Overview of Radiolocation in CDMA Cellular Systems

James J. Caffery, Jr. and Gordon L. Stüber
Georgia Institute of Technology

ABSTRACT Applications for the location of subscribers of wireless services continue to expand. Consequently, location techniques for wireless technologies are being investigated. With code-division multiple access (CDMA) being deployed by a variety of cellular and PCS providers, developing an approach for location in CDMA networks is imperative. This article discusses the applications of location technology, the methods available for its implementation in CDMA networks, and the problems that are encountered when using CDMA networks for positioning.

Wireless location has received considerable attention over the past few years. A recent Report and Order issued by the U.S. Federal Communications Commission (FCC) in July 1996 requires that all wireless service providers, including cellular, broadband PCS, and wide-area SMR licensees, provide location information to Emergency 911 (E-911) public safety services [1]. These new FCC E-911 requirements have boosted research in wireless location. The basic function of a location system is to gather information about the position of a mobile station (MS) operating in a geographical area and process that information to form a location estimate. A popular approach, known as *radiolocation*, measures parameters of radio signals that travel between an MS and a set of fixed transceivers, which are subsequently used to derive the location estimate.

Many existing wireless location systems, such as the Global Positioning System (GPS) and Loran C, make use of radiolocation techniques. With these technologies the MS formulates its own position, which can be relayed to a central site. Some approaches employ a cellular network as the transport mechanism for relaying the location estimate [2]. As an alternative to these approaches, cellular networks can be used as the sole means of providing location services, where the MSs are located by measuring the signals traveling to and from a set of fixed cellular base stations (BSs). The signal measurements are used, for example, to determine the length and/or direction of the individual radio paths, and then the MS position is computed from geometric relationships [3].

Radiolocation systems can be implemented in one of two ways. With the first approach, the MS uses signals transmitted by the BSs to calculate its own position, as in GPS. With the second approach, the BSs measure the signals transmitted by the MS and relay them to a central site for processing. The second approach has the advantage of not requiring any modifications or specialized equipment in the MS handset, thus accommodating the large pool of handsets already in use in existing cellular networks.

The remainder of this article presents an overview of wireless location in code-division multiple access (CDMA) cellular networks. The second section discusses the potential applications of wireless location. The third section provides an overview of wireless location methods, followed by the accuracy requirements for specific applications in the fourth section. The remainder of the article discusses wireless location in CDMA cellular networks, including location algorithms in the sixth section, sources of error in the seventh section, and system loading aspects in the final section.

APPLICATIONS OF WIRELESS LOCATION

Wireless location using CDMA cellular networks brings with it the possibility of several applications which will benefit businesses as well as consumers. The potential applications include:

- E-911
- Location-sensitive billing
- Fraud detection
- Cellular system design and resource management
- Fleet management and intelligent transportation systems (ITS)

Location information for wireless E-911 calls permits rapid response in situations where callers are disoriented, disabled, unable to speak, or do not know their location. An increasingly large fraction of E-911 calls are placed by cellular phones, which is a direct result of the growing number of cellular subscribers. In 1994, approximately 50,000 wireless E-911 calls per day were made in the United States, a figure that increased to 60,000 in 1996. By the year 2000, it is estimated that this figure will grow to 130,000. A recent study by the state of New Jersey indicated that wireless E-911 calls accounted for 43 percent of all E-911 calls received during wireless location trials [4].

The wireless E-911 services outlined in the 1996 FCC ruling are to be implemented and deployed in two phases. Phase I, to be completed by April 1, 1998, requires that the carriers relay the location of the cell site and/or sector receiving the E-911 call and the E-911 caller's telephone number (known as the Automatic Number Identification, or ANI) to the designated Public Safety Answering Point (PSAP), thereby allowing the PSAP to call back if the call is disconnected. Phase II, to be completed by October 1, 2002, requires that wireless carriers be able to report the location of all E-911 callers with an accuracy of 125 m (410 ft) in 67 percent of cases.

Location-sensitive billing provides a wireless carrier the ability to offer different rates depending on whether the wireless terminal is used at home, in the office, or on the road [5]. This will allow wireless carriers to offer new rate choices for their subscribers and offer rates that will bring new subscribers into their customer base. It also enables a carrier to encourage desirable usage behavior by employing location price discrimination.

Another lucrative application for location technology is in the ongoing battle against cellular phone fraud. Some carriers

0163-6804/98/$10.00 © 1998 IEEE

estimate that up to 1 percent of their customer base experiences fraud each month. Annual industry fraud ranges in the area of $500 million, all of which is passed on to wireless customers in the form of higher phone usage rates. Without the use of wireless location systems, it is very difficult to find and catch the perpetrators.

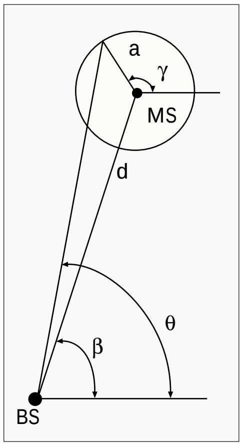

Figure 1. *The scattering model for propagation in macrocells. The MS is a distance* d *from the BS and is surrounded by a scattering ring of radius* a *[12, 14].*

Location technology could also be used in wireless system design and for radio resource and mobility management [6,7]. With the ability to locate a wireless call, system planners could dramatically improve their ability to architect cells and wireless systems. Cells could be better positioned and tuned, and spectral efficiency improved. More effective resource management could be obtained through the allocation of channels based on the knowledge of the wireless caller's location. Moreover, a service provider who may have multiple agreements with PCS, cellular, or satellite carriers could offer its customers the ability to choose a carrier that best suits their needs at any given time and location [8], thereby allowing the service provider to offer its customers a selection of carriers and price advantages.

Wireless location technology is also useful for fleet operations. Many fleet operators already make use of location technology to track their vehicles and operate their fleets more efficiently, thus improving their field service. Police and emergency vehicles, as well as taxi and other service operators, could also improve their field service through the use of location technology. Having knowledge of the location of their vehicles allows a dispatcher to locate the nearest available vehicle, greatly improving response times.

OVERVIEW OF RADIOLOCATION METHODS

Radiolocation systems can be implemented that are based on either signal strength, angle of arrival (AOA), or time of arrival (TOA) measurements, or their combinations. The signal measurements are used to determine the length or direction of the radio paths to/from an MS from/to multiple BSs. This article only considers the case where the signal measurements are made at the BSs. We note that line of sight (LOS) propagation to the BSs is essential for highly accurate location estimates.

