Abstract:

asjdajslkdajdalsdj

Contents

1 Introduciton **1**
1.1 Structure . . . 1

2 GSM **3**
2.1 A Historical Perspective . . . 3
2.2 The GSM Network . . . 5
2.2.1 Mobile Station . . . 6
2.2.2 Network Subsystem . . . 9
2.2.3 Intelligent Network . . . 14
2.2.4 Base Station Subsystem . . . 15
2.3 The U_m Interface . . . 22
2.3.1 Radio Transmission . . . 22
2.3.2 Logical Channels . . . 26
2.3.3 Layers . . . 28
2.4 IMSI-Catcher . . . 31
2.4.1 Mode of Operation . . . 32
2.4.2 Law Situation in Germany . . . 32

3 IMSI Catcher Detection **33**
3.1 Procedure . . . 33
3.1.1 Information Gathering . . . 33
3.1.2 Information Evaluation . . . 33
3.2 Frameworks and Hardware . . . 33
3.2.1 OsmoconBB . . . 33
3.2.2 Motorola C123 . . . 33
3.3 Implementation . . . 33
3.4 IMSI Catcher Detection System . . . 33
3.4.1 Configuration . . . 33
3.4.2 Operation . . . 33

4 Evaluation **35**
4.1 Open Field Statistics . . . 35
4.1.1 Bayesian Filter . . . 35
4.1.2 Detection System . . . 35

4.2 Example Scenarios 35

5 Conclusion **37**
5.1 Future Work 37

Bibliography **I**

Acronyms **VII**

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 which place in the network an IMSI-catcher tries to take over. The U_m interface will be described in detail in Section 2.3 since this is the entry point for gathering information from IMSI-catchers. Section 2.4 will finally explain how an IMSI-catcher works and how it differs from the system components it replaces as well as state from a technical and law perspective why these devices have become a threat to all-day privacy.

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 the umbrella of the ETSI, many Sub Technical Committees (STCs) began to work on different aspects

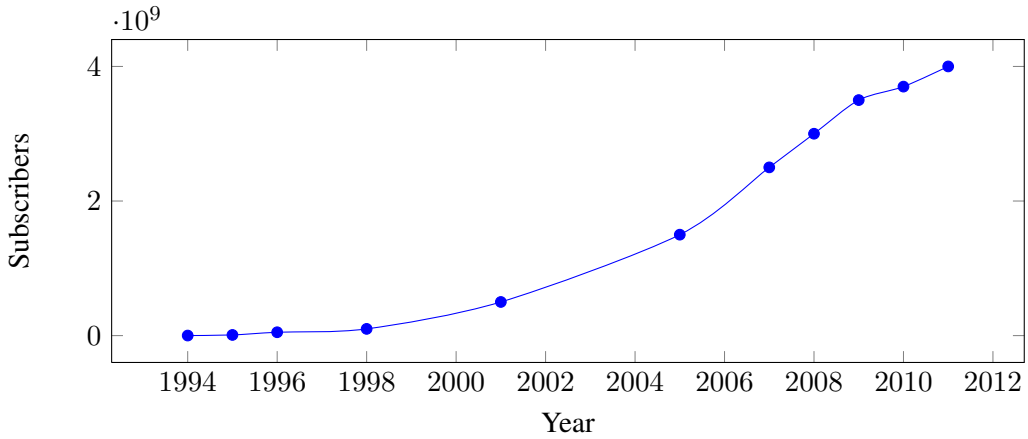


Figure 2.1: Growth of mobile GSM subscriptions. Compiled from [8, 10, 9]

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), 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

- Development and maintenance 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 telephony 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 2.2 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 2.2.4.
- 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.

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

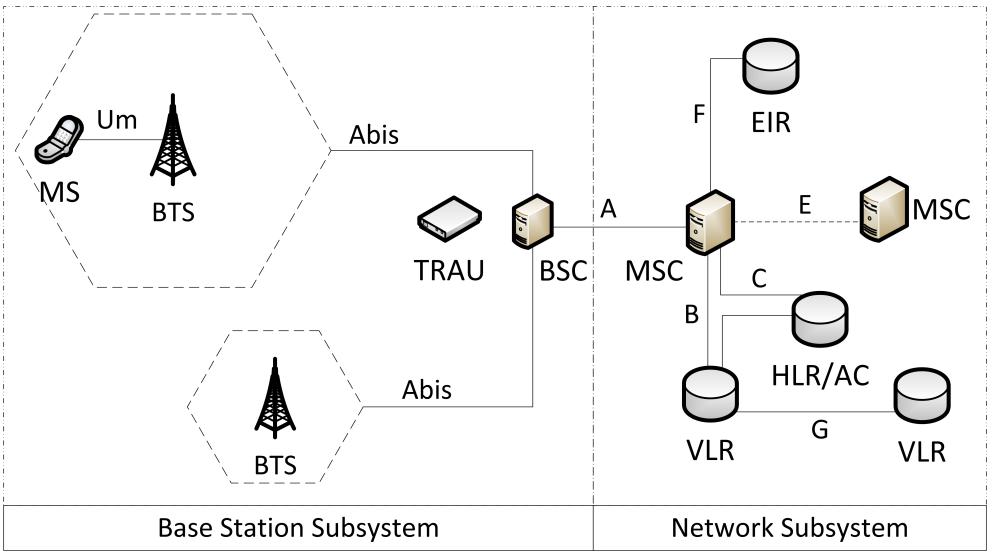


Figure 2.2: The main components of a GSM network. The TRAU can be either build in to the BTS or BSC, here the BSC was chosen.

- 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.

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. 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]:

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

- 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 2.2.2.
- 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 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, or the north american 850MHz 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 four bands. These are called dual-band, tri-band and quad-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].

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

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]

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 2.2.2. 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. It has at most 15 digits and is divided into three parts, Mobile Country Code (MCC),Mobile Network Code (MNC) and Mobile 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

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.

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 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 2.2.

Mobile Switching Center

The MSC is the component that does the actual routing of calls and therefore the core component of the NSS. It basically works like any other Integrated Services Digital Network (ISDN) exchange device with additional functionality to manage mobility. Since 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 (MM).

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 transmission of 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 from these is called MM. Since the participants can freely move around in the network and thus cannot be identified the same way 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, that update the current location in the databases for other MSCs to look up. Also during calls if the subscriber leaves the respective service area of the switching centre, 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 connecitons 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.

