theoretical coverage of an area without any overlapping cells or gaps in the coverage. Squares or equilateral triangles could also be used but the hexagon is the closest approximation to a circle. The use of hexagons also makes the theoretical calculation of several system parameters much easier.

Reuse Number

In an attempt to gain the maximum reuse of frequencies for a cellular system, cells are arranged in clusters To determine the minimum-size cluster that can be used it is necessary to calculate the interference level generated by cochannel cells. Since there are several options to the size of cell clusters (see Figure 4–3 for several examples), a relationship to determine the reuse distance has been determined that relates cluster size, cell radius, and the reuse distance. The frequency reuse distance can be calculated by:

$$D = R(3N)^{1/2} \qquad 4.$$

where R = cell radius and N = reuse pattern.

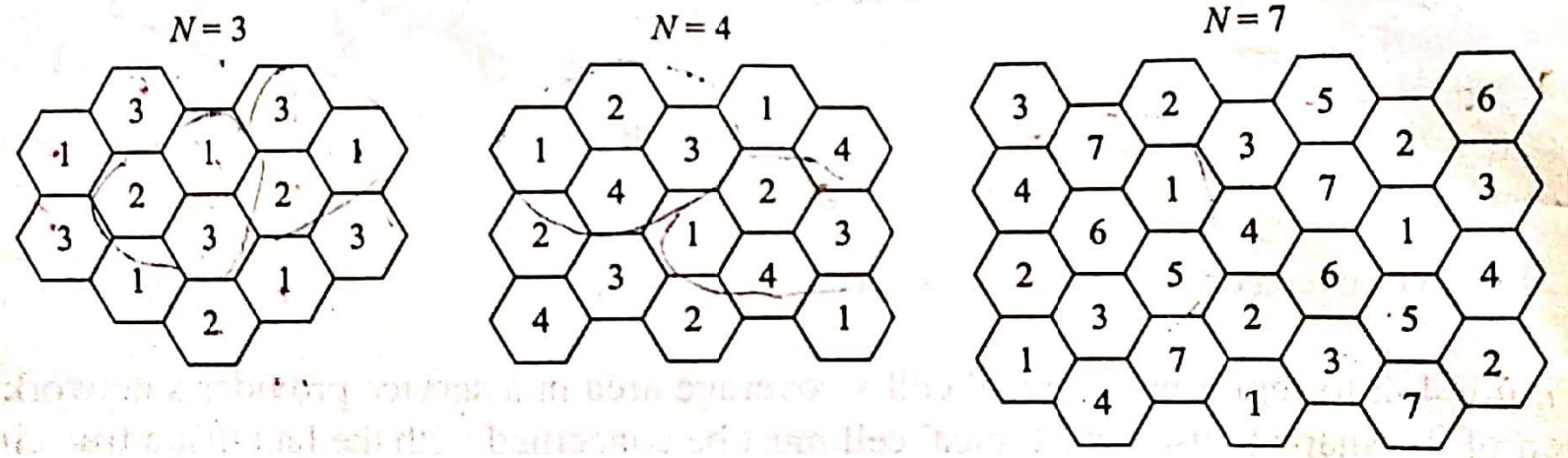

Figure 4–3 Various cellular reuse patterns.

Values of N can only take on numbers calculated from the following expression: $i^2 + ij + j^2$ where i and are integers.

As can be seen from Equation 4-1, the smaller the value of N the closer the reuse distance and therefo the larger the system capacity or total number of possible users. It should be pointed out that reducing th size of the reuse distance D may provide the ability to handle more subscribers but it also increases netwo

costs in terms of the required hardware and acquisition of cell sites, increases the complexity of the network, and increases the number of operations required to provide mobility. The following example will illustrate the relationship between cluster size and reuse distance.

Example 4–2

For a mobile system cluster size of 7, determine the frequency reuse distance if the cell radius is five kilometers. Repeat the calculation for a cluster size of 4.

Solution: Figure 4–4 shows the typical arrangement for a cluster size of $N = 7$ and the reuse distance for cell 3. This is the cluster size typically used for the first-generation AMPS system used in the United States.

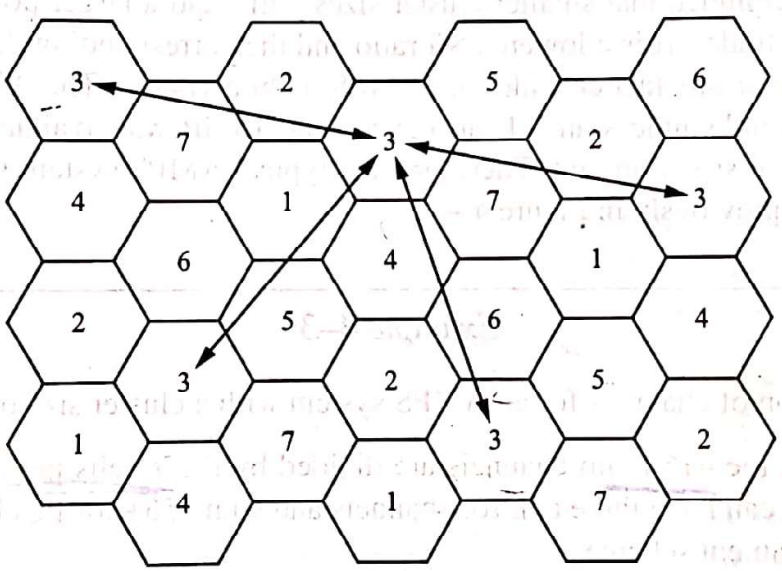

Figure 4–4 A frequency reuse diagram with the reuse distance, D, indicated (cluster size $N = 7$).

As mentioned earlier, using the expression $i^2 + ij + j^2$, one can show that a possible value for N is 7. As shown in Figure 4–4, the hexagons (cells) are arranged with one hexagon in the center of a cluster and six other hexagons surrounding the middle hexagon. Adjacent clusters repeat the previous pattern. The reuse distance is found from the following equation:

$$D = R(3N)^{1/2}$$

Therefore, for a cluster size of 7,

$$D = 5(3 \times 7)^{1/2} = 5(21)^{1/2} = 5(4.5823) = 22.913 \text{ km}$$

For a cluster size of 4, the reuse distance is given by:

$$D = 5(3 \times 4)^{1/2} = 5(12)^{1/2} = 5(3.464) = 17.32 \text{ km}$$

As can be seen, a smaller cluster size results in a smaller reuse distance.

Cellular Interference Issues

As already covered in the previous section, the frequency reuse distance can be calculated from Equation 4-1. Additionally, more complex calculations can yield the signal-to-interference ratio for a particular cluster size, *N*. The **signal-to-interference ratio** (S/I or SIR) gives an indication of the quality of the received signal much like the time-honored signal-to-noise ratio (SNR) measurement. Using a fairly simple mathematical model for S/I ratio calculations involving omnidirectional cells yields the results tabulated in Table 4–1 for several common values of *N*:

Table 4–1 Signal-to-interference ratio for various cluster sizes.

Cluster Size, N	*S/I Ratio*
3	11.3 dB
4	13.8 dB
7	18.7 dB
12	23.3 dB

The reader should be reminded that smaller cluster sizes will yield a larger possible subscriber base but as shown in Table 4–1 the trade-off is a lowered S/I ratio and the corresponding decrease in radio link quality. As a practical example of this fact consider the AMPS mobile system. The AMPS system did not yield usable voice-quality radio links unless an S/I ratio exceeding 18 dB was available. This value of S/I was only possible for a cluster of size 7 and up. Therefore, the typical AMPS system was deployed with a cluster size of $N = 7$ as shown previously in Figure 4–4.

Example 4–3

Show a possible distribution of channels for an AMPS system with a cluster size of $N = 7$.

Solution: For this situation, the 416 radio channels are divided by the 7 cells per cluster to yield 59+ channels per cell site. Each cell can have three control channels and some 56+ traffic channels. Table 4–2 shows one possible channel assignment scheme.

Table 4–2 A possible assignment of AMPS channels for a cluster size of 7.