SIGNAL STRENGTH

Radiolocation using signal strength is a well known location method that uses a known mathematical model describing the path loss attenuation with distance [9,10]. Since a measurement of signal strength provides a distance estimate between the MS and BS, the MS must lie on a circle centered at the BS. By using multiple BSs, the location of the MS can be determined.

For signal-strength-based location systems, the primary source of error is multipath fading and shadowing. Variations in the signal strength can be as great as 30–40 dB over distances on the order of a half wavelength (1/2-λ). Signal strength averaging can help, but low-mobility MSs may not be able to average out the effects of multipath fading, and there will still be the variability due to shadow fading. The errors due to shadow fading can be combatted by using premeasured signal strength contours centered at the BSs [11]. However, this approach assumes a constant physical topography and requires that contours be mapped out for each BS.

Finally, in CDMA cellular systems the MSs are power controlled to combat the near-far effect. Time-division multiple access (TDMA) cellular systems use power control to conserve battery power in the MSs. Therefore, for signal-strength-based systems it is necessary that the transmit power of the MSs be known and controlled with reasonable accuracy.

ANGLE OF ARRIVAL

AOA techniques estimate the MS location by first measuring the AOAs of a signal from an MS at several BSs through the use of antenna arrays. Scattering near and around the MS and BS will alter the measured AOA. In the absence of an LOS signal component, the antenna array will lock on to a reflected signal that may not be coming from the direction of the MS. Even if an LOS component is present, multipath will still interfere with the angle measurement. The accuracy of the AOA method diminishes with increasing distance between the MS and BS due to fundamental limitations of the devices used to measure the arrival angles as well as changing scattering characteristics.

For macrocells, scattering objects are primarily within a small distance of the MS, since the BSs are usually elevated well above the local terrain [12, 13]. Consequently, the signals arrive with a relatively narrow AOA spread at the BSs. Jakes [12] and Gans [14] have modeled this situation by assuming a ring of scatterers about the MS, with the BS situated well outside the ring (Fig. 1). For microcells, the BSs may be placed below rooftop level. Consequently, the BSs will often be surrounded by local scatterers such that the signals arrive at the BSs with a large AOA spread. Thus, while the AOA approach is useful for macrocells, it may be impractical for microcells.

TIME-BASED SYSTEMS

The final class of radiolocation techniques are those based on estimating the TOAs of a signal transmitted by the MS and received at multiple BSs or the time differences of arrival (TDOAs) of a signal received at multiple pairs of BSs. In the TOA approach, the distance between an MS and a BS is measured by finding the one-way propagation time between an MS and a BS. Geometrically, this provides a circle, centered at the BS, on which the MS must lie. By using at least three BSs to resolve ambiguities, the MS's position is given by the intersection of the circles. In the TDOA approach, differences in the TOAs are used. Since the hyperbola is a curve of constant time *difference* of arrival for two BSs, the time differences define hyperbolae, with foci at the BSs, on which the MS must lie. Hence, the location of the MS is at the intersection of the hyperbolae. The essential ingredient for the time-based approaches are high-resolution timing measurements. However, it should be noted that LOS propagation conditions are still necessary to achieve high accuracy for the time-based methods. The problem of non-LOS (NLOS) propagation is addressed later.

Several methods have been proposed as means of forming time estimates in wireless systems, including phase estimation, pulse transmission, and spread spectrum techniques. Phase estimating systems employ phase detectors from which TOA information is obtained [15], and requires synchronization at three or more BSs. TOA or TDOA information can be obtained from wideband pulse transmission using correlation techniques [7, 15]. Finally, with spread spectrum signaling, the TOAs or TDOAs can also be determined through the use of a correlation techniques, as will be discussed later. Spread spectrum ranging has been investigated in the literature [16, 17] and is the principle behind GPS [18].

ACCURACY REQUIREMENTS

An important consideration for subscriber location is the accuracy needed for specific applications. Although it is always desirable to achieve the highest possible accuracy, some applications may require higher accuracy than others, and others may be limited by the cost of providing high accuracy. We have already mentioned that wireless E-911 services would require a location accuracy to within 125 m for 67 percent of cases. Other applications such as location-sensitive billing, fraud detection, and cellular system planning would all require high accuracy for them to be useful to service providers and to the public.

Several location applications, such as fleet management and some ITS services, can utilize lower-accuracy location techniques. For these applications, precise location of the MSs is unneccessary, and knowledge of their general vicinity will do. For example, knowing only the cell or sector a caller is in provides a simple but effective approach for providing coarse location information. The usefulness of this approach, however, depends on the cell sizes, with smaller cells providing more accurate location information. In this manner of usage, the cellular network operates as a proximity location system. Signal strength location methods are also a reasonable approach, and offer somewhat higher accuracy than simply knowing in which cell a call is made. AOA approaches could also find a role in lower-accuracy applications. Alternatively, time-based radiolocation methods could be used, but without the high timing resolution equipment. Finally, handoffs can also be monitored to provide coarse location estimates since knowledge of the handoff direction can provide information about the general vicinity of the MS. Soft handoffs in CDMA systems could be valuable in this respect.

RADIOLOCATION IN CDMA CELLULAR SYSTEMS

The IS-95A CDMA uplink is composed of access channels and reverse traffic channels [19], each of which may provide signals for radiolocation. The reverse traffic channel is only active when a call is in progress, so its use for location is limited. For E-911, it would be possible to use the reverse traffic channel since an E-911 call must be made before the emergency can be reported. However, for other applications such as fleet management and ITS services, location updates may be needed even when a MS is not transmitting on the reverse traffic channel. For these applications, the radio signals to be used for radiolocation must come from the access channel, which is only used by the MS to respond to pages and orders from the BS, make call originations, send data burst messages, or send registration messages [19]. Of these messages, only the registration message can be sent autonomously by the MS without an explicit command by the BS.[1] Use of autonomous access channel transmissions has the advantage of not consuming system resources by the BS to process and transmit messages to the MS, as is the case for an ordered registration. Hence, autonomous registration updates could provide the signals used for wireless location when the MS is idle.