The U_m interface will be of special interest to this project since it is the source for gathering broadcast information about the network and the respective base stations without directly registering with them. The interface itself and how to harvest information will be explained in detail in Section 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.

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

Visitor Location Register

As can be seen in Figure 2.2 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 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 2.3. 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:

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

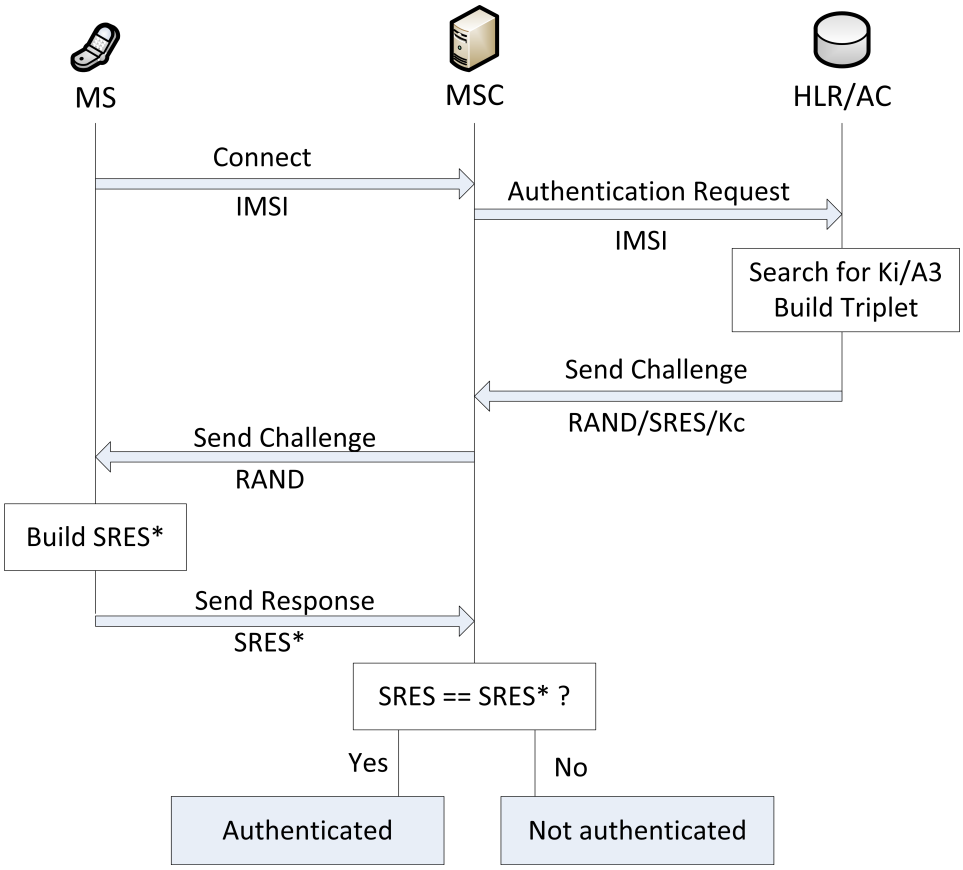


Figure 2.3: Authentication procedure.

- 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.

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 [15].

2.2.3 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

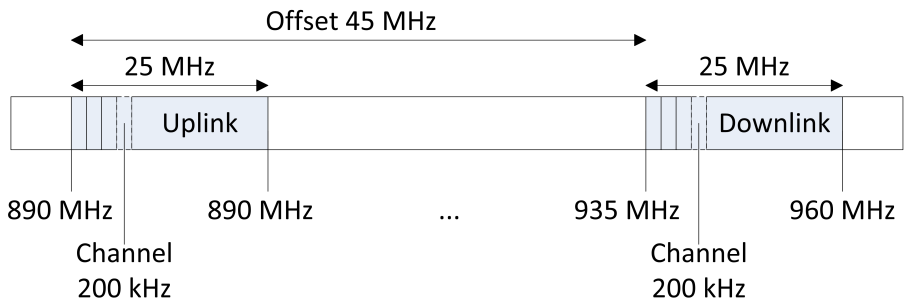


Figure 2.4: Mapping of functional entities on the 900Mhz band.

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.

2.2.4 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.

Before discussing the individual components of this subsystem, it is important to understand how the frequencies in the radio network are used, and what architectural impacts this sparse resource has on the network and the components itself.

Frequencies and the Cellular Principle

A frequency band as shown in Figure 2.4 is distributed into different functional entities. The band is divided into a range for the uplink, the part that is used by the MS to upload data into the network and the downlink, that is utilised by the network to send data back. In the 900MHz band each of these has a width of 25MHz. For other bands the numbers differ and can be seen in Table 2.4 but the functionality is the same. These bands themselves are furthermore divided into channels, each spanning 200kHz, which accounts for 125 channels on 25MHz.

Each of which is identified by its Absolute Radio Frequency Number (ARFCN). This is a simple numbering scheme, given to those 200kHz channels. The frequencies and ARFCNs are connected as follows:

$$F_{\text{Uplink}} = \text{Start}_{\text{Band}} + 0.2 \cdot (\text{ARFCN} - (\text{Start}_{\text{ARFCN}} - 1)) \tag{2.1}$$

$$F_{\text{Downlink}} = F_{\text{Uplink}} + \text{Offset}_{\text{Band}} \tag{2.2}$$

In case of the 900MHz Band this would be:

$$F_{\text{Uplink}} = 890 + 0.2 \cdot (\text{ARFCN} - (1 - 1)) \tag{2.3}$$

$$= 890 + 0.2 \cdot \text{ARFCN} \tag{2.4}$$

$$F_{\text{Downlink}} = F_{\text{Uplink}} + 45 \tag{2.5}$$

A short overview of the ARFCNs can also be seen in Table 2.4.

