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
Konrad Meier

May 7, 2012

Abstract:

asjdajslkdajdalsdj

Contents

Chapter 1.

Introduction

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 [10, 14, 13] 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.

1.2. Disclaimer

Chapter 2.

GSM

This chapter will give a short overview of some important aspects of GSM networks and protocols. The first section presents 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 essential protocol basics will be explained, important 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 main source for gathering information from IMSI-catchers. Section 2.4 will finally explain how an IMSI-catcher works and how it replaces the system components 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 from *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 900 MHz band. 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 and Northern Telecomunication (NMT) in Scandinavia.

In February 1987 the committee submitted the basic parameters of GSM. Not after 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 foundation for allowing international operation of mobile stations using the standard interfaces agreed upon earlier that year. CEPT itself was around since 1959 and its members 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*. The very same year the specifications for Digital Cellular System 1800 (DCS1800) were submitted. These were essentially the same specifications translated to

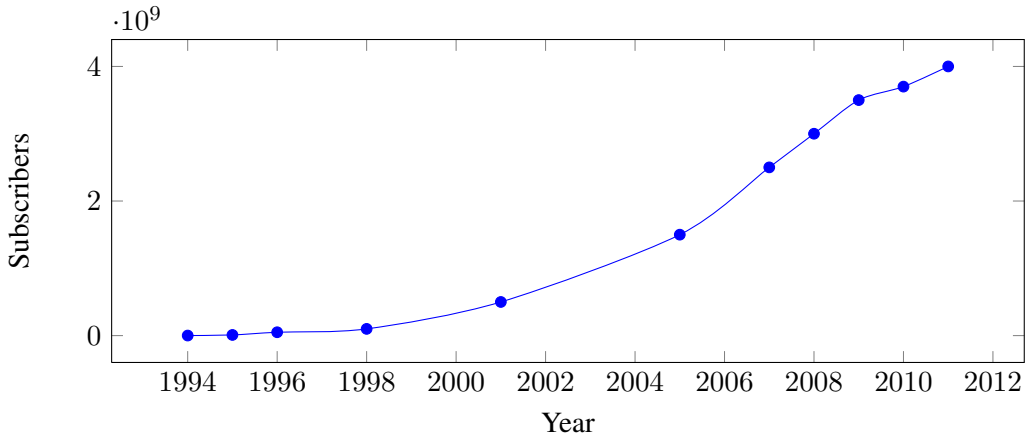


Figure 2.1.: Growth of mobile GSM subscriptions. Compiled from [10, 14, 13]

the 1800 MHz band and the foundation for the USA's 1900 MHz band. Under 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 early as 1993 they already counted more than one million subscribers [10]. Also many networks on different frequency bands (900 MHz , 1800 MHz , 1900 MHz) 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 [17] as:

- Liberalisation 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 five organisational partners with the goal of standardisation of mobile communications with focus on developing specifications for a third generation mobile radio system. These partners were the Association of Radio Industries and Businesses (ARIB), the ETSI, the Alliance for Telecommunications Industry Solutions (ATIS), the Telecommunications Technology Association (TTA) and the Telecommunications Technology Committee (TTC). The

focus was later expanded in the light of the *International Mobile Communications-2000*-project [9] by 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 [18] is a protocol that enables mobile users to download data with speeds up to 84 MBit/s since release 9. High Speed Uplink Packet Access (HSUPA) [19] is a related protocol in the High Speed Packet Access (HSPA) family that provides similar 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 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 by Sauter [23] will be used. It describes the main parts as:

- **Basestation Subsystem (BSS):** this part is also called radio network and contains all the technology necessary for connecting mobile subscribers to the telephone 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 discussed 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

[1] 3GPP - Specification Groups,`http://www.3gpp.org/` [Online; Accessed 04.2012]