Cell 1	*Cell 2*	*Cell 3*	*Cell 4*	*Cell 5*	*Cell 6*	*Cell 7*
Control Channels						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
Traffic Channels						
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	...	...	...	...	...
...	...	...	...	...	...	401
402	403	404	405	406	407	408
409	410	411	412	413	414	415
416						

Note how each cell has a channel spacing of 7 × 30 kHz = 210 kHz and that this channel allocation is repeated in each cluster of 7 cells. Another way of assigning channels when the cluster size is 7 will be introduced later.

4.3 CAPACITY EXPANSION TECHNIQUES

As cellular mobile telephone service grew in popularity during the 1990s, the need to expand system capacity also grew. Most cellular providers will initially implement their systems by providing service in a coverage area with the least amount of initial investment (i.e., the least number of cell sites). As demand grows the system is usually expanded with additional cell sites to handle the increased traffic. There are several ways in which a service provider may increase capacity. The first and simplest method is to obtain additional frequency spectrum. Although this sounds like a fairly straightforward approach, it has proven to be one of the most expensive. Government auctions have sold frequency spectrum to service providers in countries all around the world. The fairly recent auctions of the PCS bands in the United States by the FCC in the mid-1990s yielded approximately $20 billion. The results of those high prices caused several of the top bidders for that spectrum to eventually declare bankruptcy. Another problem with this approach is that in many instances there is no frequency spectrum available to be auctioned off. In the United States as in many countries worldwide, previous spectrum allocations and incumbent radio services or applications are inhibiting and in some cases preventing the expansion of new advanced wireless mobile technologies. This topic will be treated more fully in other chapters.

The other approaches to capacity expansion are either architecturally or technologically enabled. Changes in cellular architecture like cell sectoring, cell splitting, and using various overlaid cell schemes can all provide increased system capacity. Another technique is to employ different channel allocation schemes that effectively increase cell capacity to meet changes in traffic patterns. Lastly, the adoption of next-generation technology implementations tends to provide an inherent capacity expansion within the new technology itself. The next few sections will provide more detail about these different methods.

Cell Splitting

If a cellular service provider initially deploys a network with fairly large cells, the coverage area will be large but the maximum number of subscribers will be limited. If a portion or portions of the system experience an increasing traffic load that is pushing the system to its limit (subscribers experience a high rate of unavailable service or blocking) then the service provider can use a technique known as **cell splitting** to increase capacity in the overburdened areas of the system. Consider the following example of cell splitting shown in Figure 4–5. Assume that Cell A has become saturated and is unable to support its traffic load. Using cell splitting, six new smaller cells with approximately one-quarter the area of the larger cells are inserted into the system around A in such a way as to be halfway between two cochannel cells. These

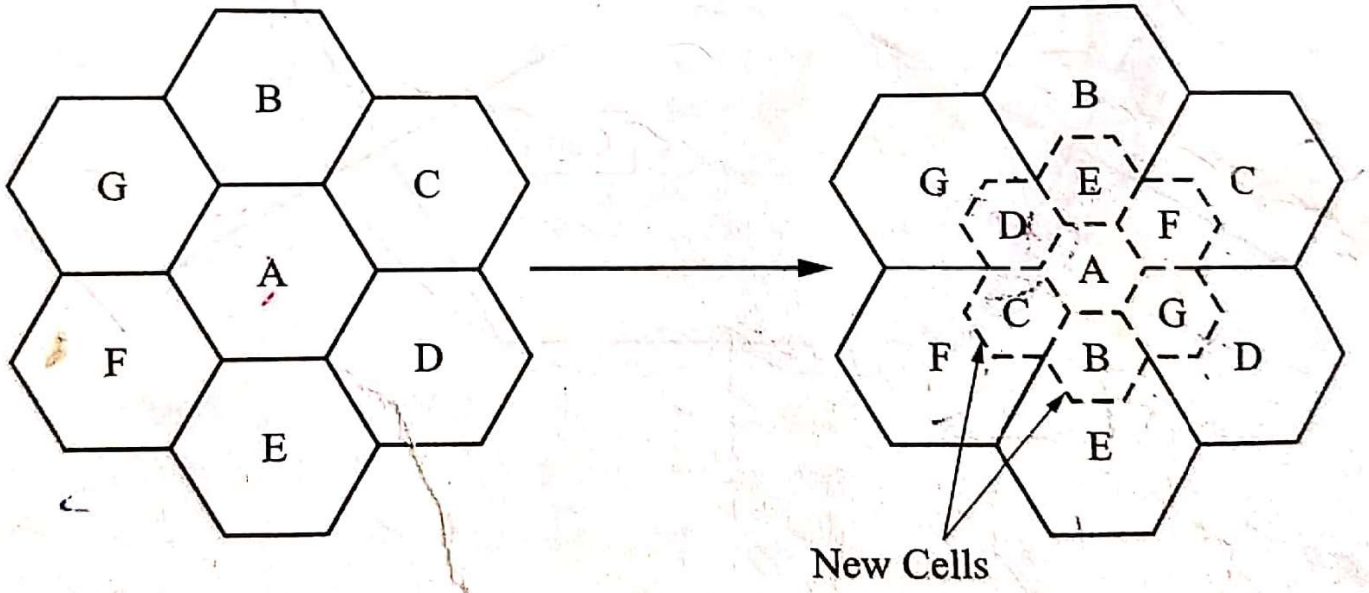

Figure 4–5 Increasing capacity by cell splitting.

smaller cells will use the same channels as the corresponding pair of larger cochannel cells. In order that the overall system frequency reuse plan be preserved, the transmit power of these cells must be reduced by a factor of approximately 16 or 12 dB.

Cell splitting will work quite well on paper; however, in practice many times the process is not as smooth as one would desire. Very often, due to the difficulty of acquiring appropriately located cell sites, the conversion process will be prolonged and different size cells will exist in the same area. In these cases, it is necessary to form two groups of channels in the old cell; one group that corresponds to the small-cell frequency reuse requirements and another group that corresponds to the old-cell reuse requirements. Usually the larger cell channels are reserved for highly mobile traffic and therefore will have fewer handoffs than the smaller cells. As the splitting process moves toward completion the number of channels in the small cells will increase until eventually all the channels in the area are used by the lower-power group of cells and the original Cell A has had its power reduced and also joins the new smaller cluster. As traffic increases in other areas of the system this process may be repeated over again. Eventually the entire system will be rescaled with smaller cells in the high-traffic areas and larger cells on the outskirts of the system or in areas of low traffic or low population density.

Cell splitting effectively increases system capacity by reducing the cell size and therefore reducing the frequency reuse distance thus permitting the use of more channels.

Cell Sectoring

Another popular method to increase cellular system capacity is to use **cell sectoring.** Cell sectoring us directional antennas to effectively split a cell into three or sometimes six new cells. The vast majority cellular providers use this technique for any of the cellular systems presently in operation. As shown Figure 4–6, the new cell structure now uses three-directional antennas with 120-degree beamwidths "illuminate" the entire area previously serviced by a single omnidirectional antenna. Now the channels all cated to a cell are further divided and only used in one sector of the cell.