An additional method which is called time multiplexing, which will be explained in further detail in Section2.3, makes is possible to map $125 \cdot 8 = 1000$ channels that could be used for voice transmission onto that band. Some of these channels need to be used for signalling. Even though the number by itself seems high it would never suffice to service a large urban area. This is one of the reasons why another frequency band in the 1800 MHz range has been opened, with 75 MHz up- and downlink supporting 375 channels. That by itself would also never suffice to service the huge number of subscribers, therefore the GSM network like any other modern mobile radio network is based on a cellular architecture which makes it possible to reuse frequencies. The range of one receiver station is drastically reduced to service only a small area. This is called the cell of the BTS, which in theory can be approximated by a hexagon. Each of these cells is assigned a different frequency, to avoid interference. However after a certain distance, the frequency reuse distance D, is covered, the exact same frequency can be used again by another BTS. D is chosen large enough so that interference doesn't have an impact on overall call quality. Figure 2.5 shows such an arrangement. Also a comparison with realistic cells can be seen, which differ in their appearance from the optimized hexagon model. The borders are blurred because of interference, reflection- and shadowing effects, and cells in the more urban areas are smaller than cells on the countryside, where the density of subscribers is less and thus can be handled by fewer BTSs. The band has been divided

Table 2.4: Frequencies in the different bands [15].

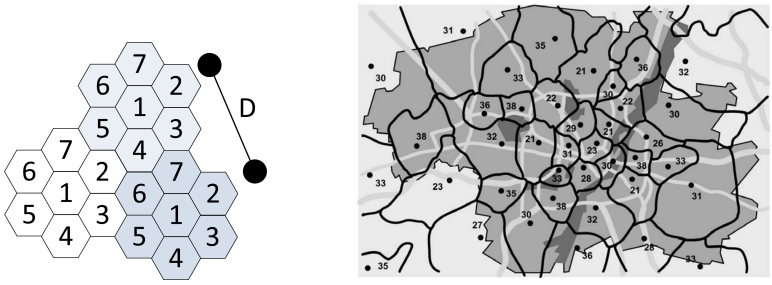


Figure 2.5: Theoretical arrangement of radio cells compared to a realistic alignment. Cells with the same number share the same frequency [8].

into 7 frequency ranges, which are only reused (cells with the same number) after distance D is covered. For an arbitrary division of the frequency band into k partitions and a cell radius of R geometric derivations from the hexagon model yield for the frequency reuse distance D [8]:

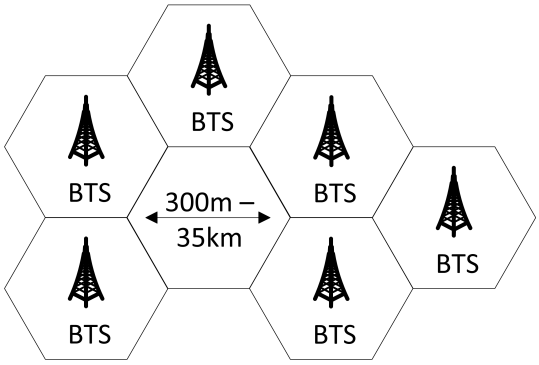
$$D = R \cdot \sqrt{3k} \tag{2.6}$$

This procedure raises the number of effectively usable by a large factor. However certain disadvantages [12] come with this procedure as well. Increasing the amount of receivers automatically increases the cost of infrastructure for the provider. Due to the nature of the mobility of subscribers, this increases the amount of Handovers needed, since it is more likely that a subscriber leaves a small cell during an active call. Also an update of the location of a subscribers needs to be done more often, to ensure reachability for incoming calls. These inflict increased signalling load on the network itself.

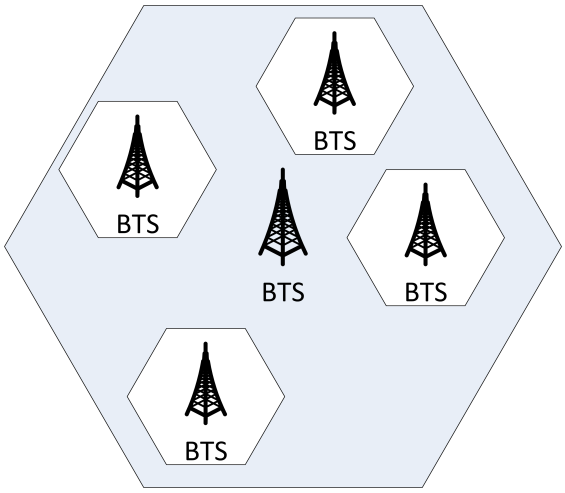
Base Transceiver Station

Also called Base Stations are the entry points to the network for subscribers. Theoretically a BTS can serve a cell of 35 km radius, however this is decreased by interference, reflection- and shadowing effects. The limiting factor here are the number of subscribers itself and the ME that is used by them. A single station can only serve a limited number of users which yields a radius as low as 100 m for a single BTS [15] in dense urban housing areas. On the countryside where population is less dense, the limiting factor can also be transmission power of the ME. Therefore cells with a radius above 15 km are seldom seen.

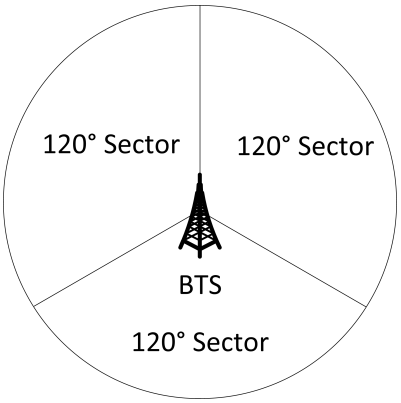
BTSs and their corresponding cells can have different configurations depending on load, or morph structure of the surroundings. The main configurations will now be dis-



(a) Stantard configuration.



(b) Umbrella cell configuration.



(c) Sectorised configuration.

Figure 2.6: Common base station configurations. Compiled from [12].

cussed shortly. In a *standard configuration* every base base station has its own Cell Identity (CI), it is a one to one mapping of cells to BTS. This is an cost effective way of providing service to a rural or sparse settled area. An comparative illustration of configurations can be found in Figure 2.6. The *umbrella configuration* is build around one central BTS that is on high ground compared to its neighbours and has a higher transmission power. Thus the notion of this particular base station wrapping all the others in the area. Due to interference the frequency used by the wrapping base station cannot be used by the others. Nevertheless in some scenarios like alongside highways in urban areas this makes sense. A car that moves fast from one cell to the next may need a lot of Handovers thus inflicting a large amount of signalling load on the network. These fast moving subscribers are assigned to the umbrella station, that way less to no Handovers are needed. This configuration however is not defined in the GSM specifications and needs additional software in the BSC, thus it is considered a proprietary function [12]. The *sectorized configuration* has become the de facto standard for urban areas. In the other configurations a single BTS covers always a 360° area, and a certain distance is kept to its next neighbour to avoid interference in overlapping areas. The idea is to use antennas which only cover a certain angle, like 180°, 120° or 60° dividing a cell into two, three or six sectors respectively each having its own BTS. Main advantages are that each single BTS has to deal with less subscribers and that in a multi-sector configuration frequencies can be reused inside a cell, which is a great advantage for these densely settled areas.