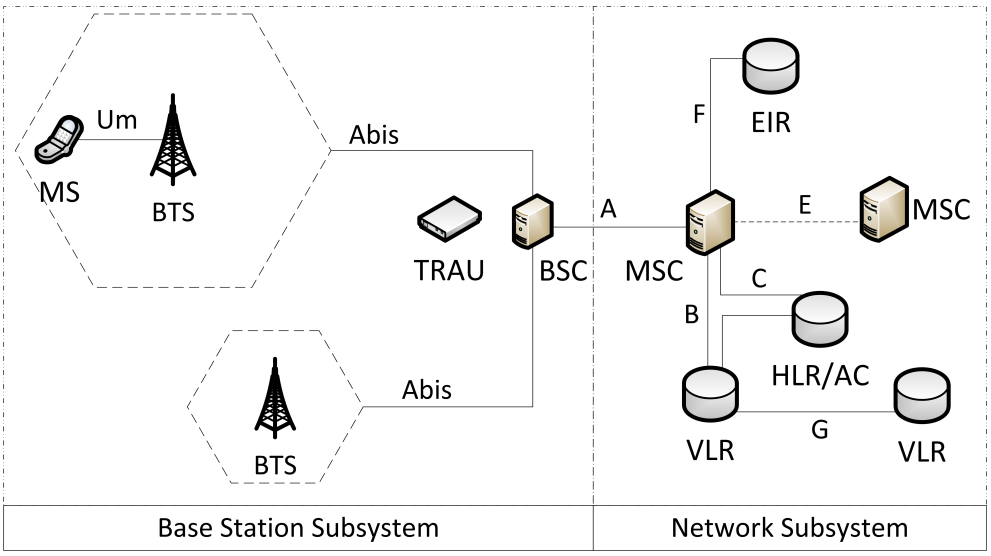


Figure 2.2.: The main components of a GSM network.

networks or the Public Standard Telephone Network (PSTN). The databases that contain subscriber information and location information for connected users are located here.

- **Intelligent Network Subsystem (IN):** this part of the network augments the core network with value-added service (VAS) [26]. In order to provide extra functionality the IN consists of several Service Control Point (SCP) databases. Some of the most widely 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) [10] or limit the BSS entity to the provider part and define an additional entity for the MS [16, 24]. 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 ever smaller mobile phones with ever more functionality year by year to a point where not the technology itself was the constraining factor for size but the user interface, e.g. button and display sizes. This trend changed however with the upcoming of so called smart-phones. With weight being the driving factor and not size resolution and display sizes started to increase again but the devices

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

became ever thinner. 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 [4] summarizes the mandatory and optional features of a MS. Some of the most important mandatory features are [17]:

- Dual Tone Multi Frequency (DTMF) signalling capability.
- Short Message Service (SMS) capability.
- The ciphering algorithms A5/1 and A5/2 need to be implemented.
- Display capability for short messages and dialled numbers, as well as available Public Land Mobile Network (PLMN)s.
- A cyphering indicator that shows the user whether encryption is activated on the current connection or not.
- 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 rather is part of the software or firmware. Tools like *ZiPhone*[1] for iOS devices[2], especially iPhone, can change this supposedly unchangeable identifier.

A way to categorize different MEs is by supported frequency band and power class rating according to GSM 05.05 [3]. Most mobile phones and smart-phones 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 are different for each of the frequency bands, since output needed in higher frequency bands (1800/1900 MHz) is less compared to the 900 MHz band or the north American 850 MHz 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, three 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

[1] Unlock iPhone 4, Jailbreak iPhone, `http://www.ziphone.org/` [Online; Accessed 04.2012]
[2] Apple iOS5, `http://www.apple.com/ios/` [Online; Accessed 04.2012]

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 via A8
PIN	Secret numeric password to use the 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 [17]

car installed ME. The plug-in format is also called ID-000 and can be found in ISO/IEC 7810 [5].

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 and Kc 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 Sauter's book [23].

The IMSI as described in GSM 23.003 [8] 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

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.

only the last part is the personal identification number of the subscriber.

13091283012938

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 PLMN. 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 [27]. 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 Network Subsystem 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). These 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 is 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 PLMN 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 providers' 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 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 which 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 connections 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 initiate 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 avail-

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)

able freely or are 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 2.2 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 they 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 one-time IMSI called Temporary IMSI (TMSI) and information in which LA the MS was registered last is transmitted. 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 access the network. 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 two providers Vodafone and E-Plus support blacklisting of IMEIs [30]. Different companies like Airwide Solutions (now acquired by Mavenir)[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[2] outlined in Figure 2.3. The steps of the procedure can be summarized as follows:

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

[2] A procedure where one party poses a question, a so called challenge and the party to be authenticated has to provide a valid answer.