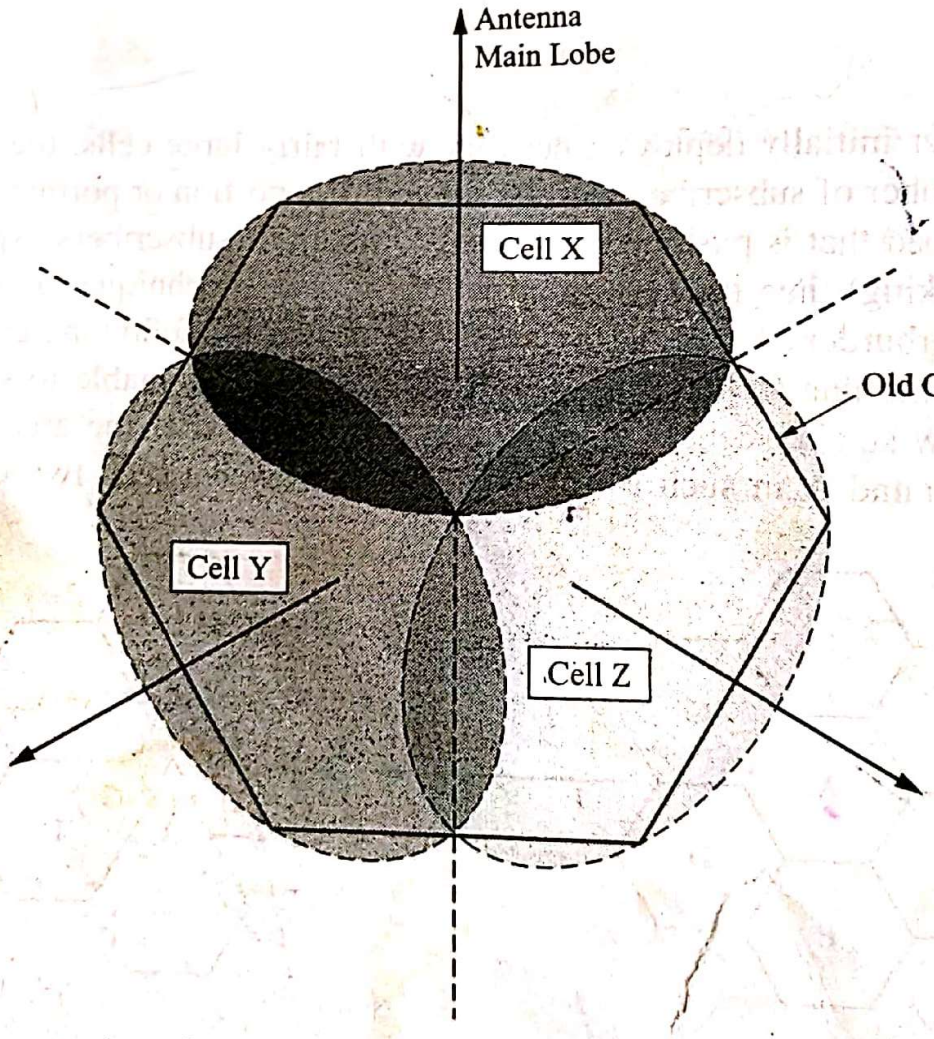

Figure 4–6 Increasing capacity by cell sectoring.

Smart Antennas

In the 3G specifications, the support of smart antenna technology is included. This technique to improve system performance makes use of phased array or "beam steering" antenna systems. These types of antennas can

use narrow pencil-beam patterns to communicate with a subset of the active users within a cell. Once a mobile subscriber has been located by the system, a narrow radio beam may be pointed in the user's direction through the use of sophisticated antenna technology. The use of a radio link that approaches point-to-point type link characteristics is extremely useful in a mobile environment. Besides the elimination of most multipath signals, a fact that will certainly improve system performance, the amount of interference received will be reduced and system capacity can be increased. As the mobile user moves about the coverage area, the smart antenna will track the mobile's motion. See Figure 8–18 for a depiction of a smart antenna system.

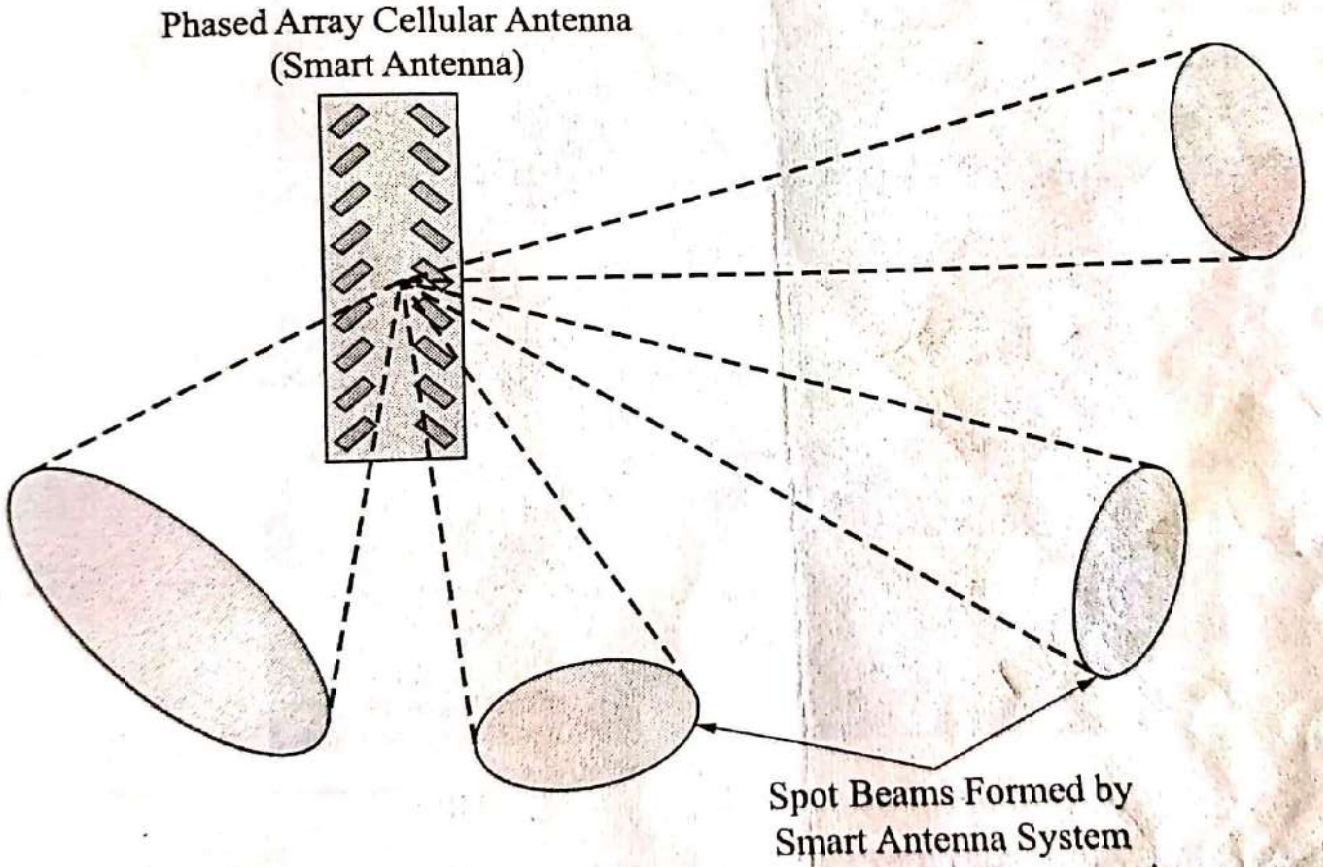

Figure 8–18 Depiction of a 3G smart antenna system.

4.5 MOBILITY MANAGEMENT

The most important characteristic of wireless telecommunications systems is the ability to provide mobility to the user. The general public has demonstrated its desire for "untethered" electronic communications many times since the first radio signals were transmitted over 100 years ago. Whether it has been the acceptance of car radios, cordless telephones, or cellular phones, the early rate of adoption of each of these innovations has been exponential in nature. The number of worldwide mobile telephone subscribers is predicted to pass two billion by the year 2007. As stated before, wireless mobile telephones are evolving into more than just voice-oriented devices. Modern mobiles or subscriber devices have the ability to provide data services and access to the Internet with ever increasing data transmission rates. The functionality of these subscriber devices is being enhanced by multimedia capabilities that support voice, high-quality audio, and video messaging. Cell phones with built-in video cameras are in fact here and no longer just a futuristic invention made popular by the Dick Tracy comic strips of so many years ago.

With the likelihood of the cellular subscriber base exceeding more than two billion within this decade, one might pause for a moment to consider the complexity of the systems needed to manage all these users. Certainly there is a need for a physical infrastructure to support the operations mentioned earlier but there also is a need for a radio network that manages the countless operations needed to make the entire system function correctly.