Baste Station Controller

The BSC is the central unit in the BSS. It can be compared to a digital exchange in a standard telephone network with additional mobile extensions. The design idea was to remove all radio related load from the MSC into the radio subsystem. Therefore a BSC manages the multitude BTSs in the BSS.

First and foremost it is a switching centre. This means it has to switch incoming traffic channels from the MSC over the A-interface to channels on the outgoing A_{bis}-interface which leads over the BTS and thus the air interface to different MSs. As a result the initialisation and maintenance of signalling and voice channels are its main tasks. What channels are and how they are established is explained in Section 2.3.2. For the sake of functional explanation of the BSC it will suffice to regard a channels as a communication line for a particular purpose like receiving or sending voice data or another channel for sending broadcast information. Due to the nature of a mobile network certain other tasks have to be performed like Handovers and power management [15]. We will now look at the different tasks in more detail.

A *signalling channel* is needed when a subscriber wants to start a call or send a text message. The MS sends a channel request message to the BSC which needs to check if any Standalone Digital Control Channels (SDCCHs) are free. If there are free channels, one of those channels is activated via the BTS and an immediate assignment message

is sent via the Access Grand Channel (AGCH) containing the number of the assigned channel. From this point on the MS can sent data on the assigned channel that reach the MSC. For incoming calls a prior step has to be taken. The MSC sends a message to the BSC that contains the IMSI, TMSI and LA of the subscriber that is being called or texted. This message is forwarded to and broadcasted by all cells in that LA on the Paging Channel (PCH). As soon as this message arrives at the respective MS it requests a channel with the procedure outlined above.

After a signalling channel is found that way, a *voice channel* can be initialised. The MSC sends an assignment request message to the BSC after the start of the call has been determined on the previously assigned SDCCH between the MSC and the MS. A free Traffic Channel (TCH) is assigned and the MS can tune in to this channel and send an acknowledgement to the BSC, which in turn sends an acknowledgement that the assignment has been completed to the MS and the MSC.

Power management is an essential part for heightened mobility. Basis for power management is that continuous measurements have to be done. These signal quality measurements are taken by the BTS and forwarded to the BSC. If transmission strength has to be turned up or can be turned down, the BSC informs the BTS which in turn distributes the information periodically to the connected mobile phones via a Slow Access Control Channel (SACCH). Minimisation of transmission power has the advantage of longer uptime for MSs since the battery will be less strained.

As mentioned before a *Handover* is necessary when a subscriber leaves the area of a cell and needs to be assigned to another one or if the reception of the current cell at the subscriber's end is far worse than those of neighbouring cells. A Handover takes place during an active call therefore first of all a TCH in the target cell has to be activated. Once this is done the new cell address and frequency is sent to the MS over the Fast Access Control Channel (FACCH) along with a command that triggers the Handover. After synchronising with the new cell an acknowledgement is sent by the base station to the controller to switch the voice connection to the new cell. What remains is freeing the old TCH for further use with other subscribers.

Transcoding rate and Adaption Unit

Inside the NSS voice data is moved with 64 kbit/s over E-1 connections. The resources on the air interface are much scarcer, therefore this amount of voice data cannot directly be sent to MSs through the radio network. The data rate on the U_m interface for voice is about 22.8 kbit/s as will be broken down in detail in Section 2.3.1. Since the channel is noisy and prone to errors, a lot of this bandwidth has to be subtracted for error correction purpose leaving around 13 kbit/s for actual voice data [15]. The 64 kbit/s PCM signal is sent from the MSC to the BSC on its way, it is compressed and then sent over the air interface. On the other side, the compressed 13 kbit/s signal is decompressed to 64 kbit/s again. The compression and decompression on the subscriber's side is handled by

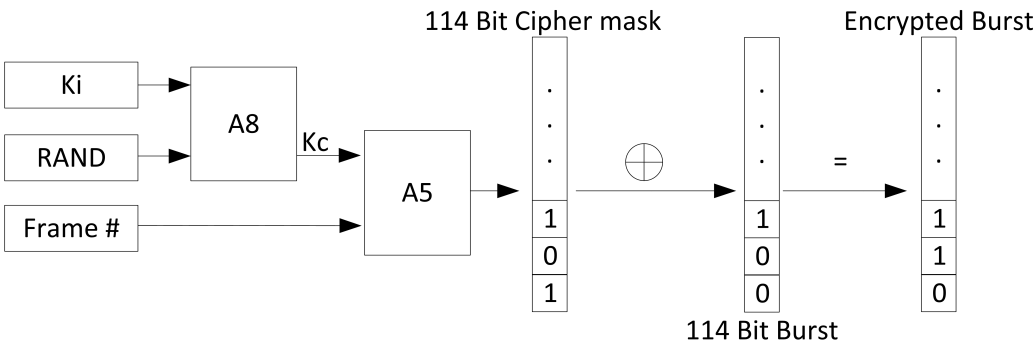


Figure 2.7: Cyphering procedure for one frame of voice data. Adopted from [15].

the ME while on the network side the TRAU is responsible for these tasks. Additionally the TRAU can choose from a variety of codecs (compression/decompression algorithms). The one normally used is called Full Rate codec. Another interesting codec is the Half Rate codec, which compresses the voice signal to 7 kbit/s thus making it possible to route double the amount of TCHs since one channel can be used to transfer two different voice signals. This is interesting for crowded events where a lot of subscribers need to be served by a relatively small number of BTS.

One of the most important tasks of the TRAU apart from compressing, decompressing and correcting transmission errors, is ciphering the voice data. As in most cases when handling continuous data a stream cyphering algorithm is used. The stream cypher key K_c that is generated by the authentication centre. It is generated by the A8 algorithm on the SIM card with a random number (RAND) and the secret key Ki as input. Since the transmission of voice data is split into frames it suffices to encode the data on a per frame basis. Kc and the current frame number are the inputs for the algorithm A5 which generates a 114 bit cyphering sequence that can be XORed with the frame. This sequence changes every frame since it uses the current frame number as input. The complete procedure is outlined in Figure 2.7.

