UNIVERSITY OF FREIBURG

DEPARTMENT OF COMPUTER SCIENCE
CHAIR OF COMMUNICATION SYSTEMS

MASTER THESIS

IMSI-CATCHER DETECTION

Author:
Thomas Mayer

Supervisor:
Prof. Dr. Schneider
Dennis Wehrle

January 19, 2012

Abstract:

asjdajslkdajdalsdj

List of Figures

List of Tables

Contents

1 Introduciton

Boundless communication for everyone, everywhere, anytime. That was the main idea and dream behind the development of the Global System for Mobile Communications (GSM) technology. Considering its reception and growth [8, 10, 9] it can be said that GSM was one of the most successful technologies of the last 30 years. Since the advent of portable radio equipment and portable microprocessors, mobile phones became technologically possible in the 80's. From this point on,

1.1 Structure

The remainder of this thesis is structured as follows: Chapter 2 will give an overview of how the GSM network is structured as well as describe the different components needed for operation and how they work together. The second part of this chapter will discuss how the U_m interface, or air interface works and what kind of information can be drawn off this interface. The last part shows how an IMSI-Catcher works and where is it situated in the network shown before. Possible attacks of how an IMSI-Catcher can be introduced in such a network are listed as well. Finally there will be a discussion about the judicial situation in Germany concerning means of electronic surveillance for crime prevention and how this affects privacy and the basic rights of citizens.

The next chapter outlines the frameworks and the hardware that was used for this project.

2 GSM

This chapter will give short overview of some important aspects of GSM. The first section will give a brief historical summary on the evolution of GSM and how it came to be what it is today. In section 2.2 the system architecture and its components as well as protocol basics will be explained that are essential to understand how an IMSI-catcher operates. Section 2.4 will describe how an IMSI-catcher works and how it differs from the system components it replaces.

2.1 A Historical Perspective

The acronym GSM was originally derived fom *Group Spéciale Mobile*. This committee was part of the Conférence Européenne des Administrations des Postes et des Télécommunications (CEPT) 1982, with the task of developing a pan-Eurpean digital cellular mobile radio standard in the 900MHz range. 1986 the frequency range was officially licensed. The foundation of this task group was a direct answer to the development of independent and incompatible analog radio networks during the 80's. Examples of such networks were the C-Netz in Germany the Total Access Communication System (TACS) in the UK or Northern Telecomunication (NMT) in Scandinavia.

In 1987 the committee submitted the basic parameters of GSM in February. Not far after, in September, the Memorandum of Understanding (MoU) was signed in Copenhagen by 15 members of 13 Countries that were dedicated to deploy GSM in their respective countries. This agreement was the basis for allowing international operation of mobile stations, using the interfaces agreed upon earlier that year. CEPT itself was around since 1959 and the member founded the European Communication Standards Institute (ETSI) in 1988. In the same year the committee submitted the first detailed specification for the new communications standard. The acronym was reinterpreted in 1991, after the committee became a part of the ETSI in 1989 to *Global System for Mobile Communications*. In the very same year the specifications for Digital Cellular System 1800 (DCS1800) were also submitted. These were essentially the same specifications, translated in the 1800MHz range and the foundation for the USA's 1900MHz band. Under

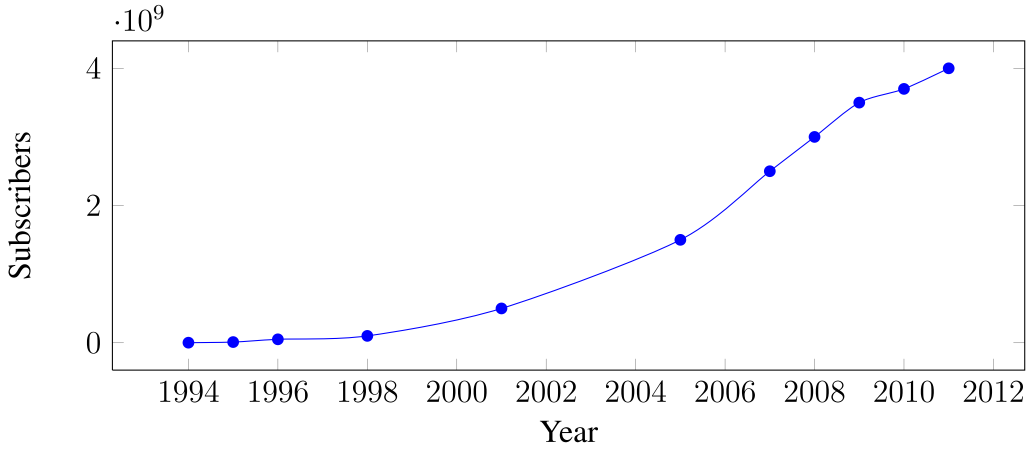

Figure 2.1: Growth of mobile GSM subscriptions. Compiled from [8, 10, 9]