Contrast a wireless system with a traditional wireline system where the physical infrastructure is connected to the fixed subscriber device and therefore the signals are guided by the transmission media to the correct destination. Indeed, although the PSTN needs a switching "fabric" at the core of the network to direct one's call to the correct telephone, once the connection is made, there is an end-to-end physical path for the signal to propagate over. A wireless system does not have the luxury of knowing where the mobile subscriber is at all times and therefore must incorporate a means to determine this information and subsequently infuse this data into the system. At the same time, a mobile station should have the ability to be able to continuously access or use the services of the system that it is connected to. Wireless network functionalities necessary for efficient system operation are achieved through the use of programmable information processing systems and information data-bases built into the major system components (e.g., MSC and BSC) and the radio signal measurement capabilities built into the air interface components (i.e., base and mobile stations). The next several sections will discuss the concept of mobility management for cellular systems. The goal of these sections is to explain how the network knows where the subscriber is (location management) and how it keeps track of and in contact with the mobile station as the subscriber moves around from cell to cell (handoff management).

Mobility management for wireless LANs and other wireless data networks covered by the IEEE 802.XX standards will be covered in the chapters devoted to those topics.

Location Management

Location management is the process of keeping track of the present or last known location of a mobile station and the delivery of both voice and data to it as it moves around. Since there are literally hundreds of thousands of worldwide cell sites, there needs to be functionality built into every cellular system that will provide the system with the ability to locate one particular mobile station out of the billion plus in existence. This process is best explained, in the case of a voice call, as follows: When a call is made that passes through the PSTN, a dedicated traffic channel must be set up from the BS to the MS for a call to be completed. The PSTN sets up the circuit over the fixed part of the network and the wirel

Location Management

Location management is the process of keeping track of the present or last known location of a mobile station and the delivery of both voice and data to it as it moves around. Since there are literally hundreds of thousands of worldwide cell sites, there needs to be functionality built into every cellular system that will provide the system with the ability to locate one particular mobile station out of the billion plus in existence.

This process is best explained, in the case of a voice call, as follows: When a call is made that passes through the PSTN, a dedicated traffic channel must be set up from the BS to the MS for a call to be completed. The PSTN sets up the circuit over the fixed part of the network and the wireless network will

allocate a pair of radio channels for the air interface connection. Naturally, for this process to be successful, the location of the MS must be known. Additionally, if the mobile moves during the time span of the conversation, a process must be in place to provide for a continuous radio link even though the mobile might move into another cell. For the case of a data transfer, packets are typically addressed to an end terminal or destination device. The packets are directed through the data network by routers to a particular device. For a fixed device this corresponds to a fixed location. For the mobile device it is necessary to know the location of the device before the data packet can be delivered to it. Furthermore, the system must know the availability of the called party. In a fixed system, busy signals are used to denote a telephone already in use. For a mobile system, the mobile may be in use or may not even be turned on. In both of these cases, the network must be able to determine the status of the mobile and take the necessary action to deal with the incoming call or data transfer. This action might be the playing of a recorded message indicating that the mobile is busy and then implementing an answering machine function or the storage of the data transfer information on some type of network storage device for later delivery.

In general, there are three basic functions performed by location management: location updating, sending paging messages, and the transmission of location information to other network elements. The next several sections will examine these generic network operations in more detail. Later chapters will provide system-specific details.

Location Updating

The location updating function is performed by the mobile station. Recall that when the MS is first turned on, it performs an initial system registration or "attach" with the base station of the cell that it is located in and thereafter this information is periodically checked to verify its accuracy and prevent an accidental detach of the mobile from the system. If the mobile does not change location, the access point to the fixed network remains unchanged and the fixed portion of the wireless network delivers information to the mobile using this particular access point.

The system is designed so that the mobile station will send an update message every time it changes its point of access to the fixed network. As stated earlier, after the initial power-up registration the mobile station and base station will periodically exchange their respective identification information. If the MS receives the ID of a BS or a location area (LA) that is different from the value stored in its memory (this could happen through a handoff during a call or simply be due to the mobile's change of location), the MS will send a location updating request message to the fixed network through this new access point and also provide information about the mobile's previous access point. This information will be entered into a VLR database maintained by the fixed portion of the wireless network and be used by the network to locate the MS. The motion of the MS can therefore be tracked by this process to a specific LA or base station. This process has its drawbacks because updates are periodic and therefore introduce some uncertainty into the exact location of the mobile. In an extreme case, a mobile may be turned off and transported across the country by the subscriber. In this instance, an incoming call to the mobile while it is out of service will result in a page being sent to the last known access point, which would produce a no response or failed page. After that failed attempt, the system might possibly page a group or groups of surrounding cells, which will also fail. The system would then enter its voice message mode indicating the unavailability of the mobile. When the mobile is turned on again, this problem will be resolved by the system when new registration information is received and the mobile's location is updated within the fixed portion of the system. Now any calls will be directed to the mobile's new location.

A balance needs to be achieved by the wireless network involving the number of update messages and the number of cells that must be paged by the system to locate the mobile. If updating is performed very frequently, the location of the mobile will be known with a greater degree of certainty; however, the system resources (both radio and network) used to accomplish this task will be excessive. On the other hand, if updating is performed infrequently, the number of access points that need to be paged to find the mobile increases and may have the adverse effect of causing too many calls to be dropped or data packets lost due

to long delays in the determination of the mobile's location. A forthcoming example will illustrate a typical system that provides a compromise between these two conflicting goals.

There are usually two types of updating schemes used by wireless networks—static and dynamic. For static schemes, the cellular network's geographic layout determines when the location updating needs to be initiated. For dynamic schemes, the user's mobility and the cellular system layout both contribute to the initiation of the location updating algorithm.

Today, most cellular systems use the static method of location updating (see Figure 4–14). In this approach, a group of cells is assigned a location area identification value (LAI) (refer back to Figure 3–9). As shown in Figure 4–14, each BS in the LA broadcasts its ID number in a periodic fashion over a control channel. The MSs that are attached to the base stations within the LA are required to listen to the control channel for the LA ID. If the LA ID changes, the MS will have to send a location update message to the new base station. The BS will forward the updated information to the VLR database located in the fixed portion of the wireless network. Now, if there is an incoming message for an MS, a paging message will be sent to all the cells in the LA where the MS is listed as being present. The MS, unless it has moved into another LA, will respond to the paging message. One problem faced by a static location area ID scheme is known as the "ping-pong" effect. This effect can occur if the mobile is moving in a path that takes it back and forth between the borders of two LAs. This problem can also affect the handoff process. Practical solutions used to prevent this effect will be presented when handoff is discussed.

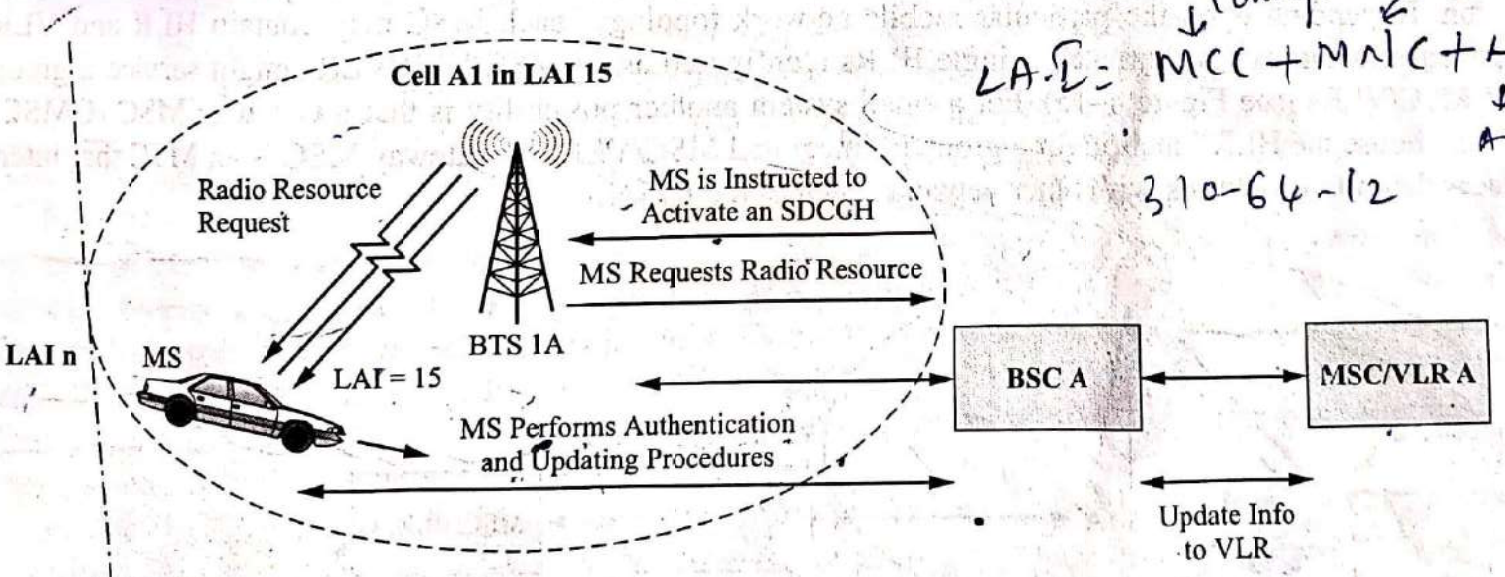

Figure 4–14 Cellular location updating.