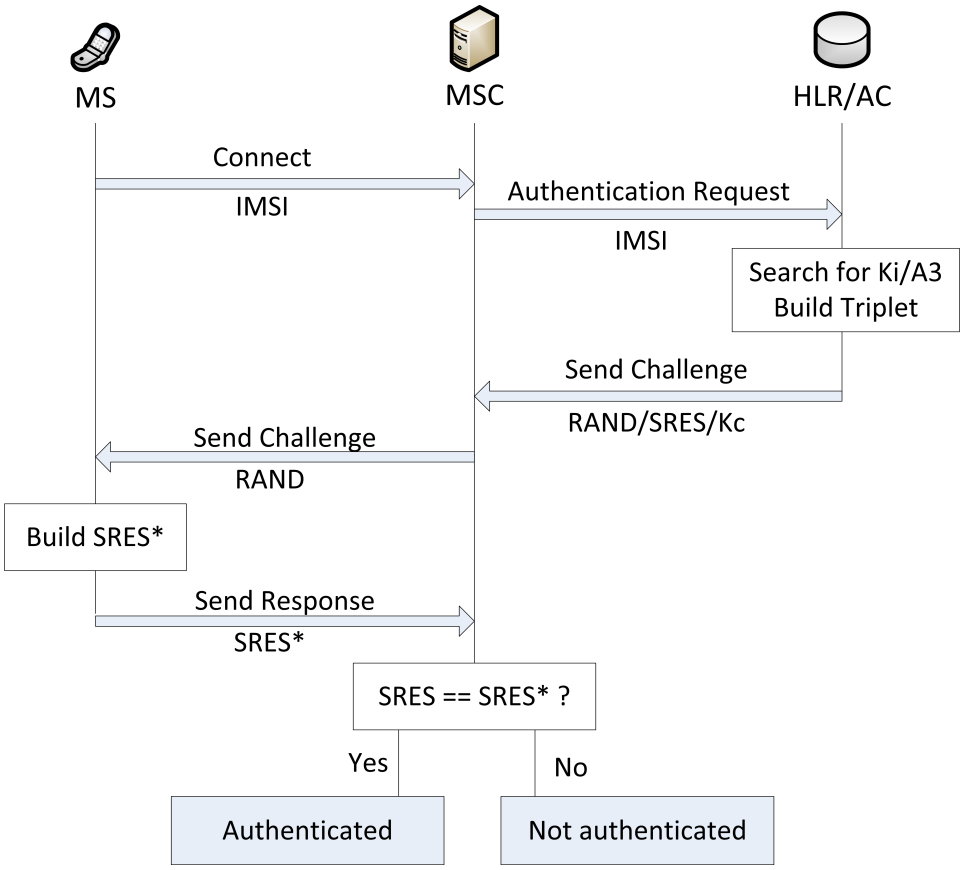


Figure 2.3.: Authentication procedure.

1. User connects to the network or triggers an event that needs authentication at the MSC. There are two possible scenarios from here on.

   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 built 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 using the algorithm A8.

   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 Kc 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* match, 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 [23].

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 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 features that were not interoperable. To standardise these services the 3GPP and the ETSI defined the Customized Applications for Mobile network Enhanced Logic (CAMEL) protocol in TS 23.078 [7]. 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 provider's network. Its main components are the Base Station Controller (BSC), the Base Station Transceiver (BTS) and the Transcoding Rate and Adaption Unit (TRAU). Connecting a mobile subscriber works via radio which is why this subsystem is sometimes also called the radio network [23]. Inside the radio network of a certain area there is one BSC that connects to multiple BTSs and one more TRAUs depending on whether the TRAU is attached to the BSC or to all the BTSs. 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 of 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 900 MHz band each of these has a width of 25 MHz . These bands themselves are furthermore divided into channels, each spanning 200 kHz, which accounts for 125 channels on 25 MHz .

Each of which is identified by its Absolute Radio Frequency Number (ARFCN). This

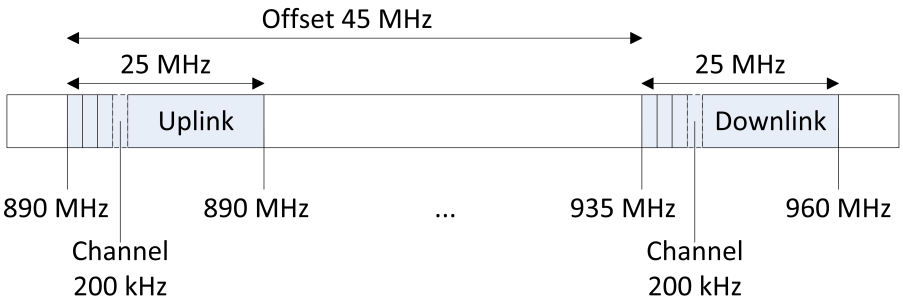


Figure 2.4.: Mapping of functional entities on the 900 MHz band.

