Chapter 21

GSM CELL SITE FORENSICS

Christopher Swenson, Tyler Moore and Sujeet Shenoi

Abstract Cell site forensics is a new and growing area of digital forensics, enabling investigators to verify a mobile phone subscriber's location at specific times. This paper focuses on cell site forensics in GSM networks. In particular, it discusses current methods utilizing call detail records generated from telephone switches that provide information about cellular calls and text messages, and the cellular towers on which calls/messages were placed and received.

Keywords: GSM networks, cell site forensics, subscriber location estimation

1. Introduction

Cell phones are small, mobile, integrated communications and computing devices. They have become indispensable to the daily activities of much of the world's population. As such, cell phones are data repositories, holding evidence of legal—and illegal—activities. Specifically, digital evidence is stored in cell phone SIM cards, internal memory chips and external memory devices. Numerous techniques and tools have been developed for extracting and analyzing evidence from cell phones and peripherals.

Less well-known, but equally important for evidentiary purposes, is information about mobile subscribers and phone calls that is stored within the mobile communications network infrastructure. Mobile networks maintain information about who called whom, from where, when, and for how long [3]. This information can pinpoint a mobile subscriber's location at a specific time and the subscriber's movement over time. It can demonstrate the mobile subscriber's presence at the scene of a crime. Moreover, historical location-time data pertaining to mobile subscribers may provide details about the "dynamics" of a crime, from planning to execution.

Cell site forensics involves the application of scientific techniques to analyze mobile communications network data. Current methods examine call detail records (CDRs) that are created by telephone switches for billing purposes. CDRs are generated, for example, whenever a subscriber makes or receives a call, sends or receives a text message, or moves to a new area of cell phone coverage. They provide detailed information about cellular calls and text messages (e.g., caller/sender, called party/receiver and time of call/message). CDRs identify the cellular towers on which calls were placed and received. These cell ids provide location information that can be refined using other data maintained by service providers, e.g., directions (azimuths) of mobile subscribers from cellular tower antennae and the power levels of subscriber to cellular tower communications.

This paper focuses on cell site forensics for GSM (Global System for Mobile Communications) networks [2, 5]. GSM is the largest mobile communications system in the world, and the fastest growing network in the United States [6]. The following sections discuss the basic concept of cell site forensics and highlight strategies for obtaining accurate time-location information from GSM networks.

2. GSM Cellular Networks

Cellular networks differ from traditional wireless telecommunications networks in three respects. First, small base stations or "cells" are used instead of large antennae. Each cell has a range of a few miles or less, which reduces the need for large, power-consuming equipment. Also, this provides greater overall bandwidth as a given frequency can be allocated to multiple cells. Second, the cell-based structure requires a mechanism for handovers—allowing users to seamlessly move between different coverage areas without dropping calls. Finally, network bandwidth released by subscribers can be reused by other subscribers.

This paper focuses on GSM networks [2, 5]. GSM was originally deployed in the early 1990s as an international standard for digital cellular networks. It is now the largest mobile communications system in the world [6]. GSM's popularity partly stems from the fact that subscribers can use the same phone in multiple countries.

Figure 1 presents a schematic diagram of a GSM network, including its connections to the public switched telephone network (PSTN) and the Internet. The portions of the network concerned with mobile telecommunications are often referred to as the public land-mobile network (PLMN). The main components of a GSM network are described below.