Dynamic location updating plans are not as popular within the wireless industry. These schemes are typically based on the status or state of the mobile. Some of the typical measures used to determine the mobile's status and hence determine the need to perform the updating algorithm are elapsed time, total distance traveled, call patterns, number of different LAs entered, and so on.

Paging Messages

An incoming call or message to a mobile station will initiate the paging of the mobile. Paging consists of the broadcasting of a message either to a cell or to a group of cells that is meant to bring a response from a single particular mobile. This response will start the process by which communications between the PSTN or the PDN will be established with the mobile. The paging of a mobile is more efficient if the exact cell the mobile is registered in is known. However, as pointed out, this information is not always available. Therefore, several different strategies for paging exist. Sometimes a scheme known as blanket paging is employed. This type of a page will be broadcast to all cells in a particular location area. If successful, the mobile will respond after the first paging cycle and delays will be kept to a minimum. Otherwise, a scheme of sequential paging is used. In this paging strategy, the cell where the mobile was last registered is paged

first. If not successful, the next group of surrounding cells is paged. If this attempt to reach the mobile is still not successful, another larger ring of surrounding cells is paged and so on until the page is successful or a paging cycle timer expires and the MS is declared unreachable by the system. Depending upon several system variables, both paging schemes offer various advantages and disadvantages.

Transmission of the Location Information between Network Elements

For location updating to work correctly in a wireless network, there must exist several databases where mobile station information can be stored and accessed by the network as needed. When a subscriber enters into a service contract with a service provider, the subscriber's mobile device is registered (i.e., mobile ID numbers are stored) in a home location register (HLR) maintained by the subscriber's home network. This HLR database is usually colocated with the mobile switching center (MSC) and also stores the user's profile, which includes permanent data about subscribers, including call plan supplementary services, location information, and authentication parameters. Another database known as the visitor location register (VLR) is also maintained by the home network and also usually colocated with the MSC (MSC/VLR). The home VLR will temporarily store information about any MS that has registered itself with the home network. Therefore, if an MS is turned on by a subscriber in the user's home network area, the home VLR will temporarily store that user's information.

Within a particular network there are usually several to many MSCs used to support the network's operation. Depending upon the particular mobile network topology, each MSC may contain HLR and VLR database functions or, alternately, single HLRs (configured as an MSC/HLR/VLR) might service a group of MSC/VLRs (see Figure 4–15). For a small system another possibility is that a Gateway MSC (GMSC) might house the HLR function for a group of integrated MSC/VLRs. A gateway MSC is an MSC that interfaces the mobile network with other networks such as the PSTN.

first. If not successful, the next group of surrounding cells is paged. If this attempt to reach the mobile is still not successful, another larger ring of surrounding cells is paged and so on until the page is successful or a paging cycle timer expires and the MS is declared unreachable by the system. Depending upon several system variables, both paging schemes offer various advantages and disadvantages.

Transmission of the Location Information between Network Elements

For location updating to work correctly in a wireless network, there must exist several databases where mobile station information can be stored and accessed by the network as needed. When a subscriber enters into a service contract with a service provider, the subscriber's mobile device is registered (i.e., mobile ID numbers are stored) in a home location register (HLR) maintained by the subscriber's home network. This HLR database is usually colocated with the mobile switching center (MSC) and also stores the user's profile, which includes permanent data about subscribers, including call plan supplementary services, location information, and authentication parameters. Another database known as the visitor location register (VLR) is also maintained by the home network and also usually colocated with the MSC (MSC/VLR). The home VLR will temporarily store information about any MS that has registered itself with the home network. Therefore, if an MS is turned on by a subscriber in the user's home network area, the home VLR will temporarily store that user's information.

Within a particular network there are usually several to many MSCs used to support the network's operation. Depending upon the particular mobile network topology, each MSC may contain HLR and VLR database functions or, alternately, single HLRs (configured as an MSC/HLR/VLR) might service a group of MSC/VLRs (see Figure 4–15). For a small system another possibility is that a Gateway MSC (GMSC) might house the HLR function for a group of integrated MSC/VLRs. A gateway MSC is an MSC that interfaces the mobile network with other networks such as the PSTN.

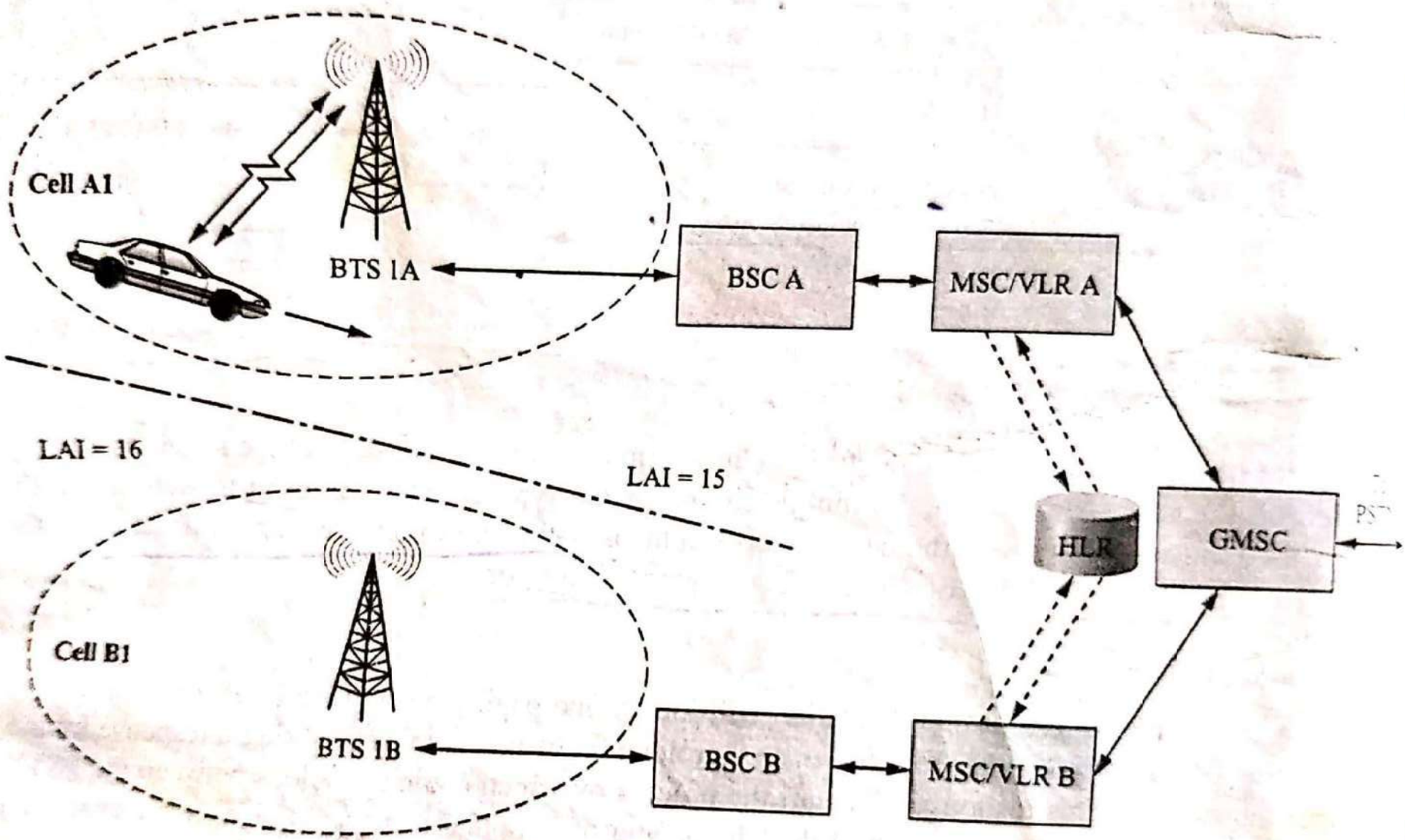

Figure 4–15 A typical cellular system.