Band	ARFCN	Uplink (MHz)	Downlink (MHz)	Offset (MHz)
GSM 900 (Primary)	0-124	890-915	935-960	45
GSM 900 (Extended)	0-124 975-1023	880-915	925-960	45
GSM 1800	512-885	1710-1785	1805-1880	95
GSM 1900 (North America)	512-810	1850-1910	1930-1990	80
GSM 850 (North America)	128-251	824-849	869-894	45

Table 2.4.: Frequencies in the different bands [23].

is a simple numbering scheme, given to those 200 kHz 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 900 MHz Band this would be:

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

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

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

For other bands the numbers differ and can be seen in Table 2.4 along with their respective ARFCN numbers but the functionality is the same.

An additional method called time multiplexing which will be explained in further detail in Section 2.3, makes is possible to map $125 \cdot 8 = 1000$ channels that could be used for voice transmission over 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 into seven frequencies 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 [10]:

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

This procedure raises the number of effectively usable by a large factor. However certain disadvantages come with this procedure as well [17]. Increasing the amount of

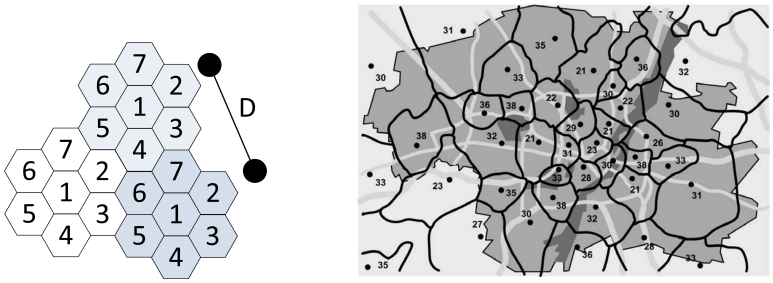


Figure 2.5.: Theoretical arrangement of radio cells compared to a realistic alignment. Cells with the same number share the same frequency [10].

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. These inflict increased signalling load on the network itself.

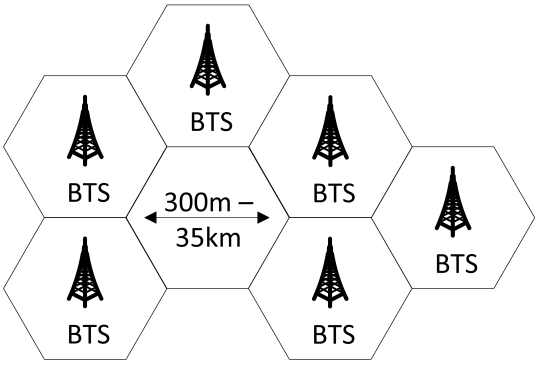
Base Transceiver Station

They are also called base stations and 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. Also this is the theoretical limit for a cell on the 900 MHz band. A 1800 MHz cell has a lower coverage since the signal falloff is greater due to the shorter wavelength. The limiting factor here are the number of subscribers itself. A single station can only serve a limited number of users which yields a radius as low as 100 m for a single BTS in dense urban housing areas [23]. On the countryside where population is less dense the constraining factor can also be transmission power of the ME. Therefore cells with a radius above 15 km are seldom seen.

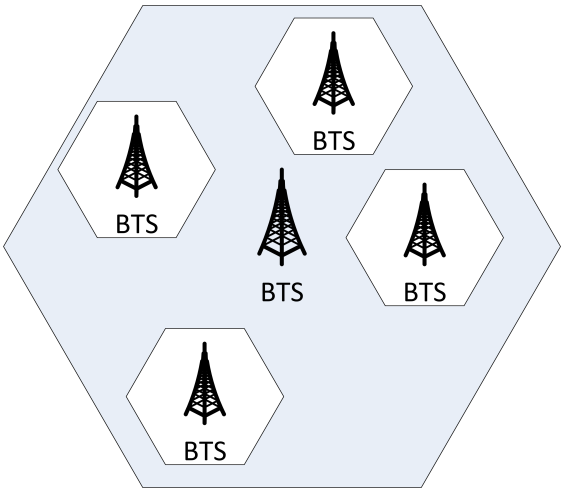
BTSs and their corresponding cells can have different configurations depending on load or morph structure of the surroundings.