the umbrella of the ETSI, many Sub Technical Committees (STCs) began to work on different aspects of mobile communication, like network aspects (SMG 03) or security aspects (SMG 10). SMG 05 dealt with future networks and especially with UMTS specifications, which eventually became an independent body inside the ETSI.

In 1992 many European countries had operational mobile telephone networks. These networks were a huge success, and as soon as 1993 they already counted more than one million subscribers [8]. Also many networks on different frequency bands (900MHz, 1800MHz, 1900MHz) were started outside Europe in countries like the US or Australia, with Telstra as the first non European provider. The rapid growth of mobile subscribers worldwide until today can be seen in figure 2.1. Three of the main reasons for this rapid growth are explained by Heine [12] as:

- Liberalization of the mobile market in Europe, which allowed for competition and thus resulting in lower prices and enhanced development.
- Expertise within the Groupe Spéciale Mobile and their collaboration with industry.
- The lack of competitive technologies.

In 1998 the Third Generation Partnership Project (3GPP) was founded by 5 organizational partners with the goal of standardization in mobile communications, with focus on developing specifications for a third generation mobile radio system. These partners were Association of Radio Industries and Businesses (ARIB),

Figure 2.2: The 3GPP Logo

ETSI, Alliance for Telecommunications Industry Solutions (ATIS), Telecommunications Technology Association (TTA) and Telecommunications Technology Committee (TTC). This focus was later expanded in the light of the *International Mobile Communications-2000*-project [7] of the International Telecomunication Union (ITU) to

- Devolpment and maintainance of GSM and General Packet Radio Service (GPRS), including Enhanced Data Rates for GSM Evolution (EDGE), which are standards for high speed packet oriented data transmission via GSM.
- Development of a third generation mobile communication system on the basis of the old GSM protocol. This standard is called Universal Mobile Telecomunications System (UMTS)
- An IP based multimedia system.

Up to now, the 3GPP has enhanced mobile standards. In 2005 the first High Speed Downlink Packet Access (HSDPA) network went online. HSDPA [13] is a protocol that enables mobile users to download data with speeds up to 84Mbit/s since release 9. High Speed Uplink Packet Access (HSUPA) [14] is a related protocol in the High Speed Packet Access (HSPA) family that provides similar high speed functionality for uploading data. These and other specification are published on the 3GPP website[1].

2.2 The GSM Network

The GSM network is a distributed, star shaped network type that is built on top of existing telephony infrastructure to additionally connect mobile users. The tele-

[1] http://www.3gpp.org/

Figure 2.3: The main components of a GSM network.

phony network is not only used to connect mobile subscribers to landline phones, but also to connect the different components of the mobile network. The main components of a GSM network can be seen in figure 2.3 as well as the interfaces that are used to connect them. There are different notions of how to distribute these components into functional entities. In the following the classification of [15] will be used. It describes the main parts as:

- Basestation Subsystem (BSS): this part is also called radio network and thus contains all the technology necessary for connecting mobile subscribers to the telephony network and routing their calls. These calls originate from the Mobile Station (MS) that will be explained in section 2.2.1, and travel over the air interface to the receiver stations for further processing. The air interface or U_m interface will be explained in section 2.3, whereas the rest of the subsystem will be argued in section 2.2.2.

- Network Subsystem (NSS): the core network, as it is sometimes called, consists of several entities that are used to establish and route a connection. This is not only limited to calls within the provider's network but also into other provider's networks or the Public Standard Telephone Network (PSTN). The databases that contain subscriber information and location information for connected users are also located here, thus this is the place where mobility management is handled.

- Intelligent Network Subsystem (IN): this part of the network augments the core network with value-added service (VAS) [17]. In order to provide extra functionality the IN consists of several Service Control Point (SCP) databases. Some of the most used services are in fact services of the IN and not core services. Examples are prepaid cards, home areas[1] or telephone number portability.