Since some strong cyphering algorithms are not permitted in certain countries, there is a variety of algorithms called A5/1, A5/2,. . . A5/n from which one needs to be chosen upon connecting to the network. However the encryption in only optional and not mandatory. If the network does not offer encryption, the ME sends its data unencrypted, without giving notice to the user in most cases. The other weakness is the locality of encryption. The procedure only affects the transmission from the ME to the BTS, everything after that is unencrypted voice data. This is especially a problem when providers use point-to-point radio systems to connect their base stations to the MSC.

2.3 The U_m Interface

As with all radio based networks, the efficiency of the interface between the MS and the BTS is of utmost importance to the overall performance of the network. The main reason for that is that resources on the air interface are scarce. Efficiency in this case can be seen as maximizing the quotient of transmission rate over bandwidth used [12].

The first section will explain how transmission in a GSM network are handled on the physical level and what techniques are used to maximize throughput. Afterwards the notion of logical channels, virtual channels that are mapped on top of the actual transmission, will be discussed and which channels are of importance for this project. The last section compares the network layers of the GSM stack to ISO/OSI layer model, to give a basis for understanding where the framework employed in the practical part is situated in that hierarchy.

2.3.1 Radio Transmission

Without additional techniques, the BTS would only be able to serve a single caller at a time. Therefore even in older radio networks like the C-Netz in Germany used Frequency Division Multiple Access (FDMA). With FDMA a specific frequency of the broad frequency band of the BTS is allocated to a specific subscriber for a call, leaving other frequencies open to use for other subscribers connected to the same base station. Essentially this means that every BTS can serve multiple frequencies at the same time. This comes at the cost of additional hardware, since all the frequencies need their own transceivers and need to be amplified accordingly to guarantee the transmission quality. Additional hardware for each channel is also required to enable duplex transmission, meaning that sending and receiving can be done at the same time.

That number of available frequencies would not suffice to meet the demand, more communication channels were needed. To that end another technique has been introduced, called Time Division Multiple Access (TDMA). In GSM networks each of these subbands yielded by the FDMA procedure has a width of 200 kHz. Onto this smaller carrier frequency, TDMA frames are transmitted, that contain eight time slots. These frames have a transmission length of 4.615 ms. Each of these timeslots could host the data of a different subscriber, although the first one is usually used for signalling procedures. An illustration of how these multiplexing methods work together can be seen in Figure 2.8.

Frame Numbering

Another important aspect is the frame hierarchy and the resulting frame numbering since it is used for ciphering as well as channel mapping and synchronisation. The frame number is broadcasted frequently on the Signalling Channel (SCH) to keep mobile subscribers in sync and inform subscribers that are about to connect or request a channel for com-

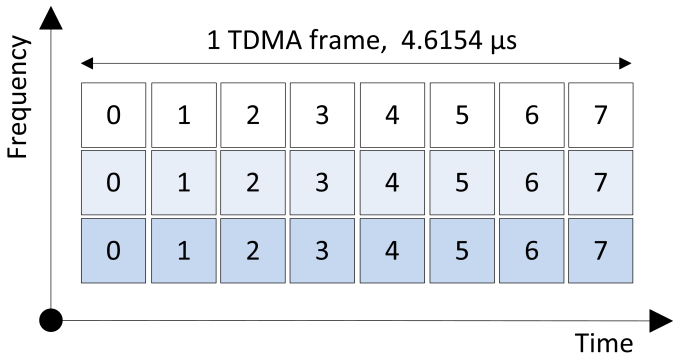


Figure 2.8: The combination of FDMA and TDMA.

munication. Figure 2.9 shows complete diagram of the numbering scheme and frame hierarchy for reference.

The timeslots on the lowest level of the hierarchy have a length of 4.615 ms $\div$ 8 = 577 μs are also known as Bursts numbered from 0 to 7. Every new TDMA frame the sequence number is increased by one. Since this number cannot be increased endlessly is repeated every 3 h 28 m 53 s and 760 ms. This is the largest chunk in the frame hierarchy and is called Hyperframe. Superframes and Multiframes are layers in between the Hyperframe and the TDMA frame. As can be seen in the diagram the two variants of Multiframes, the 26-Multiframe containing 26 TDMA frames transports traffic channels and the respective control channels and the 51-Multiframe containing 51 TDMA frames respectively which contains only signalling data. Superframes wrap these different kinds of Multiframes into packages of the same size. So either 51 26-Multiframes can be carried by a Superframe or 51 26-Multiframes yielding a duration of 6 s and 120 ms each. Finally 2048 Superframes make up the Hyperframe.

The frequency number thus is only repeated every 3 hours which makes cracking the cyphering algorithm that has the sequence number as one of its inputs and thus intercepting a call considerably more difficult. When a MS and BTS start to communicate the frame number has to be obtained by the MS from the SCH before it can ask for a channel. This is important since the frame number is a vital information indicating the chronological order of control channels. If the MS asks for a channel assignment in frame n and a channel is assigned to the MS, the assigned channels refers back to the frame n and thus the MS can find its channel amongst the others.

The last task mentioned above was synchronisation. Since the mobile station and the transceiver station cannot send at exactly the same time, uplink and downlink of a channel are shifted by three timeslots. The time in between uplink and downlink however cannot be fixed for all situations like that. During a call a participant may move around and since radio waves travel at the speed of light slight variations in timing need to be dealt with.