In a *standard configuration* every base station has its own Cell Identity (CI), it is a one to one mapping of cells to BTS. This is a cost effective way of providing service to a rural or sparse settled area since only one BTS is used to cover a large area. An comparative illustration of configurations can be found in Figure 2.6.

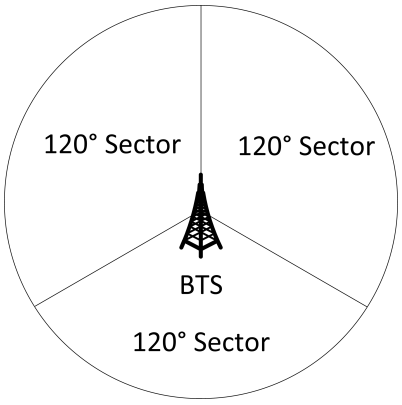
The *umbrella configuration* is build around one central BTS that is on high ground compared to its neighbours and has a higher transmission power. Thus the notion of this particular base station wrapping all the others in the area. Due to interference the frequency used by the wrapping base station 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



(a) Stantard configuration.



(b) Umbrella cell configuration.



(c) Sectorised configuration.

Figure 2.6.: Common base station configurations. Compiled from [17].

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 [17].

The *sectorised 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.

Base 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 of 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 channels as a communication line for a particular purpose like receiving or sending voice data or for sending broadcast information. Due to the nature of a mobile network certain other tasks have to be performed like Handovers and power management [23].

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 Dedicated 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. Whenever 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 by 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 [23]. The 64 kBit/s PCM signal is sent from the MSC to the MS, 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 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 codec is the Half Rate codec which compresses the voice signal to 7 kBit/s thus making it possible to 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

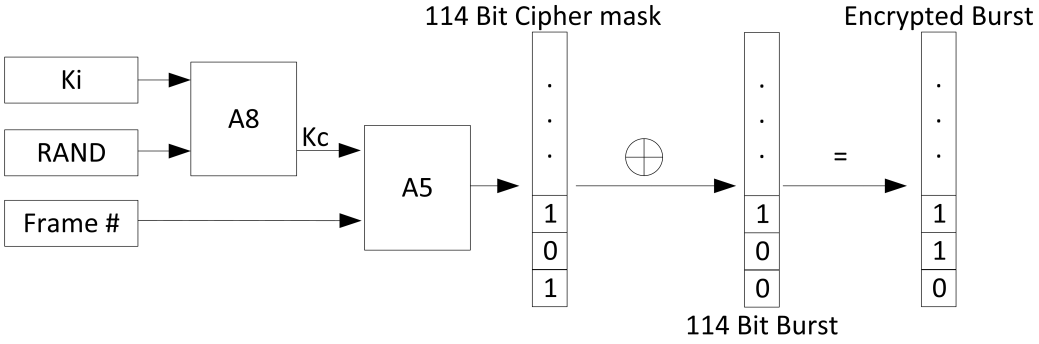


Figure 2.7.: Ciphering procedure for one frame of voice data. Adopted from [23].

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.

Some strong ciphering algorithms are not permitted in certain countries so there is a variety of algorithms called A5/0, A5/1 and A5/2 from which one needs to be chosen upon connecting to the network. However the encryption is only optional and not mandatory, the use of A5/0 indicates that no encryption is used. If the network does not offer such encryption, the ME sends its data unencrypted, without giving notice to the user in most cases. A ciphering indicator is part of most mobile phones, but on most models it is disabled by the operator to not confuse the customers. 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 wireless interface, 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 [17].

The first section will explain how transmission in a GSM network is handled on the physical level and what techniques are used to maximize throughput. Afterwards the

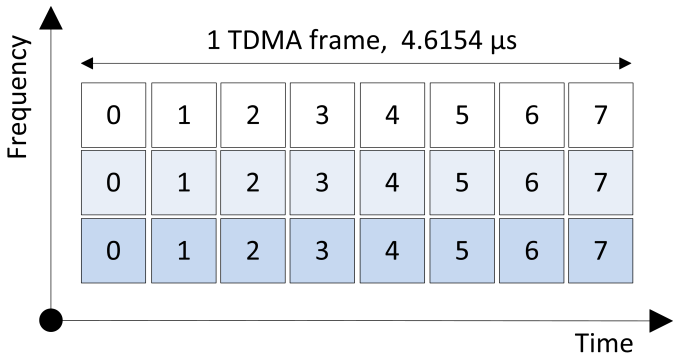


Figure 2.8.: The combination of FDMA and TDMA.