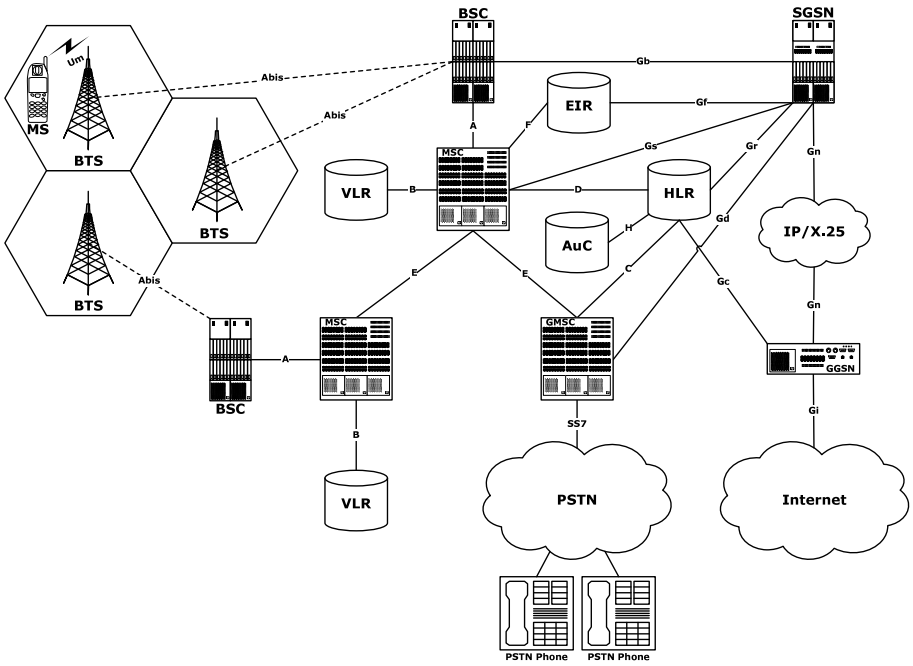

Figure 1. Schematic diagram of a GSM network.

Mobile Subscriber (MS): A mobile subscriber includes the functionality of the handset and the SIM card, which are identified by the International Mobile Equipment Identifier (IMEI) and International Mobile Subscriber Identifier (IMSI), respectively. An MS communicates with the network indirectly through cell towers known as Base Transceiver Stations (BTSs).

Base Transceiver Station (BTS): A BTS communicates with mobile subscribers using the Um interface and with the Base Station Controller (BSC) using the Abis interface. A BTS has limited decision-making duties and has practically no record storage capabilities.

Base Station Controller (BSC): A BSC is responsible for coordinating the communications of BTSs and MSCs, using the Abis and A interfaces, respectively. A BSC maintains information about the current locations of all mobile subscribers in its zone of control. However, very little of this information is stored for extended periods of time.

Mobile Switching Center (MSC): The MSC is the main decision-making entity in a GSM network. It relays communications within its child BSCs and with external MSCs using the A and E interfaces, respectively. Links between MSCs facilitate communications between mobile subscribers on different network segments and between subscribers with

different service providers. MSCs typically generate call detail records (CDRs) and collect billing information.

Gateway MSC (GMSC): The GMSC is a portal from a mobile network to other networks, especially the public switched telephone network (PSTN). A GMSC connects GSM networks to the PSTN using standard SS7 protocols, e.g., ISUP, TCAP, SCCP [1, 10], allowing calls placed on one network to be routed to another. A GMSC communicates with other MSCs using the E interface and it locates mobile subscribers by querying the Home Location Register (HLR) using the C interface.

Home Location Register (HLR): The HLR is a central repository for the current MSC locations of all subscribers. A PLMN typically has a small number of HLRs, each of which can serve several hundred thousand subscribers. An MSC uses the D interface to query an HLR for the purposes of authenticating and locating users. A GMSC communicates with an HLR using the C interface to locate users, and the Gr and Gc interfaces for GPRS location and authentication.

Visitor Location Register (VLR): The VLR is similar to an HLR, except that it contains information about mobile subscribers on a particular MSC. An MSC uses the B interface to query a VLR to determine if a subscriber is located on the MSC. The load on the master HLR is decreased because the MSC interrogates the VLR before querying the HLR.

Authentication Center (AuC): The AuC is responsible for verifying a mobile subscriber's identity and for generating keying information using the A3 and A8 cryptographic procedures. When implementing the subscriber authentication procedure, the HLR caches the A3/A8 outputs from the H interface and forwards them to the MSC.

Equipment Identity Register (EIR): The EIR maintains and enforces a blacklist of mobile handsets, mainly to curb fraud and theft. The EIR communicates with an MSC using the F interface and with a Serving GPRS Support Node (SGSN) using the Gf interface.

Serving GPRS Support Node (SGSN): The SGSN connects mobile subscribers to advanced data services provided by General Packet Radio Service (GPRS) [8]. The SGSN coordinates data sessions with mobile subscribers and relevant GGSNs using the Gn interface and the GPRS IP/X.25 core.

Gateway GPRS Support Node (GGSN): A GGSN serves as an access point for SGSNs to access a desired service, e.g., WWW and POP3. A GGSN usually communicates with SGSNs using the Gn interface and with external networks using the Gi interface.

3. Call Control Procedures

This section describes call control procedures for phone calls involving PSTN and GSM subscribers. Details of call setup and teardown procedures are provided for: (i) PSTN to PSTN calls, (ii) PSTN to GSM calls, (iii) GSM to PSTN calls, and (iv) GSM to GSM calls. These procedures provide insight on the information requirements and strategies involved in cell site forensics. Note that PSTN to PSTN calls *per se* are not relevant to GSM network forensics as the calls remain within the PSTN. However, they are discussed because PSTN call setup and teardown procedures are involved in PSTN to GSM and GSM to PSTN calls.