Other sources define the Operation and Maintainance Subsystem (OMS) [8] or limit the BSS entity to the provider part and define an additional entity for the MS [11, 16]. The three subsystems as well as the MS will now be discussed in greater detail.

[1] This service defines a geographical area, in which lower rates are calculated for mobile calls.

Figure 2.4: Evolution of mobile phones over the last decades.

2.2.1 Mobile Station

With the advent of portable microprocessors in the 80's mobile phones became possible. Advance in technology up to today yielded smaller mobile phones with more functionality year by year to a point where not the technology itself was the limiting factor for size, but the user interface, e.g. button and display sizes. Figure 2.4 shows the evolution of the mobile phone over the last decades. What hasn't changed is the basic distinction between Mobile Equipment (ME) and Subscriber Identity Module (SIM), the parts of which a MS consists.

It is hard to deliver a consistent definition for what a ME is. GSM Recommendation 02.07 [2] summarizes the mandatory and optional features of a MS. Some of the most important mandatory features are [12]:

- Dual Tone Multi Frequency (DTMF) signaling capability.
- Short Message Service (SMS) capability.
- The cyphering algorithms A5/1 and A5/2 need to be implemented. These are discussed in detail in section 2.2.3.
- Display capability for short messages and dialed numbers, as well as available Public Land Mobile Network (PLMS)s.
- Capable of doing emergency calls without SIM card.
- Machine fixed International Mobile Equipment Identifier (IMEI). In a strict sense, this disqualifies many modern mobile phones, since the IMEI is not fixed onto the device itself but is rather part of the software or firmware respectively. Tools like *ZiPhone*[1] for iOS devices[2], especially iPhone, can change this supposedly unchangeable identifier.

The range of devices complying to these specifications is rather large, so categorizing can be challenging. The intuitive approach would be to establish buckets by device type, but there are so many different devices as well as hybrid devices out there that this approach would not only be impracticable, but also too ambiguous. Does a smartphone belong into the same category as a Personal Digital

[1] `http://www.ziphone.org/`
[2] `http://www.apple.com/ios/`

Figure 2.5: Structure of the IMSI.

Assistant (PDA) or in the category of basic mobile phones; and what would a basic mobile phone be?

Another way to categorize different MEs is by supported frequency band and power class rating according to GSM 05.05[1]. Most mobile phones and smartphones belong to power class 4 and 5, which are for handheld devices. Class 4 devices have and output of 2/33 W/dBm and class 5 0.8/29 W/dBm. Classes with higher output are typically installed devices, e.g. in cars. These classes differ for the different frequency bands, since output needed in higher frequency bands (1800/1900 MHz) is less compared to the 900MHz band. The supported band is also common category, since it describes in which countries a mobile phone can be used. However it is more common nowadays that ME supports two bands or even all three bands. These are called dual-band and tri-band devices respectively.

As the name suggests, the SIM card is essentially a data storage that holds user specific data. This separation is interesting for the GSM user since it allows him/her to exchange the ME without having to contact the provider. Thus it can be used on different frequency bands and is one of the preconditions for roaming. The SIM card can either be in plug-in format or ID-1 SIM format which is normally used for telephone cards, credit cards or car installed ME. The plug-in format is also called ID-000 and can be found in ISO/IEC 7810[3].

The most important information stored on a SIM card are the International Mobile Subscriber Identification (IMSI) and the Secret Key (Ki). A subset of other parameters stored on the Electrically Erasable Programmable Read-Only Memory (EEPROM)of the card can be seen in Table 2.1.

This key is used to generate the Cyphering Key (Kc), as will be explained in Section 2.2.3. Most of this data, although not the security relevant Ki can be read via a USB SIM card reader, which can be bought for around $10 on the web. Since Ki never leaves the card, Kc has to be dynamically generated on the card. This can be done since the card itself has a microprocessor that manages the security relevant data. Key functions, like running the GSM key algorithm, verifying a Personal Identification Number (PIN) or reading a file can be accessed through the microprocessor via a communication protocol. A brief description of the protocol and functionalities can be found in [15].