IS-95A supports autonomous registration at power-up and power-down, and can be timer-based, zone-based, or distance-based. Zone-based updates occur when the MS moves from one group of BSs (i.e., a zone) to another group. Of course, this presupposes that the service provider groups BSs into zones. Distance-based registration updates occur when the MS moves from one BS to another that is at least a predefined distance away. Depending on the size of the zones and distances defined for the updates, registration updates may occur every time an MS moves into a new cell, or force the MS to travel a larger distance before an update. In either case, the mobility of the MS will determine how often the registration updates occur. To force registration updates at regular intervals, timer-based registrations can be used. The IS-95A standard makes provisions such that the time interval between successive updates is set by the BS using the parameter REG_PRD, the registration period, which can range in decimal value from 16 to 80. The MS maintains the timer which indicates timeout every $\lfloor 2^{\mathrm{REG\_PRD}/4} \rfloor \times 0.2$ s. The timer is reset after it expires, on power-up, and after implicit registration. The setting of the timer will have an effect on the load of the signaling network due to the processing of an increased number of registration updates. This issue is discussed later in the article.

TIME-BASED LOCATION ALGORITHMS

In the following, we will focus on time-based (TOA and TDOA) location algorithms, and compare their performance with AOA techniques.

COMPUTING TOA AND TDOA ESTIMATES

The time-based methods rely on accurate estimates of the TOAs or TDOAs from the signals received at several BSs. The conventional methods for computing these time estimates use correlation techniques. A straightforward method of TDOA estimation is to form the cross-correlation between signals received at a pair of BSs [21]. Suppose that the signal $d(t)$ is received at BS$_A$, corrupted by noise $n_A(t)$ such that $s_A(t) = d(t) + n_A(t)$. The same signal is received at BS$_B$ with a delay of D and also corrupted by noise $n_B(t)$, giving $s_B(t) = d(t - D) + n_B(t)$. The cross-correlation function of these signals is

$$C_{A,B}(\tau) = \frac{1}{T}\int_0^T s_A(t) s_B(t+\tau)\,dt \qquad (1)$$

The TDOA estimate is the value τ that maximizes $C_{A,B}(\tau)$. This approach requires the analog signals $s_A(t)$ and $s_B(t)$ be digitized and transmitted to a common processing site. Also, a strict time reference is required at each BS. In the IS-95A CDMA standard, all BSs are referenced to a systemwide time that uses the GPS time scale [19].

The TOA estimates can be derived from the pseudo-noise (PN) code acquisition and tracking algorithms employed in spread spectrum receivers. The time delay estimation usually takes place in two phases. Coarse acquisition determines the time delay estimate to within a chip duration and is accomplished by using a sliding correlator, matched filter, or sequential acquisition circuit. Fine acquisition maintains fine alignment between the locally generated and incoming PN sequences by using a delay-locked loop (DLL) or tau-dither loop (TDL). Many methods have been proposed for code acquisition and tracking, and the interested reader is referred to [22–24]. Previous subscriber location studies have used coarse timing acquisition to obtain TOA estimates [16, 17, 25]. The performance of TOA location using fine timing esti-

---

[1] *Note that IS-95A supports three types of registration: autonomous, ordered, and parameter-change registration [20]. There is also an implicit registration which occurs when the BS receives a call origination message or a page response message.*

mates from a DLL has also been studied in [26]. Finally, we note that TDOA estimates could be formed by differencing the TOA estimates made at several BSs.

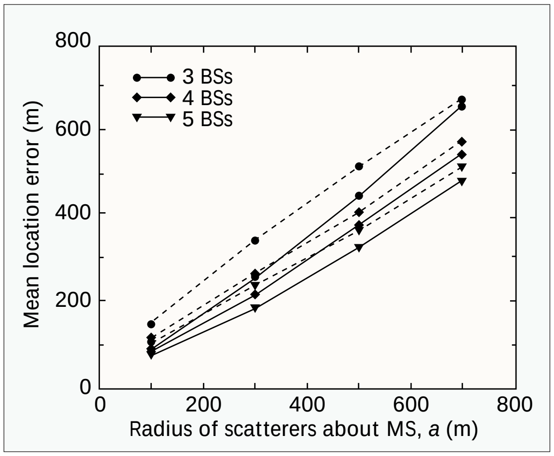

Figure 2. *Performance of the TOA and AOA location methods for a varying number of BSs and scatterer radii in macrocells. Solid lines denote results for TOA, dashed lines results for AOA.*

ALGORITHMS FOR LOCATION

The approach taken to calculate the MS position depends on whether the TOA or TDOA approach is used. A straightforward approach uses a geometric interpretation to calculate the intersection of circles for TOA or hyperbolas for TDOA. This approach becomes difficult if the hyperbolas or circles do not intersect at a point due to time measurement errors. For TDOA, however, the theory for location estimation has been thoroughly developed in the literature, where several authors have formulated techniques to solve the hyperbolic equations. Location estimates have been formed by the exact solutions to the hyperbolic TDOA equations in [27, 28], while other approaches have used a Taylor-series expansion to linearize the equations and create an iterative algorithm [29, 30]. Several other TDOA methods are based on least squares minimization of the location error [31–35].

For TOA, a popular method for computing the MS location is through the method of least squares [7, 15, 29]. Turin [15] originally formulated the approach for computing location by minimizing the sum of squares of a nonlinear cost function. The algorithm assumes that the MS, located at (x_0, y_0), transmits a waveform at time τ_0. The N BS receivers located at coordinates (x_1, y_1), (x_2, y_2), …, (x_N, y_N) receive the waveform at times $\tau_1, \tau_2, \ldots, \tau_N$. As a performance measure, we consider the function [15]

$$f_i(\mathbf{x}) = c(\tau_i - \tau) - \sqrt{(x_i - x)^2 + (y_i - y)^2} \qquad (2)$$

where c is the speed of light, and $\mathbf{x} = (x, y, \tau)^T$. This function is formed for each BS receiver, $i = 1, \ldots, N$, and all the $f_i(\mathbf{x})$ could be made zero with the proper choice of x, y, and τ. However, the measured values of the arrival times τ_i are generally in error due to imprecise measurement equipment, multipath, NLOS propagation, and other impairments.

To obtain the location estimate from the raw TOA data, the following function is formed:

$$F(\mathbf{x}) = \sum_{i=1}^{N} \alpha_i^2 f_i^2(\mathbf{x}) \qquad (3)$$

where the α_is can be chosen to reflect the reliability of the signal received at BS i. The location estimate is determined by minimizing the function $F(\mathbf{x})$.