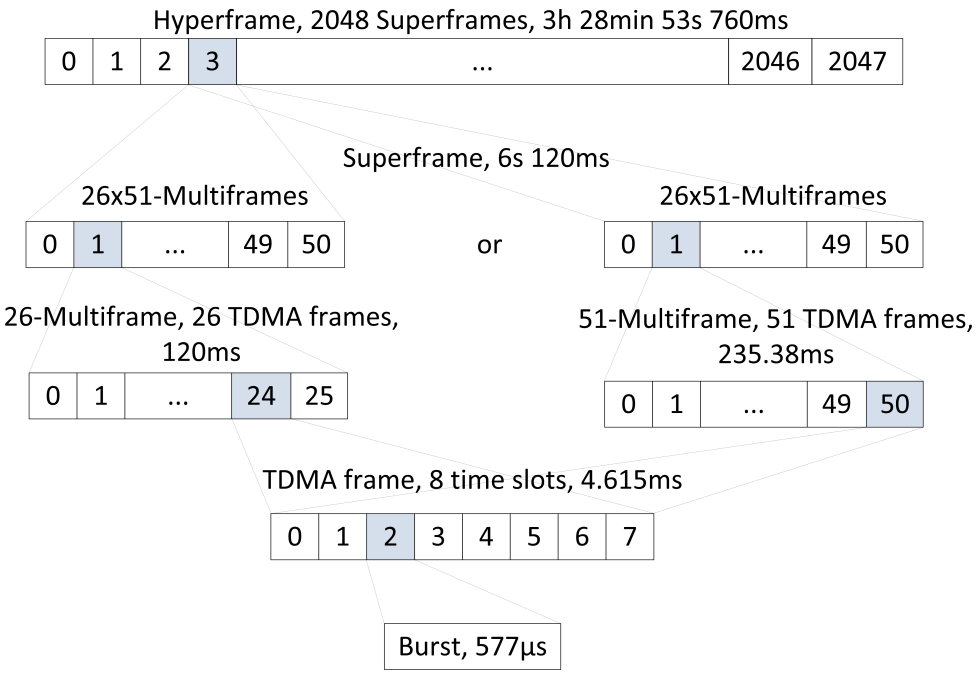


Figure 2.9: Hierarchical Composition of the different frames.

Nomal Burst	3	57 Data	1	26 Training	1	57 Data	3	8.25
Frequency Correction Burst	3	142 Fixed					3	8.25
Synchronization Burst	3	39 Data	64 Training			39 Data	3	8.25
Dummy Burst	3	Empty	26 Training			Empty	3	8.25
Access Burst	8	41 Training			36 Data	3	68.25	

Figure 2.10: Structural Comparison of different Burst types. After [8].

If not data from two participants might overlap and be rendered unusable. To avoid this problem each Burst has a Guard Time at the beginning and at the end, where no data is transmitted. The complete structure of such a Normal Burst is outlined in Figure 2.10. However this does not suffice if a subscriber moves away or to a BTS at considerable speed. Therefore a mechanism called Timing Advance is used. Basically the farther a subscriber is away from a base station the earlier a burst has to be sent, to compensate for the distance. The value for the Timing Advance is determined by the BSC after receiving a channel request message from the mobile station and afterwards constantly updated by the respective BTS. The channel request message itself has only little data and large Guard Times since Timing Advance can only be used after this first measurement.

Burst Types

As can be suspected by the paragraph above, there are different kinds of Bursts which are shown in 2.10 [8]. All Bursts contain the above mentioned Guard Times which separate them from the next Burst. In addition to data bits and known fixed bit sequences every frame has has tail bits, which mark the beginning and the end of a frame. The training sequence is a fixed bit sequence that appears in conjunction with data bit sequences. In a radio transmission procedure the signal can be distorted by shadowing, reflection, an other factors, which would result in data loss. But since the training sequence is known, it is possible to reconstruct the original signal by comparing the incoming training sequence with the expected one and thus conserving the data bits.

- Normal Burst: The basic information transmitting Burst. All information on traffic and control channels is transmitted by this Burst, except for the Random Access Channel (RACH). Furthermore this Burst contains the Stealing Flags (SFs). If these are set, the Burst contains important signalling data that has to travel fast over the FACCH however no normal data can be transmitted in this case.

- Frequency Correction Burst: This Burst is sent frequently and is used by MSs to fine tune to the frequency of the BTS. It may also be used for time synchronisation for TDMA frames by the MS. The periodic broadcasting of this frame is also called

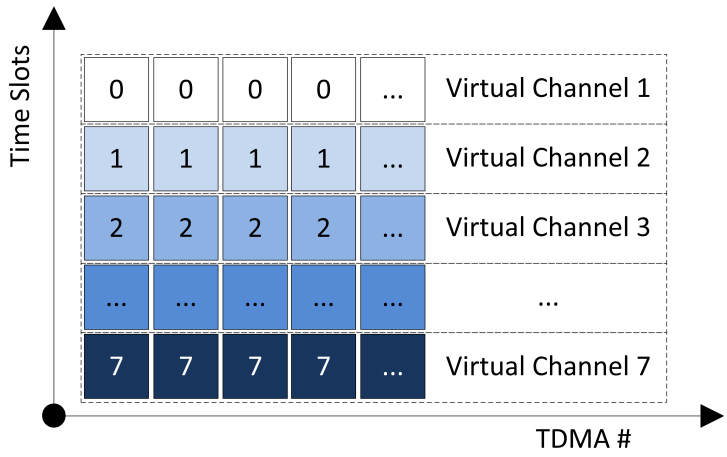


Figure 2.11: Mapping of virtual channels on time slots.

Frequency Correction Channel (FCCH) and shares a frequency with the Broadcast Channel (BCCH) as will be shown in the next section.

- Synchronisation Burst: This Burst contains time synchronisation information from the BTS to the MS as well as the running number of the TDMA frame. Periodic broadcasting of this Burst is called SCH.
- Dummy Burst: When no other Bursts are sent on the BCCH this one is sent to ensure that something is sent every time. This way the MS can keep up doing measurements even if no data needs to be transmitted.
- Access Burst: The Burst that is used to transmit data on the RACH. Since everyone can sent on the RACH without being given a timeslot via Slotted Aloha procedure, the guard times of this Burst are high since this reduces the probability of data colliding.

The information in this section described the physical properties of the Air Interface also called Layer 1 when referring to the standard ISO/OSI model. A short description of the other layers will be presented in Section 2.3.3 for the sake of completeness.

2.3.2 Logical Channels

A logical channel is a virtual construct on top of the physical construct of frames, to group information of the same kind together. Since not all information has to be sent all the time, these different information channels, e.g. broadcast information about the respective base station, can be multiplexed and sent together. The mapping of these channels on the

physical interface works in two dimensions. The first dimension is the frequency and the second the time slot. Figure 2.11 shows this mapping of channels onto time slots over the course of multiple TDMA frames for one fixed frequency. In this way, each timeslot over the course of multiple frames can be regarded as a virtual channel. These resulting virtual channels can now be used by a multitude of logical channels to transmit information.

There are two main categories of logical channels distinguished by their usage [15], dedicated channels and common channels. Dedicated channels transport data meant for a single subscriber whereas common channels contain information interesting to all subscribers.