The IMSI as described in GSM 23.003[5] uniquely identifies a subscriber. The structure can be see in Figure 2.5. It has at most 15 digits and is divided into three parts, Mobile Country Code (MCC),Mobile Network Code (MNC) and Mobile

Parameter	Description
Security Related	
A3/A8	Algorithms required for authentication and generation of the session key
Ki	Secret key
Kc	Session key, generated from a random number and Ki vie A8
PIN	Secret numeric password to use a SIM card
PUK	Secret numeric password to unlock the SIM card
Subscriber Data	
IMSI	Subscriber identification
MSISDN	Telephone number
Network Related	
LAI	Identifier of the current location area
TMSI	Temporary IMSI
Home PLMN	Multiple entries to identify the home PLMN

Table 2.1: Subset of data stored on a SIM card. Adopted from [12]

Country	MCC
Germany	262
France	208
USA	310 - 316
UK	234 - 235
Switzerland	228
Austria	232
Poland	260

Provider	Country	MNC
T-Mobile	Germany	01, 06(R)
Vodafone	Germany	02, 04(R), 09(R)
E-Plus	Germany	03, 05(R), 77(T)
O_2	Germany	07, 08(R), 11(R)
Orange	France	00, 01, 02
Swisscom	Switzerland	01
A1	Austria	01, 09

Table 2.2: Mobile Country and Network Codes. (R) denotes that the MCC is reserved but not operational as of yet, whereas (T) denotes a operational test network.

Subscriber Identification Number (MSIN), of which only the last part is the personal identification number of the subscriber. The first two are also called Home Network Identifier (HNI). The three digit MCC describes the country code, the area of domicile of the mobile subscriber. The MNC is an identification number for the home PLMS. This can either have two or three digits depending on the MCC. It is not recommended by the specification and thus not defined to mix two and three digit MNCs for a single MCC. These country codes are assigned by the ITU in ITU E.212[18]. An excerpt can be found in Table 2.2. The third part, the MSIN is a number consisting of up to ten digits, which is used for authentication of the mobile subscriber against his provider. MNC and MSIN together are called National Mobile Subscriber Identity (NMSI).

2.2.2 Base Station Subsystem

The BSS is the part of the network that provides the hard- and software for physically connecting MSs to the providers network. Its main components are the Base Station Controller (BSC), the Base Station Transceiver (BTS) and the Transcoding Rate and Adaption Unit (TRAU). Connecting of a mobile subscriber works via radio, which is why this subsystem is sometimes also called the radio network [15]. Inside the radio network of a certain area, there is one BSC that connects to multiple BTS and one TRAU. While the Transceiver station act as receiver for radio signals the controller coordinates the different receivers and relays the incoming signals to the core network. Since signals inside the core network are transmitted at other rates than in the radio network, rates need to be adapted, which is done by the TRAU.

The Cellular Principle

Baste Station Controller

Base Transceiver Station

Frequencies

Transcoding rate and Adaption Unit

2.2.3 Network Subsystem

The most important task of the NSS or Network Switching Subsystem is to establish connections and route calls between different locations. This is done by so called Mobile Switching Center (MSC), that can route a call either to another MSC, into the PSTN or another provider's network. Apart from routing, the NSS also provides the means to administer subscribers inside the network. Facilities to support this task are the Home Location Register (HLR), the Visitor Location Register (VLR), the Equipment Identity Register (EIR) as well as the Authentication Center (AC) that will now be described in further detail. The Short Message Service Center (SMSC) is also part of this subsystem handling text messages. A possible arrangement of these components is displayed in Figure 2.3.

Mobile Switching Center

The MSC is the component that does the actual routing of calls and is thus the core component of the NSS. Thus it basically works like any other Integrated Services Digital Network (ISDN) exchange device with additional functionality to manage mobility Since it would be the amount of signalling inside a PLMS would be far to big for a single MSC, there is one for every Location Area (LA). Amongst others its most important tasks are Call Control (CC) and Mobility Management.

CC entrails registration when the subscriber connects to the network as well as routing the calls or text messages from one registered subscriber to another. This routing can include transmitting calls to landlines or to networks of other providers. MSCs that bind the provider's networks to other provider's networks or the PSTN are called Gateway MSCs.