Call setup and teardown in GSM networks build on call control procedures used in ISUP, the basic call handling protocol for PSTN (SS7) calls. However, GSM call control requires extra steps to allocate radio frequencies in addition to voice trunks. Also, it incorporates cellular authentication and encryption mechanisms. Readers are referred to [1, 10] and [4] for details about ISUP and GSM call control procedures, respectively, and [9] for details about forensic techniques involving the ISUP protocol in SS7 networks.

3.1 PSTN to PSTN Calls

PSTN to PSTN call setup follows a four-step procedure involving the exchange of ISUP protocol messages.

1. The PSTN caller dials the receiver's phone number, which is interpreted by the caller's central office switch.

2. Initial address messages (IAMs) are sent from the caller's central office switch to the receiver's central office switch. The IAMs attempt to reserve a chain of voice trunks between the caller's and receiver's switches.

3. Address complete messages (ACMs) are sent back along the same path from the receiver's switch to the caller's switch, signifying that voice trunks have been successfully allocated and the receiver's phone is ringing. If the receiver is not available, the switch returns a release (REL) message with the appropriate cause code set (e.g., user busy or no answer).

4. An answer message (ANM) is sent from the receiver's switch to the caller's switch, indicating that the receiver has picked up the phone. Billing is then initiated. If the call is not completed, the call attempt will most likely not be registered in billing records,

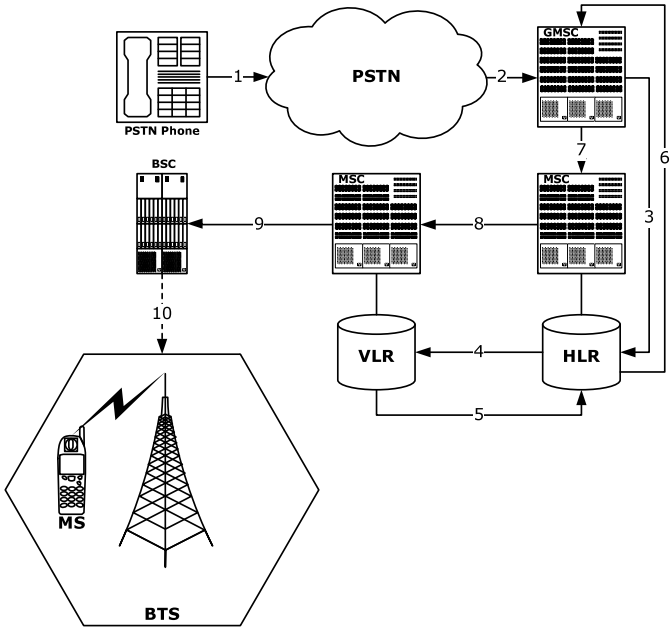

Figure 2. Call setup procedure for a PSTN to GSM call.

although it may be registered in call detail records (CDRs) generated at the switch.

PSTN calls are terminated by a sequence of release (REL) and release complete (RLC) messages. If a call is terminated within a few seconds of its initiation, the call is usually not charged and no billing record may be generated.

3.2 PSTN to GSM Calls

Call setup in GSM networks involves the exchange of numerous messages between various network components. To simplify the presentation, we list only the basic steps involved in setting up calls from PSTN to GSM networks (Figure 2).

1. The PSTN caller dials the mobile subscriber's telephone number, which is interpreted by the PSTN switch.

2. The PSTN switch generates the relevant ISUP IAM and routes it to the GMSC belonging to the service provider of the mobile subscriber.

3. The GMSC queries the HLR to identify the mobile subscriber roaming number (MSRN) for the receiver's phone number. The MSRN is the phone number assigned to the mobile phone on the network where it is currently located; it helps the switch route the call correctly. For example, suppose the receiver's cell phone number is (918) 555-1234, which has the 918 area code corresponding to Tulsa, Oklahoma. If the receiver is currently located in Oklahoma City, Oklahoma, he would be assigned an MSRN with the 405 Oklahoma City area code, e.g., (405) 555-6789. Thus, the switch would know to route the call to the receiver in Oklahoma City instead of Tulsa.

4. The HLR queries the last known VLR where the receiver was located to check if the user is still at that location and is connected to the network.