At this time, let us examine several possible scenarios that could occur during the operation of a wirele network. The first possibility has already been mentioned; the user turns on a mobile within his or her hom area. The mobile registers with the VLR for the home area. The colocated or system HLR confirms that th

Handoff Management

It addition to the location management functions already described, a cellular system needs to be able to track the location of a subscriber as that subscriber moves within a coverage area and to be able to maintain the subscriber's connection to the system. If the subscriber moves from one cell to another, the cellular system must have the ability to reconfigure the connection to the mobile from the current base station to the new BS in the new cell. This connection handover process is known as **handoff.**

For first-generation cellular systems, the handoff process for voice calls could cause a noticeable interruption of the conversation (a hard handoff) and in some severe cases dropped calls. Second-generation cellular systems using digital technology have mitigated some of these problems with seamless handoffs, and CDMA systems have incorporated soft handoffs into their systems thus all but eliminating interrupted calls. For data transmissions, handoff can result in dropped packets, but this is not as severe a problem for bursty or packet data traffic since this type of traffic only needs intermittent connectivity and retransmission can be employed to counteract lost packets.

As shown in Figure 4–16, handoff basically consists of a two-step process. First, a handoff management algorithm determines that handoff is required and initiates the process. The second step consists of actually physically restructuring the connection and then updating the network databases about the new connection and location of the MS. For the handoff process to be successful the network elements involved in the delivery of either voice or data services to the mobile must be aware of all changes to the mobile's point of access. On the air interface side of the system, the former serving point has to be informed about the change or dissociation of the mobile while the mobile is reassociated with the system through the new serving point. On the network side, the various databases must be updated to reflect the correct location of the MS. This is all necessary for the correct routing of data packets or voice calls. The next sections will provide more detail about these operations.

Handoff Control

The algorithm used to determine when to make a handoff can be located in a network element or in a mobile terminal. For cellular systems the network controls the handoff for voice calls and this is known as network-controlled handoff or NCHO. If the mobile terminal controls the handoff, this is known as mobile-controlled handoff or MCHO, and if information supplied by the mobile helps determine when handoff should occur, this is known as mobile-assisted handoff or MAHO. In all cases, the handoff-controlling entity uses some particular algorithm that employs various measures of system performance to make a decision about the need for handoff.

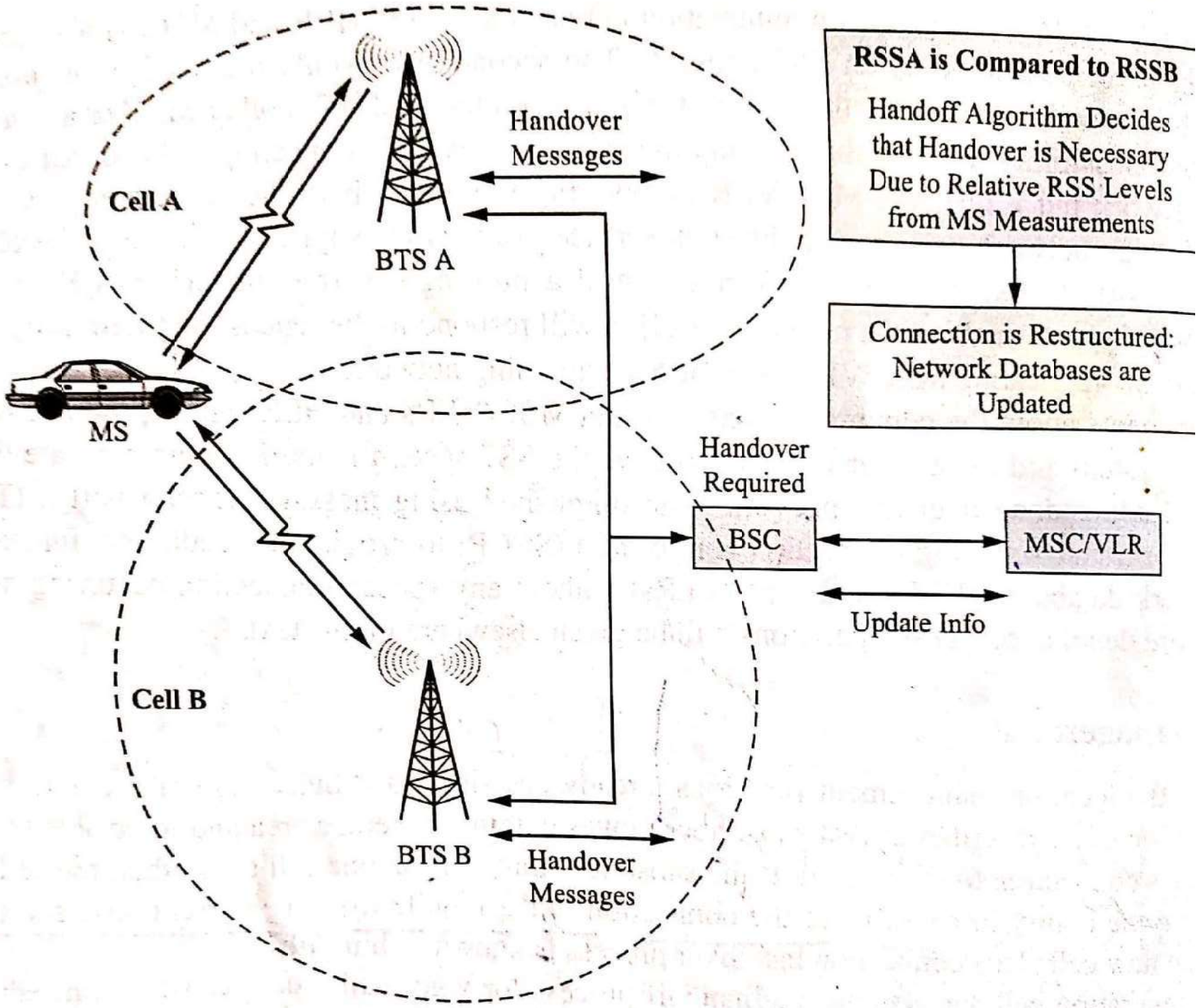

Figure 4.16 Typical cellular handoff operations

Figure 4–16 Typical cellular handoff operations.

The most common measurement used in this process is the received signal strength (RSS) from the mobile's point of attachment and the RSS of the nearest other possible points of attachment (i.e., radio base stations in adjacent cells). Other associated measurements that might be included in the process are system path loss, carrier- and signal-to-interference ratios and measures of bit error rate (BER), symbol or block error rate, and so on. A problem with using signal-strength measurements is that received signal strength can undergo extreme fluctuations due to signal fading effects that are completely random in nature. Error rates are also similarly affected by the randomness of propagation conditions.

Traditional handoff algorithms would initiate handoffs when the power received from the current RBS dropped below that received by another nearby RBS. Additional fine-tuning of the algorithm has incorporated threshold levels and hysteresis to prevent erroneous handoff requests and to mitigate the ping-pong effect mentioned earlier. As an example, with both threshold and hysteresis, handoff will only occur if the received power from a nearby RBS is above that received from the current RBS by a certain hysteresis value and the power from the current RBS is also below a certain threshold power level. Figure 4–17 shows some examples of the possible different algorithms used for handoff decision making in conjunction with the signal power being received by the current RBS and the signal power from a RBS that the MS is approaching.