The above part is also true for pure landline switching centres. What sets a mobile switching centre apart is called Mobility Management. Since the participants can freely move around in the network and thus cannot be identified the same way

Name	Between	Function
A	MSC ↔ BSS	BSS management data for Mobility Management and Call Control
B	MSC ↔ VLR	MSC receives data about MSs in the current area and sends data from Location Updates
C	MSC ↔ HLR	MSC can request routing data during call setup and send e.g. charging information
D	HLR ↔ VLR	Exchange of location-dependent subscriber data and updating the HLR (MSRN etc.)
E	MSC ↔ MSC	Executing a Handover when subscriber changes to a new MSC
F	MSC ↔ EIR	Checking white-/grey- and blacklists before giving access to the network
A_{bis}	BSC ↔ BTS	BSC receives data from MS via the BTS
U_m	BTS ↔ MS	Registration procedure, call data etc. as well as broadcast information about the network and the base station

Table 2.3: Interfaces inside the core network (upper part) and the radio network (lower part)

as a fixed landline participant, authentication before using the offered services is important. Another consequence of mobility is, that the network has to keep track of where a subscriber is and through which MSC it can be reached. This is done via Location Updates. Also during calls if the subscriber leaves the respective service area of the switching centre, then the call needs to be transferred without being interrupted. A procedure called Handover achieves just that.

For this central role to work it is necessary to be connected to all the other components of the NSS. This is done via different connectors called Interfaces. A brief description of what the different interfaces in a GSM network are and what their respective function is can be seen in Table 2.3.

Home Location Register

The HLR is the central database in which all personal subscriber related data is stored. The entries can be divided into two classes, permanent administrative and temporary data. Part of this administrative data is which services a subscriber has access to and which are prohibited (e.g. roaming in certain networks). The data itself is indexed with the customer's IMSI, to which multiple telephone numbers can be registered. Since these Mobile Subscriber Integrated Services Digital Network Numbers (MSISDNs) are independent from the IMSI a subscriber can change his telephone number and thus also move the telephone number along should he/she decide to switch to a new provider. Basic services that access is stored for in the HLR are amongst others the ability to receive and send telephone calls, use data services or send text messages. Additional services, called Supplementary Services like call forwarding or display of phone numbers during calls can also be set or unset in this database. It is up to the provider if these services are available freely or bound to a fee. The temporary data enfolds the current VLR and MSC address as well as the Mobile Station Roaming Number (MSRN) which is essentially a temporary location dependent ISDN number.

Visitor Location Register

As can be seen in Figure 2.3 there can be multiple VLRs, one for each area in a network. These registers can be seen as caches for data located in the HLR. Thus their are intended to reduce signalling between the MSC and the HLR. Each time a subscriber enters a new area, that is serviced by a new MSC, data for this subscriber is transferred to the respective VLR from the HLR. Such data includes the IMSI and the MSISDN as well as authentication data and information on which services are available to that particular subscriber. Additionally the subscriber is assigned a temporary IMSI, called Temporary IMSI (TMSI) and information in which LA the MS was registered last. In this way the regular IMSI is not used and can thus not be harvested by tapping into the radio channel. While it is possible to operate the VLR as a standalone entity, in most cases it is implemented as a software component of the individual MSC.

Equipment Identification Register

The EIR is a database that contains the IMEIs of registered MSs. It is used to determine whether a particular MS is allowed to participate in communications. For that purpose a white, a grey and a black list are used. IMEIs on the white list are allowed, while equipment that is grey-listed will be checked. The blacklist is used to refuse access to e.g. stolen equipment that has been reported to the provider. In Germany only the providers Vodafone and E-Plus support blacklisting of IMEIs[6]. Different companies like Airwide Solutions (now aquired by

Figure 2.6: Authentication procedure

Manivir)[1] offer centralised lists for providers in their Central Equipment Identity Registers (CEIRs).

Authentication Center

The AC is the network component responsible for authenticating mobile subscribers. It is a part of the HLR and the only place, apart form the customer's SIM card where the secret key Ki is stored. The authentication is not only done once when the subscriber connects to the network, but rather on many occasions e.g. the start of a call or other significant events to avoid misuse by a third party. This authentication routine is a key based challenge-response procedure outlined in Figure 2.6. The steps of the procedure can be summarized as follows:

1. User connects to the network or triggers an event that needs authentication at the MSC.

   In the first case the IMSI is part of the authentication request and the AC starts with searching for the corresponding Ki and authentication algorithm A3. An authentication triplet is build using Ki which consists of the components:

   - RAND: a 128 bit random number.
   - SRES: a 32 bit number called signed response, which is generated by A3 with Ki and RAND as inputs.
   - Kc: the ciphering key that is used to cypher the data during transmission. It is also generated with Ki and RAND.