Several methods have been proposed for forming the solution to this least squares problem. Turin suggested linearization of the $f_i(\mathbf{x})$ using a Taylor-series expansion. This leads to a set of linear equations that can be solved for the unknown x, y, and τ. An alternative approach is to use a gradient descent method [26]. These methods, such as the steepest descent method, are well known with well-developed theory [36].

PERFORMANCE OF TOA VS. AOA

The performance of the TOA algorithm in Eq. 3 has been evaluated in a simulated multipath environment. The results are shown in Fig. 2 along with the corresponding results for an AOA system (see [26] for details). These results are based on the macrocellular propagation model in Fig. 1 which assumes a scattering ring of radius a about the MS. The propagation channel is modeled by a τ-spaced wideband channel model [37] with delays and tap weights given by a COST 207 6-ray reduced typical urban power delay profile. The first arriving ray is assumed to be a reflection off the scattering ring. The TOA method outperforms the AOA method by approximately 100 m in absolute position error when three BSs are used for location. Diminishing returns occur when more BSs are used. Also from the figure, it is evident that the FCC Phase II requirement would only be met for scatterer radius $a < 200$ m.

We note that the results shown in Fig. 2 are idealized in the sense that they assume no multiple access interference. This and other sources of error for location in CDMA cellular systems are discussed in the following section.

SOURCES OF ERROR

Sources of error in wireless location systems include multipath propagation, NLOS propagation, and multiple access interference. Steps must be taken to mitigate these impairments to improve the location accuracy.

MULTIPATH

Multipath propagation is the primary reason for inaccuracies observed in the AOA and signal strength measurement systems. Multipath also affects the time-based location systems, causing errors in the timing estimates even when there is an LOS path between the MS and BS. Conventional delay estimators, which are usually based on correlation techniques, are influenced by the presence of multipath, especially when the reflected rays arrive within a chip period of the first arriving ray. When the first ray arrives with less power than later arriving rays, conventional delay estimators will detect a delay in the vicinity of these later arriving rays. Several authors have studied the effects of multipath on coarse [38, 39] and fine acquisition techniques [40]. An illustration of the latter case is shown in Fig. 3, where the "S-curve" of a DLL is shown to be affected by multipath. This example assumes a two-ray channel, where the second ray has half the power of the first ray and is delayed by half a chip duration. The multipath component is seen to bias the tracking of the DLL. Several methods have been developed to mitigate the effects of multipath on delay estimation, including a high-resolution frequency estimator [41] and a least mean square (LMS) technique [42]. Super-resolution techniques such as the Root-MUSIC and TLS-ESPRIT algorithms have been utilized to detect multipath components that conventional detectors are unable to detect [43, 44]. Delay estimators based on the Extended Kalman Filter (EKF) have also been developed for multipath corrupted signals [45]. Techniques for mitigating the effects of multipath propagation are valuable for any cellular system, and continue to be an open area of research.

NLOS PROPAGATION

With NLOS propagation, the signal arriving at the BS from the MS is reflected or diffracted and takes a longer path than the direct path. The typical error introduced by NLOS propagation has been measured in the Global System for Mobile Communications (GSM) system, which indicates that NLOS error can average 400–700 m [46]. NLOS propagation will bias the TOA or TDOA measurements even when high-resolution timing techniques are employed and there is no multipath interference. Therefore, it is important to find methods to mitigate the NLOS error. One such method is to distinguish between LOS and NLOS BSs by measuring the standard deviation of the TOA measurements [47]. The standard deviation of the range measurements is much higher for NLOS propagation than LOS propagation [46]. By using a priori information about the range error statistics, the range measurements made over a period of time and corrupted by NLOS error can be adjusted to values near their correct LOS values. A second approach is to reduce the weights of the NLOS BSs in the least squares algorithm (fifth section). The effects of reduced weighting for NLOS BSs is shown in Fig. 4, where a three-BS scenario has been simulated. The horizontal lines correspond to the case when all BSs (both LOS and NLOS) are equally weighted in the algorithm. The remaining two curves correspond to the case when the LOS BS is given unity weight, while the NLOS BS weights are varied from 0.1 to 0.9. It is seen that the performance is improved over equal weighting of the LOS and NLOS BSs. This approach, however, requires a means of determining NLOS BSs.

An alternate approach is to make algorithmic changes to the location algorithm, to exploit the fact that the range error from NLOS propagation is always positive. This is because the NLOS corrupted TOA estimates are always greater than direct TOA values. Therefore, we note that the true location must always lie inside the circles of radius $r_i = c(\tau_i - \tau)$, $i = 1,\ldots,N$, about the N BSs, since the MS cannot lie farther than its corresponding range estimate (Fig. 5). It is easily demonstrated that the least squares algorithm often fails this principle. Mathematically, the above observation implies

$$r_i \equiv c(\tau_i - \tau) \geq \sqrt{(x_i - x)^2 + (y_i - y)^2} \tag{4}$$

where (x, y) is the position of the MS. A new location algorithm can be formed by constraining the estimates to satisfy Eq. 4 at each iteration. As a result of the constrained algorithm, the error that results from NLOS propagation is reduced, especially when three BSs are used. Figure 6 shows how the error can be reduced by using a constrained algorithm. Note that this approach yields diminishing returns as the number of BSs used in the location process is increased. Again, we note that these are only a few methods for mitigating the NLOS error and that a solution to this problem is still an open area for research.