Cellular service provider engineers are continually fine-tuning system handoff algorithms to improve system performance. Measures of system performance might include such things as call blocking and call dropping probability, required time to complete a handoff, and system handoff rate. Although these performance measures are typically used to improve the delivery of voice calls and the efficiency of the network, they might not necessarily result in higher data throughput rates or provide for required QoS continuity during a handoff, all important issues in the delivery of data services.

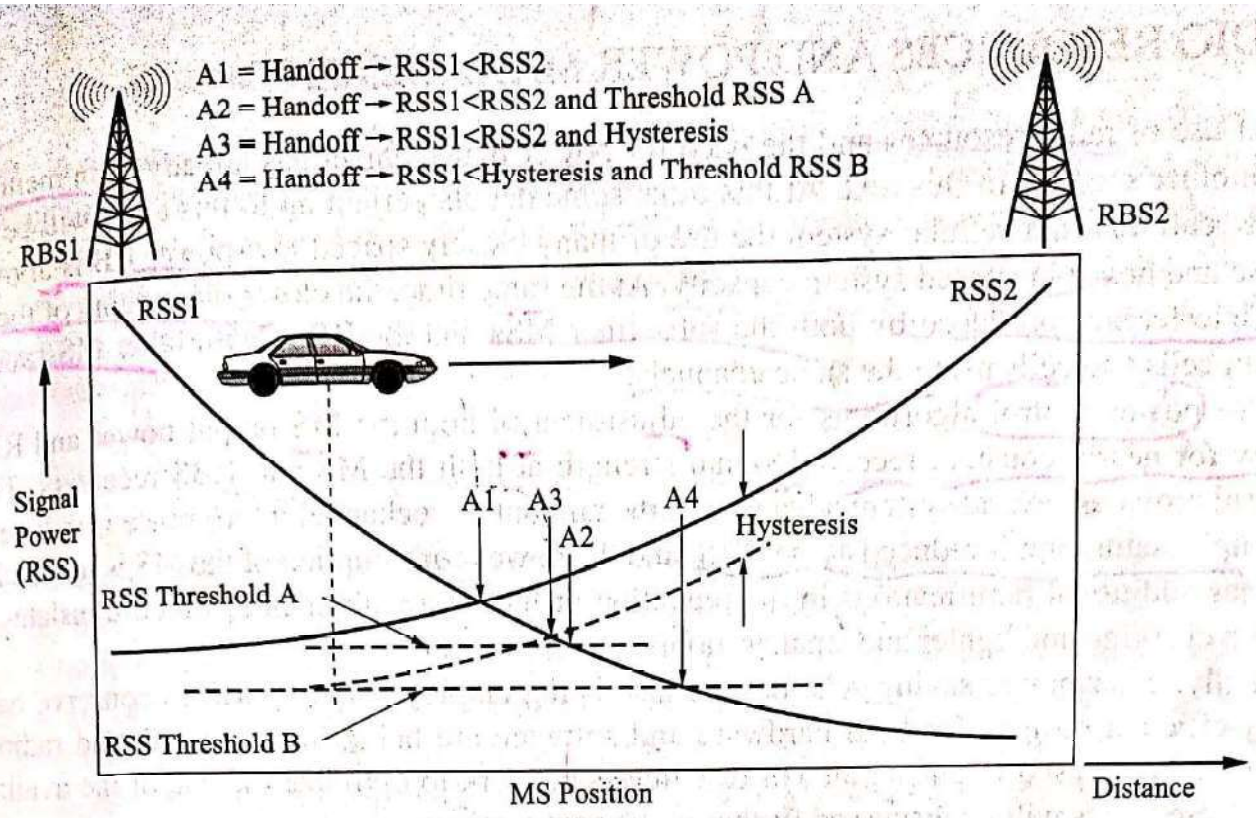

Figure 4–17 Typical handoff algorithms using RSS measurements.

Handoff Operations

Handoff management requires the transmission of messages between various network elements to facilitate the handoff process. As depicted in Figure 4–16, signal power levels being received by the current and handoff candidate radio base stations and the mobile station are first relayed to the radio base station and then to the base station controller (BSC). When these levels meet the criteria for a handoff, the process is initiated. A handoff message is sent to the mobile from the current radio base station that requests the mobile station register with a new radio base station that is also identified in the message. When the mobile performs this task, the MSC/VLR is updated to reflect the new mobile point of attachment (i.e., the new RBS) and any other changed system parameters. If the MSC/VLR most recently registered with is not the same as the last, then the new VLR must send an interrogation message to the home HLR to obtain the subscriber profile and authentication information. The HLR responds over the SS7 network with the authentication information. If the mobile is authenticated, then the new radio base station sends a message to the mobile assigning a new pair of traffic channels to the MS and the RBS for the continuation of a voice conversation. The HLR database is updated so that it knows where the mobile is and the new VLR database adds the new mobile to its list of subscriber terminals that are being serviced by the particular MSC/VLR. As a last act, the HLR sends a message to the old MSC/VLR to purge the mobile from its list of actively attached subscriber terminals. More detail about handover operations will be given in Chapter 5. Additionally, any data packets that were intended for delivery to the MS from the old MSC/VLR that may have been placed in a temporary network storage area should be either deleted or redirected to the new MS access point.

As one can see, there are many necessary message transfers occurring between wireless network elements and subsequent operations to be performed by these same elements for a successful mobile station handoff. There are also other types of possible handoffs that have not been addressed here such as the various types of intracell or intra-BSC handoffs. Since the exact details of mobility management procedures for different cellular systems are specific to those systems, more details will be provided about these topics in later chapters when individual systems (GSM, TDMA, and CDMA) are covered.

4.6 RADIO RESOURCES AND POWER MANAGEMENT

The efficient use of radio resources and the need for power management has already been mentioned several times in other sections of this text. At this time, some details pertaining to this topic will be offered to the reader. Recall that in a cellular system the use of many closely spaced low-power RBSs allows for frequency reuse and hence increased system capacity. At the same time, the closer the spacing of the RBSs the greater the interference produced by both the subscriber MSs and the RBSs with other MSs and RBSs in both adjacent cells and cells using the same channels.

The use of power control algorithms for the adjustment of both the MS output power and RBS output power allow for nearly constant received signal strength at both the MS and RBS receivers. This use of power control provides several system advantages: the amount of cochannel interference is reduced, the risk of signal coupler saturation is reduced at the RBS, and the power consumption of the MS is reduced. This last advantage has additional ramifications in the reduction of battery requirements, which translates to longer time between charging and lighter and smaller mobile terminals.

Additionally, other power saving schemes are also being employed by the MS to conserve battery life, new energy-efficient designs for both hardware and software are being implemented, and radio resource management is being used to enable an MS or wireless network to optimize the use of the available radio resources. These topics will be discussed further in the next sections.

Power Control

As stated previously, cochannel interference is the limiting factor for the reduction of cluster or frequency reuse size, *N*. The use of power control algorithms for the output power of the MS and the RBS allows the system to use the lowest possible output powers to achieve the minimum S/I ratio that can be tolerated and still provide good-quality communications. This means that for an MS close to the RBS both devices will lower their output power and as the mobile moves farther from the RBS both devices will in all likelihood have to increase their output power. Any reduction in output power from the nominal design power for the RBS or MS will produce a reduced amount of cochannel and adjacent channel interference for other cells using the same frequency channels.

Since the power output of both the RBS and the MS must be constantly adjusted due to the numerous changes in signal strength caused by fading and any motion of the mobile, several different methods of power control can be employed in a wireless network.

One typical system algorithm for power control usually consists of two phases. The first phase occurs when the MS initially registers with the system upon power-up. In this phase, the MS uses the nominal (maximum) power output allowed by the system. The first measurements of signal strength made by the RBS are used by the BSC to determine a valve of reduced MS output power. Power control messages are quickly sent to the MS to reduce its output power; however, this first power reduction is usually limited to avoid the possibility of a dropped call. In the second phase of this process, additional measurements are made and the MS power is adjusted as needed. The power output of the RBS is also adjusted on a case-by-case basis to yield the required signal strength at the MS. In this situation, whenever a new connection is made, the RBS initially transmits with its nominal or maximum output power. As done with the MS, the output power of the RBS is quickly reduced to a point where more stable measurements can be made and then the power control algorithm adjusts the output power as needed. If the mobile is operating in the discontinuous transmission mode, the algorithm must be modified to take this fact into account.