5. The VLR replies to the HLR's query with the receiver's status.

6. The HLR replies to the GMSC's query, identifying the MSC for routing the call.

7,8. The GMSC forwards the IAM through the GSM network core.

9. The MSC initiates call control procedures for setting up the voice call to the mobile subscriber (receiver). It notifies the BSC that the subscriber is receiving the call.

10. The BSC notifies the mobile subscriber (MS) via the BTS of the incoming call, and begins to check the receiver's credentials and allocate resources, e.g., voice circuits and radio frequencies.

Billing is initiated as soon as the mobile subscriber (receiver) answers the call, and the call is noted in the MSC. A call terminated within a few seconds of initiation is usually not billed and no CDR may be generated.

Call teardown can be initiated in many ways, e.g., when a subscriber goes out of range, hangs up, or runs out of minutes. When the MSC notes that one of the parties ends the call, it begins to teardown the call for the mobile subscriber by releasing its resources, while notifying the remote party that the call is complete by performing the ISUP teardown procedure (a REL message followed by a RLC message are sent to both parties). Procedures for tearing down GSM to PSTN calls and GSM to GSM calls are practically identical.

3.3 GSM to PSTN Calls

The call setup procedure for a GSM to PSTN call is relatively similar to the setup procedure for a PSTN to GSM call. Some clarifications are provided below.

1. After determining that the call is not local via VLR and HLR queries, an IAM is sent to the GMSC to route the call to the PSTN.

2. While waiting for the ACM from the GMSC, the MSC initiates the call setup procedure for the GSM subscriber (caller), allocating the required radio frequencies and performing authentication.

3. Upon receiving the ANM from the GSMC, the call is routed from the GMSC to the subscriber (caller).

3.4 GSM to GSM Calls

Call setup procedures for GSM to GSM calls can vary significantly according to the circumstances of the two subscribers. If the two mobile phones have different service providers or are located in different countries, the call setup procedure is similar to that for the PSTN-initiated and GSM-initiated calls described above.

If the GSM subscribers are on the same network, the MSC first queries the VLR to determine if the call is local (in which case it does not have to reserve voice trunks outside the MSC). If the call is local, radio allocations are made to both subscribers and voice communications are routed through the MSC. If the subscriber (receiver) is not local, the MSC queries the HLR to determine where to route the call. An IAM is then sent to the appropriate MSC, and the call proceeds in the same way as PSTN-initiated and GSM-initiated calls.

4. Call Records

This section describes the data pertaining to cell phone calls that are generated within the network and often stored by service providers. The data are indispensable to cell site forensics, especially in obtaining historical time-location information about mobile subscribers.

As described in the previous section, signaling messages are generated whenever a call is initiated in a GSM network. The switches at both ends of the call may record details about calls if certain conditions are satisfied. For example, a switch may be configured to generate records for calls only if they complete, for calls that are more than a few seconds

long, or for all calls that are attempted. In general, record generation and record storage times vary from provider to provider.

4.1 Call Detail Records

Call detail records (CDRs) are generated and stored by telephone network switches. CDRs are consolidated at fixed intervals to create billing records, which only contain information related to customer billing. As such, billing records tend to be fewer in number than CDRs and contain less information about network events.

GSM 12.05 [3] originally specified seventeen types of CDRs for logging events. Almost all the CDRs indicate mobile subscriber location and time. However, many of the CDRs are optional and others may only be partially recorded.

The most commonly generated CDRs are: (i) Mobile originated/terminated call records, (ii) Mobile originated/terminated SMS records, (iii) HLR location update records, and (iv) VLR location update records. The following subsections provide details about these records, which are particularly useful for cell site forensics. The records are only partially specified for reasons of space. Important fields are displayed along with their descriptions and whether they are mandatory (M), conditional (C) or optional (O).

Mobile Originated/Terminated Call Records: Mobile originated call (MOC) records are typically generated by the originating MSC for all outgoing call attempts. Mobile terminated call (MTC) records are generated upon call termination. MOC and MTC records may be generated even when call attempts fail. Table 1 presents the MOC record fields; MTC records have almost identical fields. Note that for a mobile originated call, only the origination cell id is recorded. On the other hand, for a mobile terminated call, only the destination cell id is recorded. In general, an MSC has limited information about a call on the other end, and it sees little difference between PSTN originated and mobile originated calls.