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 the 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 Frequency Division Multiple Access (FDMA) is used. 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 sub-bands 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 two are 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 communication. Figure 2.9 shows a complete diagram of the numbering scheme and frame hierarchy for reference.

The timeslots on the lowest level of the hierarchy have a length of $4.615\,\text{ms} \div 8 = 577\ \mu\text{s}$ and 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 it 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 as well as the respective control channels and the 51-Multiframe with its 51 TDMA frames with signalling data only. 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 one Hyperframe.

The frequency number thus is repeated every 3 hours this way which makes cracking the ciphering 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 through 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. 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

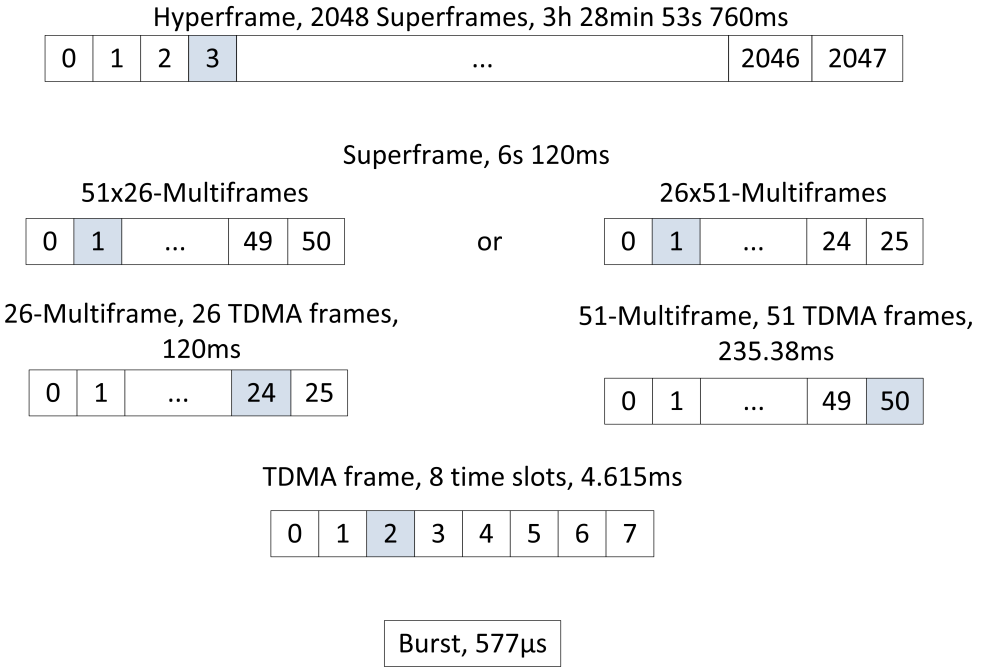


Figure 2.9.: Hierarchical Composition of the different frames.

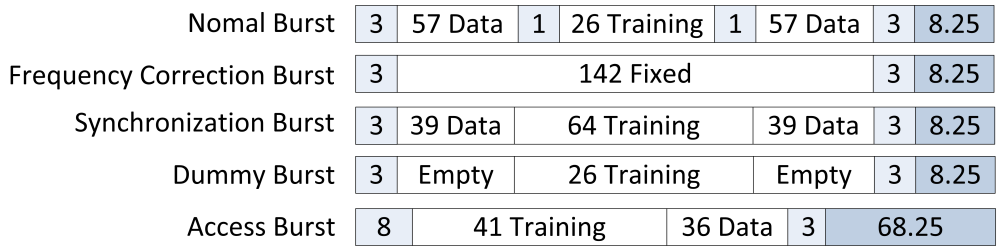


Figure 2.10.: Structural Comparison of different Burst types. After [10].

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 suggested by the paragraph above there are different kinds of Bursts which are shown in 2.10 [10]. All Bursts contain the before mentioned Guard Times which separate them from the next Burst. In addition to data bits and known fixed bit sequences every frame 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. During a radio transmission procedure the signal can be distorted by shadowing, reflection, or other factors which would result in a loss of data. 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 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 by the MS to do time synchronisation for TDMA frames. The periodic broadcasting of this frame is also called 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 TDMA frame number. Periodic broadcastings of this Burst form the SCH.