Another possible power control method employs a complex algorithm that uses information about all active radio links in a system to adjust the output powers of all the RBSs and MSs to achieve maximum and also equal S/I ratios for all radio links. In each of these systems, output powers are usually adjustable in incremental steps of 2 dB or less.

Power Saving Schemes

In addition to the power saving schemes outlined in the previous section, there are several other ways in which MS battery power may be conserved. It is well known that the mobile consumes the greatest amount of power during the transmission of a signal to the RBS. Less power is consumed during the reception of a signal from the RBS. Another mode of MS operation can exist and that is known as "standby." In a standby mode, much less power is consumed by the mobile than in either the transmission or reception mode. There are several techniques used with mobile stations to achieve standby status.

Discontinuous Transmission

Using speech detection methods, a mobile may be programmed to only transmit when there is speech activity by the user. The radio base station sets a discontinuous transmission (DTX) bit to either permit or disallow this mode of operation and includes it in an overhead message to the mobile during initial registration by the mobile. Just using straight speech detection methods can cause problems due to the unnatural resulting sound of the system as perceived by the users. To compensate for this, a low-power background or comfort noise signal is generated by the mobile receiver during gaps of silence or no speech activity. This operation is also repeated at the base station controller or TRC for the benefit of the calling party.

Sleep Modes

Another common technique used to save MS battery power is to put the MS into a sleep mode when there are periods of no activity. For this scheme, the RF portion of the mobile's circuitry is powered off while waiting between messages. The mobile will periodically awaken and read control channel messages from the system so as to not miss a paging message but with much less overall power consumption.

Energy-Efficient Designs

The use of the most power-efficient semiconductor technologies is normally a given in the design of cellular mobile stations. Additional power saving can be achieved through the use of power-efficient modulation and coding schemes. However, another area that can provide power efficiencies is in the design of the protocols used in a wireless network and in the software design employed by the MS itself. As the cellular world evolves toward universal 3G deployment, system designers are implementing these protocol- and software-based power saving ideas and designs into new systems. As digital signal processor (DSP) technology advances, the eventual use of software radios will be another step in the evolution of lower-power, reconfigurable, advanced wireless radio systems that can last longer between battery recharges.

Radio Resource Management

Radio resource management is used to provide several functional improvements and necessary operations to permit the correct operation of a wireless network. The first and most important aspect of radio resource management is to implement system power control that reduces interference and therefore allows for system capacity to be maximized. As pointed out before, a side benefit of this control function is the increase in MS battery life. Another improvement afforded to the system is that the MS is directed toward the best radio channel connection available to it within the cell. This is made possible by the constant transmission of measurement information from the MS to the BS and then to the BSC. Finally, the use of a wireless network radio resource management scheme enables the handoff operation. Without this network management function, handoff could not operate as seamlessly and efficiently as it does in today's systems. More details of radio resource management functions and organization used by particular radio systems will be presented in the chapters devoted to the individual systems.

4.7 WIRELESS NETWORK SECURITY

Unlike wireline telecommunications systems that usually provide some modest amount of security throug infrastructure design and physical installation, wireless technologies pose special security concerns. Th unguided nature of wireless signals exposes them to the possibility of undesired interference and interce tion. This section will present some of the security requirements for both the air interface and the fixe infrastructure of the wireless network itself and conclude with a brief overview of present wireless securit techniques.

Wireless Network Security Requirements

Just as the wireline telecommunications networks require increasingly more effective security in this post 9/11 world, the security requirements of wireless networks are very similar to their wired counterparts. The need for privacy in the transmission of a voice conversation is necessary regardless of the means used to deliver the signal. The ability for anyone to attain the unauthorized interception of a private conversation is not a desired feature of any telecommunications system. The newer digital cellular systems make any interception of voice conversations extremely difficult due to the conversion of the voice signals from analog to digital form and the ciphering of the transmitted digital information by the system. However, with the increasing use of wireless data services and e-commerce activities, the need for more secure wireless networks is becoming more important as more wireless cellular users avail themselves of these new data services and more sensitive economic information is transmitted over wireless networks.

In addition to the transmission of voice or data traffic over the air interface, a certain amount of sensitive control and identification information is transmitted over control channels to the fixed wireless network. There is certainly a potential for the misuse of this type of information and the possibility of someone obtaining telecommunication services (teleservices) fraudulently as happened with the first-generation analog cellular system.

Presently the GSM Association maintains a global central equipment identity register (CEIR) database in Dublin, Ireland, of all handsets that have been approved for use on GSM networks. The database categorizes these approved handsets as being on a White List. There is also a CEIR Black List of handsets that should be denied access to the network due to being reported as either lost or stolen or otherwise unsuitable for use. GSM cellular operators that employ an EIR in their network use it to keep track of handsets to be blocked. If they are also registered users of the CEIR, they call in daily to share their database with the CEIR, and each day the CEIR creates a master Black List that the operator can download the following day. In this way any stolen or lost handset is blocked by the next day after it has been reported missing.

Network Security Requirements

In addition to the privacy and fraud concerns for the air interface portion of the network, there are also security issues involving the fixed portion of the network. The fixed wireless network infrastructure includes numerous network elements that are involved in identification, authentication, billing functions, and so on. However, most of these network elements and the transmission facilities between them enjoy the same level of physical security (or lack thereof) as the traditional PSTN or PDN telecommunications systems. As the wireless cellular system transitions to an all-IP network there will be a need to employ increased security measures to prevent hacking of the system and the possible infection of system components by software viruses. After the events of 9/11, the threat of terrorism is all too real and one can no longer discount any type of infrastructure target as being unrealistic.

Network Security

There are several methods by which the security of air interface messages can be enhanced. The most viable method is to employ encryption techniques. These techniques rely on the scrambling of the message using

particular key to perform the encryption. Various encryption techniques have been used since the need for confidentiality first arose. Most encryption techniques are known as secret-key algorithms since the key to the encryption is kept secret from everyone but the two end users of the communications channel.

However, as complex as one can make the encryption process it seems that it is always possible to break the code given enough computational power and time. The field of telecommunications infrastructure security is a very hot research topic right now with the reality of a proliferation of attacks on the Internet as well as the high threat of global terrorism. As with many of the topics discussed to this point, security details of particular wireless systems will be presented with the particular technology.

Security issues concerning wireless LANs will be presented in the chapters addressing IEEE 802.XX wireless technology.

QUESTIONS AND PROBLEMS

1. What factors determine frequency reuse distance?
2. What advantage does the use of a cellular architecture provide?
3. What factors limit cell size?
4. A cell tower located near an interstate highway would most likely provide service to what type (size) of cell?
5. Determine the frequency reuse distance for a cell radius of twenty kilometers and a cluster size of 7.
6. Determine the frequency reuse distance for a cell radius of two kilometers and a cluster size of 4.
7. Construct a chart that shows how a cellular system with a cluster size of 4 could have twenty-eight channels assigned to the system in such a manner as to maximize channel spacing.
8. For a particular radio transmission technology, a minimum S/I ratio of 15 dB is needed for proper operation. What is the minimum required cluster size?
9. What will be the resulting (ideal) increase in cellular system capacity for a typical cell splitting scheme?
10. For a cell splitting scenario, why must the cell transmit power be reduced?
11. How is cell splitting different from cell sectoring?
12. What possible limitations can you conceive that would impose a practical limit on cell sectoring?
13. What is the driving force for the adoption of microwave cellular backhaul networks?
14. What has been the traditional method used to provide connectivity between the cellular network and the PSTN?
15. If and when the all-IP core network becomes a reality, how will voice traffic be carried to the cellular network?
16. Mobility management consists of several basic functions. What are they?
17. When does the location updating function occur?
18. What two basic operations occur during the handoff process?
19. Why is power management so important for cellular wireless systems?
20. Describe the process of power control used by cellular systems.
21. What is meant by the term *discontinuous transmission* in the context of wireless cellular systems?
22. What is meant by the term *sleep mode* in the context of wireless cellular systems?
23. Describe how the GSM Association provides a form of security to its members.
24. What is the basic form of security employed by cellular wireless systems?
25. Describe secret-key encryption.