   To save signalling bandwidth, usually more than one authentication triplet is generated and returned to the MSC by the AC. It should be noted that, since a separate cyphering key is used, the secret key never leaves the AC.

   In the second case, either a previously generated authentication triplet is used, or new authentication triplets are requested.

2. RAND is transmitted to the MS by the MSC where the signed response SRES* is created by the SIM card using A3, Ki and RAND.

3. An authentication response containing SRES* is sent back to the MSC.

[1] http://www.mavenir.com/

4. If SRES and SRES* are the same, the subscriber is authenticated.

Remarkable properties of this procedure are that by using a cyphering key that is generated by a random number and a secret key, the secret key itself never leaves the AC. Apart from that the use of a random number prevents replay attacks on SRES. It should also be noted that this way of authenticating only works for authenticating the subscriber to the network. It is a one way authentication. The subscriber needs to trust the network. This is a design flaw that IMSI-Catchers use to lure MS into their fake network. In UMTS networks that flaw was fixed and the authentication procedure was made mutual.

2.2.4 Intelligent Network

The two subsystems above are necessary for the correct operation of a GSM network. While the IN is not essential for operation, all providers offer additional services that need additional logic and databases. These databases are called SCP databases and are one of three possible Signaling System 7 (SS-7) nodes. They can influence the build-up of a connection or modify parameters for that specific connection.

Two of the most common services offered are Location Based Services (LBS) and prepaid services. An Example for a well known LBS that is provided by the IN is a dynamic calling rate service. If the mobile subscriber is in a specific geographical area, the SCP can modify the Billing Record to lower the calling rates. This is known as home-zone. If a mobile subscriber uses a prepaid service, an account is created for this subscriber that can be topped up. Afterwards calls and text messaged use up the money on that account. This is an alternative to a monthly bill and attracted many customers since its advent in the mid 90's. For this service the SCP needs to constantly update the money on the account during calls and when text messages are sent.

Since these services were defined as additional and thus no specification existed, they evolved into vendor specific proprietary networks, that were not interoperable. To standardize these services, 3GPP and ETSI defined the Customized Applications for Mobile network Enhanced Logic (CAMEL) protocol in TS 23.078[4]. CAMEL specifies a protocol much like Hyper Text Transfer Protocol (HTTP) that regulates how the different components of a GSM network exchange information. As such it is not an application itself but rather a framework to build vendor independent, portable services.

2.3 The U_m Interface

2.3.1 Layers

2.3.2 The Radio Channel

2.3.3 Logical Channels

2.4 IMSI-Catcher

2.4.1 Mode of Operation

2.4.2 Possible Attacks

2.4.3 Law situation in Germany

Bibliography

[1] Radio access network: Radio transmission and reception. GSM 05.05, http://www.3gpp.org/ftp/Specs/archive/05_series/05.05/0505-8k0.zip, 1999.

[2] Digital cellular telecommunications system (phase 2+): Mobile stations (ms) features. GSM 02.07, http://www.3gpp.org/ftp/Specs/archive/02_series/02.07/0207-710.zip, 2000.

[3] Identification cards – physical characteristics. ISO/IEC 7810:2003, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31432, 2003.

[4] Customised applications for mobile network enhanced logic. GSM 23.078, http://www.3gpp.org/ftp/Specs/archive/23_series/23.078/23078-b00.zip, 2011.

[5] Numbering, addressing and identification. GSM 23.003, http://www.3gpp.org/ftp/Specs/archive/23_series/23.003/23003-a30.zip, 2011.

[6] Equipment identity register. http://en.wikipedia.org/wiki/Central_Equipment_Identity_Register, 2012.

[7] CHAUDHURY, P., MOHR, W., AND ONOE, S. The 3gpp proposal for imt-2000. *Communications Magazine, IEEE 37*, 12 (1999), 72–81.

[8] EBERSPÄCHER, J., VÖGEL, H.-J., BETTSTETTER, C., AND HARTMANN, C. *GSM – Architecture, Protocols and Services*. Wiley, 2009.

[9] Gsm/3g stats. http://www.gsacom.com/news/statistics.php4, 2011. [Accessed: 28/11/2011].