- Dummy Burst: When no other Bursts are sent on the frequency carrying the BCCH

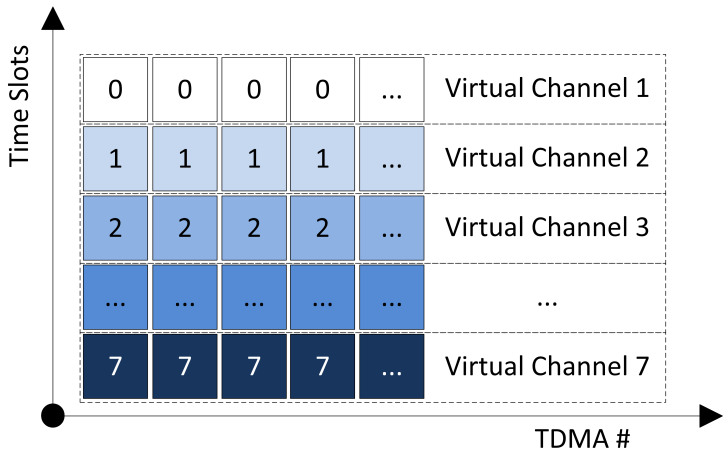


Figure 2.11.: Mapping of virtual channels on time slots.

this one is transmitted to fill the gap. 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 as to reduce the probability of data collisions.

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.

2.3.2. Logical Channels

A logical channel is a virtual construct on top of the physical construct of frames to group similar information 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.

Mapping of these channels on the physical interface works in two dimensions. The first dimension is frequency and the second is 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. 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 [23], 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. 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 synchronisation channel is used.
- FCCH: Used by MSs to fine tune to the frequency of a certain base station and helps to find 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 network 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 Chapter 3.2.1.
- 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.

	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 [10].

- 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 be mapped onto Multiframes. There is a complex multiplexing scheme defined in GSM 05.02 [6] that explains which channel combinations can occur inside a Multiframe. Since we are mainly interested in the downlink to harvest information from the BCCH Table 2.5 shows the possible combinations of logical channels inside a Multiframe on the downlink frequency. 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 for example uses TS-0 of the carrier frequency.

Figure 2.12 shows an example [23] 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 re-

spectively. 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 [17], it is more likely that it resembles M1.