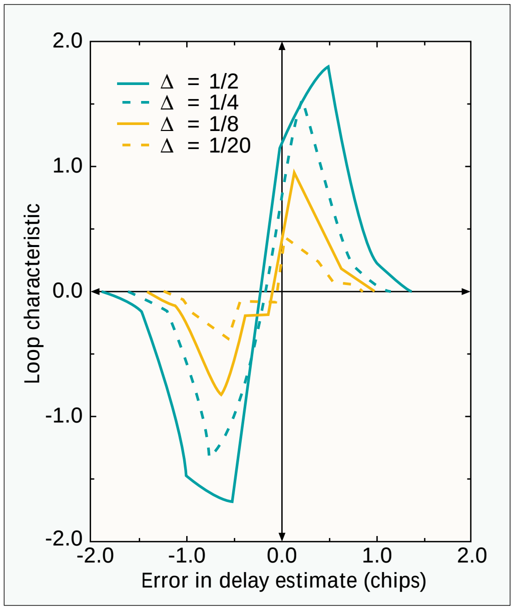

Figure 3. *The effects of multipath propagation on the S-curve of the DLL. Smaller discriminator values, Δ, reduce the effect but do not eliminate it.*

MULTIPLE ACCESS INTERFERENCE

All cellular systems suffer from cochannel interference. In cellular CDMA, users share the same frequency band with different spreading codes. One of the primary impediments to high capacity in CDMA cellular systems is the near-far effect, where the signals from the different MSs are received with unequal power at a BS making it difficult to recover the weaker users [48, 49]. It has been shown that multiple access interference greatly affects the coarse timing acquisition of spread spectrum signals [50, 51]. Likewise, the effects of multiple access interference on the conventional DLL have been shown to be quite drastic [52]. Power control schemes can be used to combat the near-far effect, which attempt to ensure that each user's signal is received with equal power at the BS [53, 54].

For subscriber location in a CDMA cellular system, the near-far effect remains a factor even when power control schemes are used. To better understand the reason refer to Fig. 7, which depicts several BSs with mobiles in each cell. Each mobile is power-controlled to its serving BS. The target MS whose location is desired (light oval) is being served by BS_0, while BS_0, BS_1, and BS_2 will be used for location. Since power control is used, all MSs served by BS_0 (deep-shaded oval) will arrive at BS_0 with approximately equal power. The same is true for the MSs being served by BS_1 (medium-shaded oval) and BS_2 (not shown). To derive the location estimate, BS_1 and BS_2 must detect the signal being transmitted by the target MS (light oval). However, the signal from the target MS at BS_1 and BS_2 may experience severe multiple access interference from MSs being served by BS_1 and BS_2, since the target MS is not power-controlled to those BSs. The interference will affect the ability of a conventional receiver to estimate the TOA or TDOA information. However, it may be possible, for instance in E-911 situations, for the MS to power up to maximum level and therefore mitigate the near-far effect. A further possibility is to

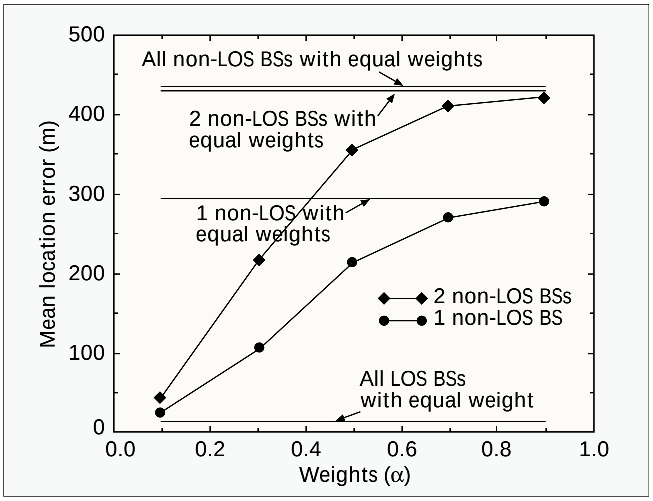

Figure 4. *Effect of NLOS weights in the TOA algorithm on the location estimates. Only three BSs are considered.*

take advantage of soft handoffs. A soft handoff occurs when an MS is in the region between two or more cells, and communicates with the other BSs to achieve a macrodiversity gain [55]. The soft handoff allows a smoother handoff with less chance for a dropped call. However, for soft handoffs to be useful for a time based location system, at least three BSs must be involved in the soft handoff, an unlikely situation [20].

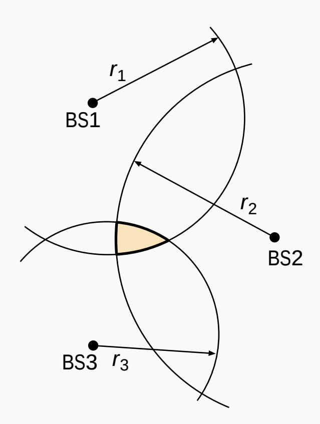

Figure 5. *The location of the MS is constrained to the intersection area (shaded region) of circles of radii* $c(\tau_i - \tau)$ *centered at* BS_i.

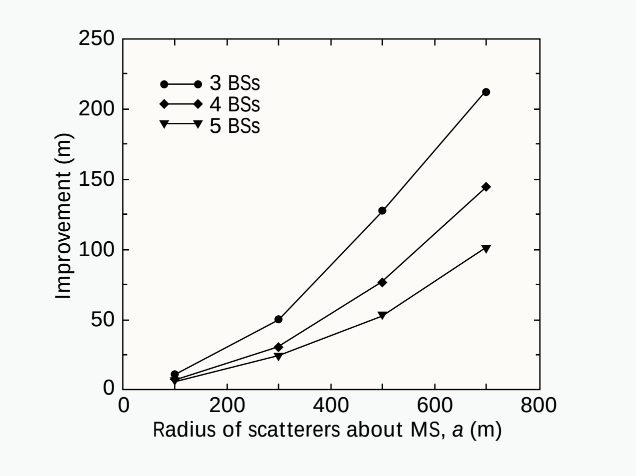

Figure 6. *Improvement that results when the constrained algorithm is used over the original algorithm for a varying number of BSs and radii of the scattering model.*

As a consequence of the research into near-far resistant CDMA multiuser detection, several authors have investigated near-far resistant delay estimators. With the interference problem we have just discussed, these provide a means of forming accurate TOA estimates for location in the presence of multiple access interference. Many of the near-far resistant delay estimators are based on subspace techniques such as MUSIC [56–58]. Other estimators have been produced in conjunction with multi-user detectors [59, 60] and interference cancellation techniques [61, 62].

SYSTEM LOADING ASPECTS

The fourth section suggested the use of timer-based registration for wireless subscriber location. However, registration at frequent intervals will increase the load in the signaling network, which will ultimately limit the frequency of registration (location) updates. To study loading effects, we examine Signaling System No. 7 (SS7), a transport mechanism for call control and database transactions [63]. The rapidly expanding wireless networks rely on intelligent network (IN) concepts to track users and deliver enhanced services. The switches and databases that perform these functions use SS7 to connect mobile switching centers (MSCs), visitor location registers (VLRs), and home location registers (HLRs). In the following, we provide a simple analysis of the effect of increased timer-based registration updates on the signaling load of the SS7 network.