Mobile Originated/Terminated SMS Records: SMS mobile originated (SMS-MO) records are typically produced by the originating MSC for all SMS messages. Similarly, SMS mobile terminated (SMS-MT) records are produced by the terminating MSC for all SMS messages sent to subscribers in its jurisdiction. Relevant fields in SMS-MO records are shown in Table 2. The SMS-MT record structure is nearly identical, except that it has information about the receiver instead of the sender.

Table 1. Relevant mobile originated call record fields.

Field	Type	Description
Record Type	M	Mobile originated
Served IMSI	M	IMSI of calling party
Served IMEI	C	IMEI of calling party (if available)
Served MSISDN	O	Primary MSISDN of calling party
Called Number	M	Number dialed by caller
Translated Number	O	Called number after MSC translation
Connected Number	O	Actual connected number (if different)
Location	M	Cell id of originating call
Change of Location	O	Timestamped changes in location area and cell id
Event Timestamps	C	Incoming traffic channel assignment
	C	Answer
	O	Release
Call Duration	M	Duration of call or holding time

Table 2. Relevant mobile originated SMS record fields.

Field	Type	Description
Record Type	M	Mobile originated
Served IMSI	M	IMSI of sending party
Served IMEI	O	IMEI of sending party (if available)
Served MSISDN	O	Primary MSISDN of sending party
Recording Entity	M	Visited MSC identifier
Location	O	Location area code and cell id of origination
Event Timestamp	M	Time SMS received by MSC
SMS Result	C	Result of attempted delivery (if unsuccessful)

HLR Location Update Records: HLRs generate records about location updates and registrations as these are often billable events, e.g., when subscribers use their cell phones while traveling outside their home area. Table 3 presents the relevant fields of an HLR location update record.

VLR Location Update Records: VLRs keep track of updates and registrations of mobile subscribers. However, VLRs do not necessarily record information about subscribers leaving their jurisdictions for new VLRs. This is because it is the new VLR's responsibility to keep such records. The key fields in VLR location update records are shown in Table 4.

Table 3. Relevant HLR location update record fields.

Field	Type	Description
Served IMSI	M	IMSI of served subscriber
Recording Entity	M	HLR identifier
Old Location	O	VMSC identifier
		VLR identifier
New Location	M	VMSC identifier
		VLR identifier
Update Timestamp	M	Time update was invoked
Update Result	C	Result of location update (if unsuccessful)

Table 4. Relevant VLR location update record fields.

Field	Type	Description
Served IMSI	M	IMSI of served subscriber
Served MSISDN	O	Primary MSISDN of served subscriber
Recording Entity	M	Recording entity (MSC/VLR) identifier
Old Location		(Not present for registration)
	C	VMSC number
	C	Location area code
New Location	M	VMSC identifier
	M	Location area code
	O	Cell id
Update Timestamp	M	Time update was invoked
Update Result	C	Result of location update (if unsuccessful)

5. Tracking Mobile Subscribers

This section discusses how location information pertaining to mobile subscribers may be estimated. It also highlights techniques for refining and verifying location estimates.

5.1 Estimating Mobile Subscriber Locations

Because of their convenience, cell phones have become indispensable to coordinating and executing criminal activities. Cell phones have traditionally been viewed as more anonymous than normal landline phones, but this is not true. CDRs generated during mobile communications provide valuable information about the identities, caller groups and lo-

cations of criminal elements. Much of this information is preserved by service providers because it is relevant to billing, and is, therefore, available to criminal investigators.

CDRs for mobile calls (Table 1) and SMS messages (Table 2) contain IMSIs that identify subscribers, IMEIs that identify handsets, along with timestamped location information. Mobile call CDRs for a network contain the cell ids of all mobile terminated and mobile originated calls in its jurisdiction (Table 1). SMS message CDRs can record the cell ids for all SMS messages (Table 2). Depending on the network topology, the radius served by a cell tower with a specific cell id may range from a few hundred yards to several miles.

When a subscriber moves between different jurisdictions in a mobile communications network, HLR and VLR updates may be required to ensure that the subscriber continues to receive service. Thus, the CDRs generated by HLR and VLR location updates (Tables 3 and 4) contain timestamped information about the movement of the subscribers. Although cell ids are not necessarily recorded in the CDRs for HLR and VLR location updates, it is still possible to analyze the timestamped "roaming" records to determine subscriber locations, e.g., on a roadway between two cities.