Dedicated Channels

As mentioned above, these channels wrap the communication of a single user with the network. These are point to point channels.

- TCH: A data channels that is used to transmit voice data or data service packages.
- FACCH: A channel for transmission of urgent signalling data, e.g. handover signalling. Since this data doesn't have to be send often, it shares a timeslot with the TCH and uses the stealing flags to insert its own data.
- SACCH: The uplink of this channel is used by the MS to transmit quality measurements of the cell and neighbouring cells to the base station, so the network can do handover decisions accordingly. The downlink is used for Timing Advance data and power management data for the MS.
- SDCCH: On this channel signalling information is sent to a subscriber as long as no TCH has been assigned during the initialisation of a call. Text messages and Location Updates are also transmitted on this channel.

Common Channels

The common channels contain data interesting to all subscribers, thus having a broadcast nature. These are point to multi-point channels.

- SCH: When the MS is looking for a cell to connect, this channel is used.
- FCCH: Used by MSs to fine tune to the frequency of a certain base station and denotes the start of a 51-Multiframe.
- BCCH: This channel is used to transmit information about the network and the base station itself through different system information messages. These contain, the netowrk name and cell identification as well as neighbourhood information on cells in the area and much more. This channel will be the main source of information for

this project, since it allows harvesting information without actively participating in the network and will thus be discussed in further detail in Section **??**.

- PCH: If a subscriber is not assigned a dedicated channel yet, i.e. he/she is not active, they are notified on this channel if there is an incoming call or text. The subscribers are identified by their TMSI which has been previously assigned upon entering the network, so the IMSI does not have to be broadcasted.
- RACH: A subscriber that has been notified over the PCH can contact the network and request a SDCCH. Since this is a channel used by all connected and idle MSs, access has to be regulated. As the name implies access is random thus it can happen that two or more MS try to send at the same time. Slotted Aloha is used to handle access, meaning there are fixed timeslots on which MSs can send data. If collisions occur, the data is discarded and each MS has to wait a random time interval before sending again.
- AGCH: This is the channel used to respond to a MS if a request has been made on the RACH. The acknowledgement message also contains information on which SDCCH to use.

Combinations

These channels cannot arbitrarily mapped onto timeslots. There is a complex multiplexing scheme defined in GSM 05.02 [**?**] that explains which channel combinations can be broadcasted inside a Multiframe. Since we are mainly interested in the downlink to harvest information from the BCCH Table **??** shows the possible combinations of logical channels inside a Multiframe. The mapping of these specific Multiframe-configurations onto timeslots is not arbitrary either. Normally TS-0 and TS-1, the first two time slots are used handle channels with signalling information. The BCCH also uses TS-0 of the carrier frequency.

Figure 2.12 shows an example [15] for the downlink of a base station where these channel configurations can be seen. As mentioned before, TS-0 and TS-1 are used for signalling purpose where the Multiframe-configurations M5 and M7 can be found respectively. The slots for the BCCH can be seen here. The table shows, that these configurations do not contain any traffic channels. As for traffic channels, TS-2 through to TS-7 are used with the configuration M1 or M3. It cannot be seen from the data, whether full rate or half rate channels are used for transporting voice data, but since half rate channels are not used very often [12], it is more likely hat it resembles M1.

2.3.3 Layers

Design-wise the layers of the U_m interface resemble the layers of the ISO/OSI model reference model specified by the ITU. This section will give a short overview over the first

FN	TS-0	TS-1
0	FCCH	SDCCH/0
1	SCH	SDCCH/0
2	BCCH	SDCCH/0
3	BCCH	SDCCH/0
4	BCCH	SDCCH/1
5	BCCH	SDCCH/1
6	AGCH/PCH	SDCCH/1
7	AGCH/PCH	SDCCH/1
8	AGCH/PCH	SDCCH/2
9	AGCH/PCH	SDCCH/2
10	FCCH	SDCCH/2
11	SCH	SDCCH/2
12	AGCH/PCH	SDCCH/3
13	AGCH/PCH	SDCCH/3
14	AGCH/PCH	SDCCH/3
15	AGCH/PCH	SDCCH/3
16	AGCH/PCH	SDCCH/4
17	AGCH/PCH	SDCCH/4
18	AGCH/PCH	SDCCH/4
19	AGCH/PCH	SDCCH/4
20	FCCH	SDCCH/5
21	SCH	SDCCH/5
22	SDCCH/0	SDCCH/5
23	SDCCH/0	SDCCH/5
24	SDCCH/0	SDCCH/6
25	SDCCH/0	SDCCH/6
26	SDCCH/1	SDCCH/6
27	SDCCH/1	SDCCH/6
28	SDCCH/1	SDCCH/7
29	SDCCH/1	SDCCH/7

FN	TS-2	…	TS-7
0	TCH		TCH
1	TCH		TCH
2	TCH		TCH
3	TCH		TCH
4	TCH		TCH
5	TCH		TCH
6	TCH		TCH
7	TCH		TCH
8	TCH		TCH
9	TCH		TCH
10	TCH		TCH
11	TCH		TCH
12	SACCH		SACCH
13	TCH		TCH
14	TCH		TCH
15	TCH		TCH
16	TCH		TCH
17	TCH		TCH
18	TCH		TCH
19	TCH		TCH
20	TCH		TCH
21	TCH		TCH
22	TCH		TCH
23	TCH		TCH
24	TCH		TCH
25	free		free
0	TCH		TCH
1	TCH		TCH
2	TCH		TCH
3	TCH		TCH

Figure 2.12: Snippet of a Multiframe-configurations for a base station from [15].

	M1	M2	M3	M4	M5	M6	M7	M8	M9
TCH/F									
TCH/H									
TCH/H									
BCCH									
FCCH									
SCH									
CCCH									
SDCCH									
SACCH									
FACCH									
Multiframe Type	26	26	26	51	51	51	51	26	26

Table 2.5: Possible combinations of logical channels for the base station. From [8].

three layers with respect to the air interface [12]. It is important for further understanding to know what functionality can be found on which of the three lower layers, since the framework employed to gather information in this project will directly work on and with those layers.

Physical Layer (Layer 1): This layer provides the facilities for the actual transmission of data. In case of the U_m interface this is the actual radio equipment. This layer does not know data types like user or signalling data. The data that it receives from Layer 2 are either single bits or an array of bits. On the protocol side of the U_m interface the Gaussian Minimum Shift Keying (GMSK) modulation that is used to encode the data of a Burst into radio signals is part of Layer 1.