[10] Brief history of gsm and the gsma. http://www.gsm.org/about-us/history.htm, 2011. [Accessed: 28/11/2011].

[11] HAUG, T. Overview of gsm: philosophy and results. *International Journal of Wireless Information Networks 1*, 1 (1994), 7–16.

[12] HEINE, G. *GSM networks: protocols, terminology, and implementation*. Artech House, 1999.

[13] UE radio access capabilities. 3GPP TS 25.306, `http://www.3gpp.org/ftp/Specs/html-info/25306.htm`, 2011.

[14] Medium access control (mac) protocol specification. 3GPP TS 25.321, `http://www.3gpp.org/ftp/Specs/html-info/25321.htm`, 2011.

[15] SAUTER, M. *Grundkurs mobile Kommunikationssysteme : von UMTS, GSM und GRPS zu Wireless LAN und Bluetooth Piconetzen*. Vieweg, 2006.

[16] SCOURIAS, J. Overview of gsm: The global system for mobile communications. *University of Waterloo* (1996).

[17] TELECOMUNICATION STANDARDIZATION SECTOR OF ITU. Intelligent network. *SERIES Q: Switching and Signaling Q1200*, 7 (1997).

[18] TELECOMUNICATION STANDARDIZATION SECTOR OF ITU. List of mobile country or geographical area codes, 2010.

Acronyms

3GPP	Third Generation Partnership Project 4, 5, 12
AC	Authentication Center 10, 12
ARIB	Association of Radio Industries and Businesses 4
ATIS	Alliance for Telecommunications Industry Solutions 5
BSS	Basestation Subsystem 6
CAMEL	Customized Applications for Mobile network Enhanced Logic 12, 13
CEIR	Central Equipment Identity Register 12
CEPT	Conférence Européenne des Administrations des Postes et des Télécommunications 3
DCS1800	Digital Cellular System 1800 3
DTMF	Dual Tone Multi Frequency 7
EDGE	Enhanced Data Rates for GSM Evolution 5
EEPROM	Electrically Erasable Programmable Read-Only Memory 8
EIR	Equipment Identity Register 10, 12
ETSI	European Communication Standards Institute 3–5, 12
GPRS	General Packet Radio Service 5
GSM	Global System for Mobile Communications 1, 3, 5, 6, 12, 13
HLR	Home Location Register 10, 11

HNI	Home Network Identifier 10
HSDPA	High Speed Downlink Packet Access 5
HSPA	High Speed Packet Access 5
HSUPA	High Speed Uplink Packet Access 5
HTTP	Hyper Text Transfer Protocol 13
IMEI	International Mobile Equipment Identifier 7, 12
IMSI	International Mobile Subscriber Identification 8, 11
IN	Intelligent Network Subsystem 6, 12
ITU	International Telecomunication Union 5, 10
Kc	Cyphering Key 8
Ki	Secret Key 8
LA	Location Area 11
LBS	Location Based Services 12
MCC	Mobile Country Code 10
ME	Mobile Equipment 7, 8
MNC	Mobile Network Code 10
MoU	Memorandum of Understanding 3
MS	Mobile Station 6, 7, 11, 12
MSC	Mobile Switching Center 10, 11
MSIN	Mobile Subscriber Identification Number 10
MSISDN	Mobile Subscriber Integrated Services Digital Network Number 11
MSRN	Mobile Station Roaming Number 11
NMSI	National Mobile Subscriber Identity 10
NMT	Northern Telecomunication 3
NSS	Network Subsystem 6, 10
OMS	Operation and Maintainance Subsystem 6
PDA	Personal Digital Assistant 8
PIN	Personal Identification Number 8
PLMS	Public Land Mobile Network 7, 10
PSTN	Public Standard Telephone Network 6, 10

SCP	Service Control Point 6, 12
SIM	Subscriber Identity Module 7, 8
SMS	Short Message Service 7
SMSC	Short Message Service Center 11
SS-7	Signaling System 7 12
STC	Sub Technical Committee 4
TACS	Total Access Communication System 3
TMSI	Temporary IMSI 11
TTA	Telecommunications Technology Association 5
TTC	Telecommunications Technology Committee 5
UMTS	Universal Mobile Telecomunications System 5
VAS	value-added service 6
VLR	Visitor Location Register 10, 11