5.2 Refining Location Estimates

CDRs provide useful information about subscriber locations, but their estimates may lack specificity and accuracy. Service providers may not create CDRs for all call/message events, the CDRs themselves may not have values for all their fields, and the CDRs may not be stored after their information is summarized to produce billing records. Furthermore, the cell ids listed in CDRs may not provide location information of sufficient accuracy. As mentioned above, the radius served by a cell tower may range from a few hundred yards to several miles. Of course, if is known that a mobile subscriber is traveling in an automobile or train, it is possible to superimpose cell tower locations on a roadmap to obtain more accurate location estimates (possibly 20 to 100 feet).

Cellular network components often generate other useful information that can be used to refine subscriber location estimates. One example is the azimuth of a subscriber relative to a cell tower. A tower with a common triangular antenna has three possible azimuth values, corresponding to 0°, 120° and 240°. The specific angular direction of a mobile subscriber helps refine the location estimate within a cell site. The power level of a subscriber's communications with a cell tower can also help refine location estimates. Mathematical equations relating the power

level to the distance from a cell tower can be used to obtain location estimates within 230 feet [7].

Information for refining location estimates, such as azimuth values and power levels, can be obtained by analyzing a "cell site dump." However, this task is arduous, time-consuming and expensive; typically, such analyses are reserved only for investigations of serious crimes. Note that this information is related to network management, not billing, and no standards govern its collection and storage. Consequently, not every service provider collects such information, and the information, even if collected, may not be stored for more than a few weeks.

5.3 Verifying Location Estimates

In cell site forensics it is extremely important to verify that the location estimates are indeed correct. This is typically done by visiting the probable locations at each cell site with the subscriber's cell phone (if it has been seized). Alternatively, an identical model with the same service plan may be used; this information can be obtained using the IMEI and IMSI values in CDRs. The purpose of the test is to verify that had the cell phone been operating at the location at the time in question, it would have communicated with specific cell towers with the appropriate azimuth values and power levels. On-site testing helps determine whether or not certain cell towers were blocked from receiving mobile communications, for example, by buildings or landscape features. Since network topology and city topography can change fairly quickly, it is important to conduct the on-site verification of location estimates as soon as possible.

6. Conclusions

Cell site forensics provides information about a mobile subscriber's location at specific times. It can place a suspect at or near a crime scene when the crime occurred, or it can provide exculpatory evidence that the suspect was present at some other location at that time. Cell site forensics also yields valuable historical location-time data from CDRs pertaining to a group of mobile subscribers (called a community of interest). This historical data can offer insights into the dynamics of a crime, from planning to execution.

But cell site forensics is not a panacea. It only identifies a "subscriber" (via the IMSI) and the handset (via the IMEI)—not the actual individual who used the cell phone at the time in question. Other types of evidence, e.g., eyewitness reports, closed circuit TV footage and DNA evidence, are required for purposes of attribution. However, cell site forensics,

because it provides location-time data, can help law enforcement agents identify the locations where this additional evidence might exist.

References

[1] L. Dryburgh and J. Hewitt, *Signaling System No. 7 (SS7/C7): Protocol, Architecture and Services*, Cisco Press, Indianapolis, Indiana, 2005.

[2] J. Eberspächer, H. Vögel and C. Bettstetter, *GSM: Switching, Services and Protocols*, John Wiley, Chichester, United Kingdom, 2001.

[3] European Telecommunications Standards Institute, ETSI TS 100 616 V7.0.1 (1999-07), Digital Cellular Telecommunications System (Phase 2+), Event and Call Data (GSM 12.05 Version 7.0.1 Release 1998), 1998.

[4] European Telecommunications Standards Institute, 3GPP TS 23.018 V7.1.0 (2005-09), 3rd Generation Partnership Project, Technical Specification Group Core Network and Terminals, Basic Call Handling, Technical Realization (Release 7), 2005.

[5] A. Fares, *GSM Systems Engineering and Network Management*, 1stBooks Library, Bloomington, Indiana, 2003.

[6] GSM World, GSM subscriber statistics (Q1 2005) (www.gsmworld .com/new/statistics), 2005.

[7] M. Hellebrandt and R. Mathar, Location tracking of mobiles in cellular radio networks, *IEEE Transactions on Vehicular Technology*, vol. 48(5), pp. 1558-1562, 1999.

[8] J. Hoffman, *GPRS Demystified*, McGraw-Hill, New York, 2003.

[9] T. Moore, A. Meehan, G. Manes and S. Shenoi, Forensic analysis of telecom networks, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, New York, pp. 177-188, 2005.

[10] T. Russell, *Signaling System #7*, McGraw-Hill, New York, 2002.