The MSC sets up calls to mobile users via the BSs and maintains connections to other MSCs and the public switched telephone network. The HLR stores the parameters and features for a group of subscribers within a network. It contains pointers to VLRs to assist in routing incoming calls, and updates information on the location area of the MS. The VLR is a local database in charge of one or more location areas. It obtains the parameters of all subscribers currently in these areas from the HLR, and updates the HLR regarding the status of special services if necessary. Location updates record the locations of subscribers as they move through the network and are one of the key activities which generate SS7 traffic. Conventionally, whenever a user moves into a new location area (group of cells), a location update is required. However, when timer-based registration updates are used for wireless location, the registration updates will occur at regular intervals in addition to those required when moving into new location areas.

Calculation of the signaling load requires the number of location updates per unit time. The data from Table 1 show-

	Same VLR	New VLR	
		Old VLR	New VLR
	b_1	b_2	b_3
To/from MSC			
VLR in MSC	55	308	395
VLR out MSC	406	—	406
Internal SS7			
VLR in MSC	55		490
VLR out MSC	461		896
To/from VLR	461	308	801
To/from HLR	55	95	182

Table 1. *SS7 bytes generated per transaction for location updates (modified from [64]).*

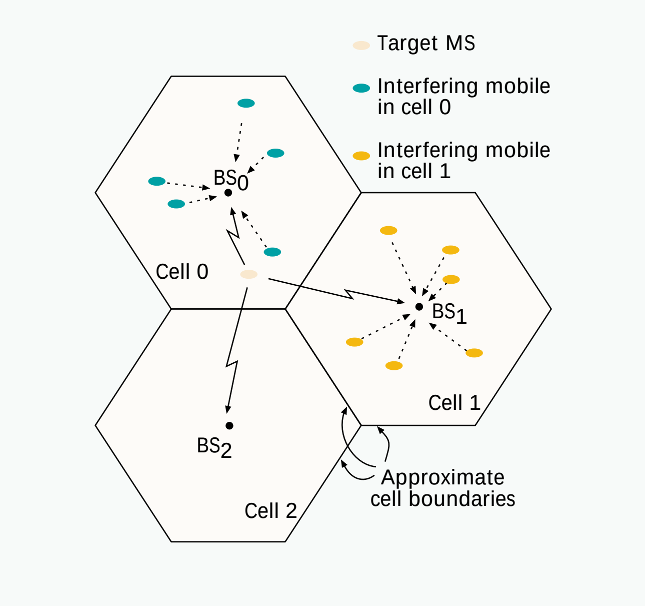

Figure 7. *An illustration of the near-far effect on wireless location in CDMA, in which three BSs are required for a 2D position estimate. The target MS may still be masked by users in other cells since it is not power-controlled to those BSs.*

ing the traffic aggregated by each network element can then be used to calculate the load in bytes. To determine the number of location updates, we need to consider updates triggered by both the crossings into a new location area and from timer-based registrations. The procedure parallels that done in [64] with the addition of the timer-based updates. The number of location updates (intra- plus inter-VLR) in an area is

$$U = N_L \cdot P_T \cdot P_{ON} \cdot (C + U_{TB}) \tag{5}$$

where N_L is the number of location areas in the switch coverage area, and P_T and P_{ON} are the probabilities that a person has a terminal and that the terminal is turned on, respectively. The term C is the number of persons (with or without MSs and with or without a call in progress) that leave the *location area* per hour (crossing updates). The term U_{TB} is the number of timer-based location updates per hour. Updates are considered even when a call is in progress, since the updates are being used both for location and to establish MS terminated calls.

A VLR controls one or more location areas, and slightly different procedures are used depending on whether the MS moves into a new VLR area or stays within the existing VLR area. Consequently, the quantities for updates in the same VLR, U_{same}, and for updates to a new VLR, U_{new}, need to be determined. These quantities are

$$U_{new} = C_L \cdot P_{ON} \cdot P_T \tag{6}$$

for updates into a new VLR, and

$$U_{same} = U - U_{new} \tag{7}$$

for updates to the same VLR. The term C_L is the number of MSs that leave the location area and move into a new VLR per hour. It should be noted that we can view timer-based updates as occurring between the crossing updates. Thus, only the crossing updates have significance in determining the number of location updates to a new VLR. The timer-based updates only have significance for location updates within the same VLR.

The number of bytes required, considering only location update traffic, is

$$\text{SS7 bytes} = b_1 \cdot U_{same} + (b_2 + b_3) \cdot U_{new}. \tag{8}$$

The quantities b_1, b_2, and b_3 are the bytes required for location updates as listed in Table 1. From the equations given, we need to estimate certain statistics about the network. Assumptions on mobility and the network configuration, in particular the cell size and location area size, are important considerations that need to be made as realistically as possible. Once these are specified the network loading due to the additional timer-based registration updates can be determined.

CONCLUSION

This article has provided an overview of wireless location methodologies in CDMA cellular networks. Radiolocation fits quite naturally with wireless networks since each is based on transmission/reception of radio signals. Also, radiolocation would allow location with existing handsets without modification. However, the implementation of a radiolocation system might require considerable modification on the network side. Depending on the accuracy required for a given application, several technological possibilities exist. For high accuracy, location by means of measuring TOAs or TDOAs appear to be the most appropriate, whereas lower accuracy location can be obtained by other means such as signal strength measurements or by simply knowing in which cell and/or sector an MS resides.

Within the confines of the IS-95A standard, the registration update message is a good starting point for providing the signals for radiolocation, especially when the MS is idle. It may be advantageous in the future to develop new location-specific signaling as the CDMA standard evolves. Moreover, techniques still need to be developed to provide some immunity to multiple access interference, NLOS propagation, and multipath propagation. Thus, it is evident that many research challenges still exist in providing high-accuracy radiolocation in CDMA cellular systems.

REFERENCES

[1] FCC Docket No. 94-102, “Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems,” RM-8143, July 26 1996.

[2] R. Jurgen, “The Electronic Motorist,” *IEEE Spectrum*, vol. 32, Mar. 1995, pp. 37–48.

[3] S. Riter and J. McCoy, “Vehicle Location — An Overview,” *IEEE Trans. Vehic. Tech.*, vol. VT-26, Feb. 1977, pp. 7–11.