Data Link (Layer 2): On Layer 2 packaging is done. The notion of data frames is introduced to have chunks of information on which error checking can be performed and potential retransmission of corrupted data. The Layer 2 protocol High Level Data Link Control (HDLC) is used as a basis for SS-7 as well as for Link Access Procedure, D Channel (LAPD). HDLC and its derivatives use start/stop markers and checksums to form data frames. The Layer 2 format changes through the course of the network, while the data packages of layer 3 stay the same. When a transmission from a MS to the BTS is done,LAPD Mobile (LAPD$_m$) is used which is essentially the same as the Layer 2 ISDN protocol with a few simplifications. From the BTS to the BSC LAPD$_m$ converts to LAPD and afterwards is exchanged to Message Transfer Part 2/SS7 (MTP 2/SS7). For the air interface LAPD$_m$ along with channel coding and Burst formatting form Layer 2. More information about these Layer 2 protocols can be found in the respective Technical

Specifications of the 3GPP [**?**, **?**].

Network (Layer 3): Layer 3 headers have to provide all the information necessary for the packet to be routed towards its recipient. As with Layer 2 information, it may be the case that this header needs to be partially rewritten during the transmission of a package. Between the MS, BTS, BSC and MSC the Radio Resource (RR) protocol and the information needed to route a call into the SS-7 subsystem are part of Layer 3. This protocol handles configuration and allocation of radio channels as well as managing the dedicated channels to the subscribers. Therefore in a strict sense MM and CC information does not belong to Layer 3 functionality but is only transported via RR between MS and the NSS [12].

2.4 IMSI-Catcher

An IMSI-Catcher is a technical device that is used to capture IMSI and IMEI numbers of mobile subscribers. The knowledge of the IMSI and IMEI numbers can be exploited to either tap into calls the particular participant is doing or pinpoint the location of the subscriber [**?**].

This topic came up in conjunction with crime fighting and prevention with the advent of mobile telephones. A mobile phone cannot be tapped in the same way as a landline phone since the subscriber can change places and also phones. This has proven to be a challenge to the authorities.

In 1996 Rohde & Schwarz a company based in Munich, Germany has developed a device called ”GA 090” which was the first IMSI-Catcher. Its was capable of yielding a list with all the IMSI number is the perimeter as well as pinpointing the location of a subscriber given the IMSI. Short thereafter the ”GA 900” was presented which had the additional capabilities of tapping into calls that originated from a particular IMSI. These commercial versions of catchers produced by Rohde & Schwarz are priced between 200 000 € and 300 000 € [**?**]. Although these catchers are meant to be bought by authorities, it is also possible to buy them as a private customer or to order them from abroad. Regulations prohibit the use of IMSI-Catchers for individuals since the frequency bands the GSM network uses are reserved for providers. However, it cannot be guaranteed that such a catcher is not used illegally. In addition to these commercial products different projects [**?**, **?**] have shown that such a device can be built at a very low budget. This only intensifies risk that is imposed by the abusive usage of such an instrument. Figure 2.13 shows a commercial model side by side with a self built catcher [1].

[1] `http://www.iwi.uni-hannover.de/lv/ucc\_ws04\_05/riemer/literatur/imsi-catcher.htm`
`http://www.heise.de/security/meldung/IMSI-Catcher-fuer-1500-Euro-im-Eigenbau-1048919.html?view=zoom\%3Bzoom=`

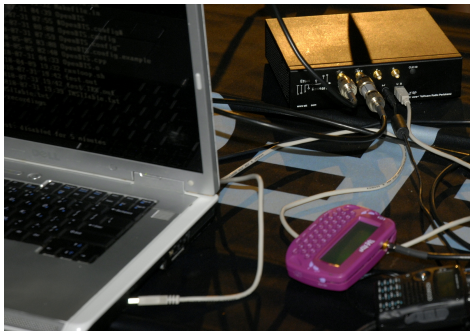


Figure 2.13: A commercial catcher by Rhode & Schwarz and a self built catcher introduced at Defcon 2010.

Section 2.4.1 will show how an IMSI-Catcher works and how subscribers can be caught. In addition the potency of these attacks will be evaluated and what risks these impose from a technical perspective. The next section will explain when a catcher can be used in Germany from a legal perspective and show that this handling imposes a privacy risk on citizens.

2.4.1 Mode of Operation

2.4.2 Law Situation in Germany

1

3 IMSI Catcher Detection

3.1 Procedure

3.1.1 Information Gathering

3.1.2 Information Evaluation

3.1.3 Problems

Solutions

3.2 Frameworks and Hardware

3.2.1 OsmoconBB

3.2.2 Motorola C123

3.3 Implementation

3.4 IMSI Catcher Detection System

3.4.1 Configuration

3.4.2 Operation

4 Evaluation

4.1 Open Field Statistics

4.1.1 Bayesian Filter

4.1.2 Detection System

4.2 Example Scenarios

5 Conclusion

5.1 Future Work

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.

List of Figures

2.1 Growth of mobile GSM subscriptions. Compiled from [8, 10, 9] 4
2.2 The main components of a GSM network. The TRAU can be either build in to the BTS or BSC, here the BSC was chosen. 6
2.3 Authentication procedure. 13
2.4 Mapping of functional entities on the 900Mhz band. 15
2.5 Theoretical arrangement of radio cells compared to a realistic alignment. Cells with the same number share the same frequency [8]. 17
2.6 Common base station configurations. Compiled from [12]. 18
2.7 Cyphering procedure for one frame of voice data. Adopted from [15]. . . 21
2.8 The combination of FDMA and TDMA. 23
2.9 Hierarchical Composition of the different frames. 24
2.10 Structural Comparison of different Burst types. After [8]. 25
2.11 Mapping of virtual channels on time slots. 26
2.12 Snippet of a Multiframe-configurations for a base station from [15]. . . . 29
2.13 A commercial catcher by Rhode & Schwarz and a self built catcher introduced at Defcon 2010. 32

List of Tables

2.1 Subset of data stored on a SIM card. Adopted from [12] 8
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. 9
2.3 Interfaces inside the core network (upper part) and the radio network (lower part) 11
2.4 Frequencies in the different bands [15]. 17
2.5 Possible combinations of logical channels for the base station. From [8]. . 30

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