[4] State of New Jersey, “Report on the New Jersey Wireless Enhanced 911 System Trial: The First 100 days,” June 16, 1997.

[5] L. Stilp, “Carrier and End-User Applications for Wireless Location Systems,” *Proc. SPIE*, 1996, pp. 119–26.

[6] I. Paton *et al.*, “Terminal Self-Location in Mobile Radio Systems,” *Proc. 6th Int’l. Conf. Mobile Radio and Pers. Commun.*, 1991, pp. 203–7.

[7] H. Hashemi, “Pulse Ranging Radiolocation Technique and Its Application to Channel Assignment in Digital Cellular Radio,” *Proc. IEEE Vehic. Tech. Conf.*, 1991, pp. 675–80.

[8] A. Giordano, M. Chan, and H. Habal, “A Novel Location-Based Service and Architecture,” *Proc. IEEE PIMRCe*, 1995, pp. 853–57.

[9] W. Figel, N. Shepherd, and W. Trammell, “Vehicle Location by a Signal Attenuation Method,” *IEEE Trans. Vehic. Tech.*, vol. VT-18, Nov. 1969, pp. 105–10.

[10] M. Hata and T. Nagatsu, “Mobile Location Using Signal Strength Measurements in a Cellular System,” *IEEE Trans. Vehic. Tech.*, vol. VT-29, May 1980, pp. 245–51.

[11] W. Smith, Jr., “Passive Location of Mobile Cellular Telephone Terminals,” *Proc. IEEE Int’l. Carnahan Conf. Security Tech.*, 1991, pp. 221–25.

[12] W. C. Jakes, *Microwave Mobile Commun.*, IEEE Press, 1994.

[13] J. Parsons, *The Mobile Radio Propagation Channel*, Halsted Press, 1992.

[14] M. Gans, “A Power-Spectral Theory of Propagation in the Mobile-Radio Environment,” *IEEE Trans. Vehic. Tech.*, vol. VT-21, Feb. 1972, pp. 27–38.

[15] G. Turin, W. Jewell, and T. Johnston, “Simulation of Urban Vehicle-Monitoring Systems,” *IEEE Trans. Vehic. Tech.*, vol. VT-21, Feb. 1972, pp. 9–16.

[16] P. Goud, A. Sesay, and M. Fattouche, “A Spread Spectrum Radiolocation Technique and Its Application to Cellular Radio,” *Proc. IEEE Pacific Rim Conf. Commun., Comp. and Signal Processing*, 1991, pp. 661–64.

[17] J. Caffery, Jr. and G. Stüber, “Vehicle Location and Tracking for IVHS in CDMA Microcells,” *Proc. IEEE PIMRC*, 1994, pp. 1227–31.

[18] P. Enge, “The Global Positioning System: Signals, Measurements, and Performance,” *Int’l. J. Wireless Info. Networks*, vol. 1, no. 2, 1994, pp. 83–105.

[19] TIA/EIA IS-95, “Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Digital Cellular System,” PN-3422, 1994.

[20] V. Garg, K. Smolik, and J. Wilkes, *Applications of CDMA in Wireless/Personal Communications*, Prentice Hall, 1997.

[21] C. Knapp and G. Carter, “The Generalized Correlation Method for Estimation of Time Delay,” *IEEE Trans. Acoustics, Speech, and Signal Processing*, vol. ASSP-24, Aug. 1976, pp. 320–27.

[22] Simon *et al.*, *Spread Spectrum Communications,* vol. III, Computer Science Press, 1985.

[23] J. Holmes, *Coherent Spread Spectrum Systems*, Wiley, 1982.

[24] R. Ziemer and R. Peterson, *Digital Communications and Spread Spectrum Systems*, Macmillan, 1985.

[25] E. Hepsaydir and W. Yates, “Performance Analysis of Mobile Positioning Using Existing CDMA Network,” *Proc. IEEE ISSSTA*, 1994, pp. 190–92.

[26] J. Caffery, Jr., and G. Stüber, “Subscriber Location in CDMA Cellular Networks,” to appear, *IEEE Trans. Vehic. Tech*.

[27] B. Fang, “Simple Solutions for Hyperbolic and Related Position Fixes,” *IEEE Trans. Aerospace and Elect. Sys.*, Sept. 1990, pp. 734–53.

[28] K. Ho and Y. Chan, “Solution and Performance Analysis of Geolocation by TDOA,” *IEEE Trans. Aerospace and Elect. Sys.*, vol. 29, Oct. 1993, pp. 1311–22.

[29] W. Foy, “Position-Location Solutions by Taylor-Series Estimation,” *IEEE Trans. Aerospace and Elect. Sys.*, vol. AES-12, Mar. 1976, pp. 187–93.

[30] D. Torrieri, "Statistical Theory of Passive Location Systems," *IEEE Trans. Aerospace and Elect. Sys.*, vol. AES-20, Mar. 1984, pp. 183–97.

[31] J. Smith and J. Abel, "The Spherical Interpolation Method of Source Localization," *IEEE J. Oceanic Eng.*, vol. OE-12, Jan. 1987, pp. 246–52.

[32] J. Smith and J. Abel, "Closed-Form Least Squares Source Location Estimation from Range-Difference Measurements," *IEEE Trans. Acoustics, Speech, and Signal Processing*, Dec. 1987, pp. 1661–69.

[33] J. Abel, "A Divide and Conquer Approach to Least Squares Estimation," *IEEE Trans. Aerospace and Elect. Sys.*, Mar. 1990, pp. 423–27.

[34] Y. Chan and K. Ho, "A Simple and Efficient Estimator for Hyperbolic Location," *IEEE Trans. Signal Processing*, Aug. 1994, pp. 1905–15.

[35] B. Friedlander, "A Passive Location Algorithm and Its Accuracy Analysis," *IEEE J. Oceanic Eng.*, Jan. 1987, pp. 234–44.

[36] G. Beveridge and R. Schechter, *Optimization: Theory and Practice*, MacGraw-Hill, 1970.

[37] G. Stüber, *Principles of Mobile Communication*, Kluwer, 1996.

[38] E. Sourour and S. Gupta, "Direct-Sequence Spread-Spectrum Parallel Acquisition in a Fading Mobile Channel," *IEEE Trans. Commun.*, July 1990, pp. 992–99.

[39] B. Ibrahim and A. Aghvami, "Direct Sequence Spread Spectrum Matched Filter Acquisition in Frequency-Selective Rayleigh Fading Channels," *IEEE JSAC*, vol. 12, June 1994, pp. 885–90.

[40] W. Sheen and G. Stüber, "Effects of Multipath Fading on Delay-Locked Loops for Spread Spectrum Systems," *IEEE Trans. Commun.*, vol. 42, Feb./Mar./Apr. 1994, pp. 1947–1956.

[41] K. Krizman, T. Biedka, and T. Rappaport, "Wireless Position Location: Fundamentals, Implementation Strategies, and Sources of Error," *Proc. IEEE VTC*, 1997, pp. 919–23.

[42] H. So and P. Cheng, "Target Localisation in Presence of Multipaths," *Elect. Lett.*, vol. 29, Feb. 4 1993, pp. 293–94.

[43] L. Dumont, M. Fattouche, and G. Morrison, "Super-Resolution of Multipath Channels in a Spread Spectrum Location System," *Elect. Lett.*, Sept. 15 1994, pp. 1583–84.

[44] H. Saarnisaari, "TLS-ESPRIT in a Time Delay Estimation," *Proc. IEEE VTC*, 1997, pp. 1619–23.

[45] R. Iltis, "Joint Estimation of PN Code Delay and Multipath Using the Extended Kalman Filter," *IEEE Trans. Commun.*, vol. 38, Oct. 1990, pp. 1677–85.

[46] M. Silventoinen and T. Rantalainen, "Mobile Station Emergency Locating in GSM," *Proc. IEEE Int'l. Conf. Pers. Wireless Commun.*, 1996, pp. 232–38.

[47] M. Wylie and J. Holtzman, "The Non-Line of Sight Problem in Mobile Location Estimation," *Proc. IEEE ICUPC*, 1996, pp. 827–31.

[48] R. Lupas and S. Verdú, "Near-Far Resistance of Multiuser Detectors in Asynchronous Channels," *IEEE Trans. Commun.*, vol. 39, Apr. 1990, pp. 496–508.

[49] G. D. Vitantonio and F. D. Ferrari, "On the Application of Near-Far Resistant Techniques to DS-CDMA Systems," *Proc. IEEE PPIMRC*, 1994, pp. 70–74.

[50] U. Madhow and M. Pursley, "Acquisition in Direct-Sequence Spread-Spectrum Communication Networks: An Asymptotic Analysis," *IEEE Trans. Info. Theory*, vol. 39, May 1993, pp. 903–12.

[51] G. Corazza and V. Esposti, "Code Acquisition in DS-SSMA Systems in the Presence of Multiple Access Interference and Data Modulation," *Euro. Trans. Telecommun. and Related Tech*., Feb. 1994, pp. 27–37.

[52] J. Caffery, Jr. and G. Stüber, "Effects of Multiple-Access Interference on the Non-Coherent Delay-Lock Loop," submitted to *IEEE Trans. Commun.*, 1997.

[53] J. Holtzman, *CDMA Power Control for Wireless Networks*, Kluwer, 1992, pp. 299–311.

[54] W. Lee, "Power Control in CDMA (Cellular Radio)," *IEEE VTC*, 1991, pp. 77–80.

[55] A. Viterbi, *CDMA: Principles of Spread Spectrum Communication*, Addison-Wesley, 1995.

[56] E. Ström *et al.*, "Propagation Delay Estimation in Asynchronous Direct-Sequence Code-Division Multiple Access Systems," *IEEE Trans. Commun.*, Jan. 1996, pp. 84–93.

[57] S. Bensley and B. Aazhang, "Subspace-Based Channel Estimation for Code Division Multiple Access Communication Systems," *IEEE Trans. Commun.*, Aug. 1996, pp. 1009–20.

[58] J. Joutsensalo, "Algorithms for Delay Estimation and Tracking in CDMA," *Proc. IEEE VTC*, 1997, pp. 366–70.

[59] A. Radovic, "An Iterative Near-Far Resistant Algorithm for Joint Parameter Estimation in Asynchronous CDMA Systems," *Proc. Proc. 5th Int'l. Symp. PIMRC*, 1994, pp. 199–203.

[60] R. Iltis and L. Mailaender, "An Adaptive Multiuser Detector with Joint Amplitude and Delay Estimation," *IEEE JSAC*, vol. 12, June 1994, pp. 774–85.

[61] M. Latva-aho and J. Lilleberg, "Delay Trackers for Multiuser CDMA Receivers," *Proc. IEEE ICUPC*, 1996, pp. 326–30.

[62] W. Zhaocheng *et al.*, "Synchronization Consideration in Multiuser CDMA Environment," *Proc. Int'l. Conf. Commun. Tech.*, 1996, pp. 103–6.

[63] B. Jabbari, "Intelligent Network Concepts in Mobile Communications," *IEEE Commun. Mag.*, vol. 30, Feb. 1992, pp. 64–69.

[64] K. Meier-Hellstern, E. Alonso, and D. O'Neil, "The Use of SS7 and GSM to Support High Density Personal Communications," *Proc. IEEE ICC*, 1992, pp. 1698–1702.

BIOGRAPHIES

JAMES J. CAFFERY, JR. (james.caffery@ece.gatech.edu) received a B.S.E.E (summa cum laude) from Bradley University, Peoria, Illinois, in 1992 and an M.S. degree from the Georgia Institute of Technology in 1993. He is currently a Ph.D. student at the Georgia Institute of Technology, Atlanta, where his research interests include code-division multiple access systems, parameter estimation, and subscriber location in mobile cellular radio networks.

GORDON L. STÜBER (stuber@ece.gatech.edu) received B.A.Sc. and Ph.D. degrees in electrical engineering from the University of Waterloo, Ontario, Canada, in 1982 and 1986, respectively. In 1986, he joined the School of Electrical and Computer Engineering, Georgia Institute of Technology, where he is currently a professor. His research interests are in wireless communications and communication signal processing. He has authored the textbook *Principles of Mobile Communication* (Kluwer, 1996). He served as an editor for spread spectrum with *IEEE Transactions on Communications* from January 1993 to December 1997. He is currently serving as technical program chair for the 1998 IEEE International Conference on Communications to be held in Atlanta, Georgia, June 7–11, 1998.