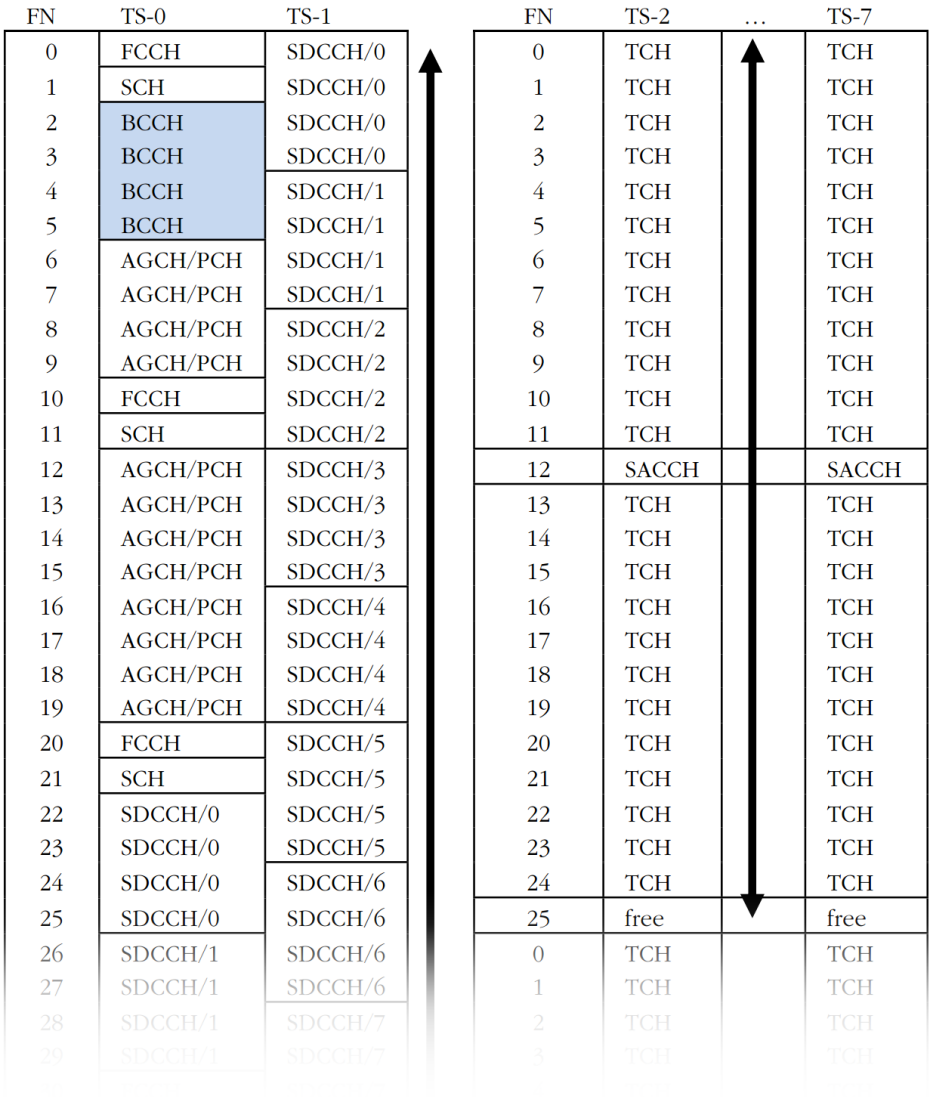
2.3.3. Layers

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 three layers with respect to the air interface [17]. 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 algorithmic 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 and potential retransmission of corrupted data can be performed. 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 may 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 [1, 2].

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



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 [23].

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 [17].

2.4. IMSI-Catcher

An IMSI-Catcher is a technical device that is used to capture the IMSI and IMEI numbers of mobile subscribers. The knowledge of the IMSI and IMEI numbers can be exploited to either tap into the participant's calls or pinpoint the location of the subscriber [12]. Another less known functionality is that if catchers do not relay intercepted calls they can be used to suppress mobile communication in a certain area e.g. during a police operation [31].

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 thus there is no designated line associated with him/her. 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 numbers in 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 capability of tapping into calls that originated from a particular IMSI. These commercial versions of catchers produced by Rohde & Schwarz were priced between 200 000 € and 300 000 € in 2001 [12]. 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 [28, 25] have shown that such devices can be built at a very low budget. This only intensifies the risk that is imposed by the abusive usage of such a catcher. Figure 2.13 shows a commercial model side by side with a self built catcher.

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 under which circumstances a catcher can be used in Germany from a legal perspective and show that this handling poses the risk of privacy breach to citizens.

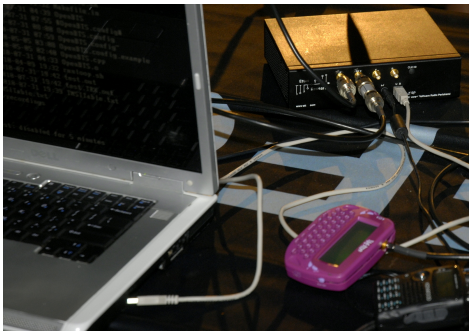


Figure 2.13.: A commercial catcher by Rhode & Schwarz [12] and a self built catcher introduced at Defcon 2010 [25].

2.4.1. Mode of Operation

Basically an IMSI-Catcher masks itself as a base station and lures subscribers in its perimeter to connect to it without their knowledge. The attack shown in Figure 2.14 is broadcasting a new Location Area Identifier (LAI) to the MS at very high power, suggesting that the MS entered a new area and has to re-authenticate [11].

Once a subscriber connects to the device, a command is sent to the MS which asks for the SIM's IMSI. This command is normally only used in case of an error [12] but can be abused this way.

This is only possible since authentication in a GSM network is one-sided as discussed earlier in Section 2.2.2. The subscriber has no way of checking the authenticity of a base station but rather has to trust the broadcasted identifier which can be easily forged by a catcher. At this stage, the subscriber can already be localized as being in a certain distance of the catcher.

Having the IMSI the authorities can now also query the provider for personal information about the subscriber, however criminals may use fake credentials when obtaining a SIM card. Since it is only possible to catch all the IMSIs in an area, the person to be observed has to be followed and the catcher has to be used multiple times. Each time it yields a set of numbers in the area. The IMSI that is part of all the sets is the IMSI of the person under observation. More catchers can now be used to triangulate the position. The next step is also possible because of a design decision made in the GSM protocol. Encryption itself or certain kinds of strong encryption are not allowed in all countries. Therefore it is possible for the base station to request the encryption algorithm A5/0 which means that no encryption will be used for the calls at all. Only a few mobile phones display that encryption has been disabled by the BTS.

At this point the setup for a man-in-the-middle attack [11] on calls is completed. The

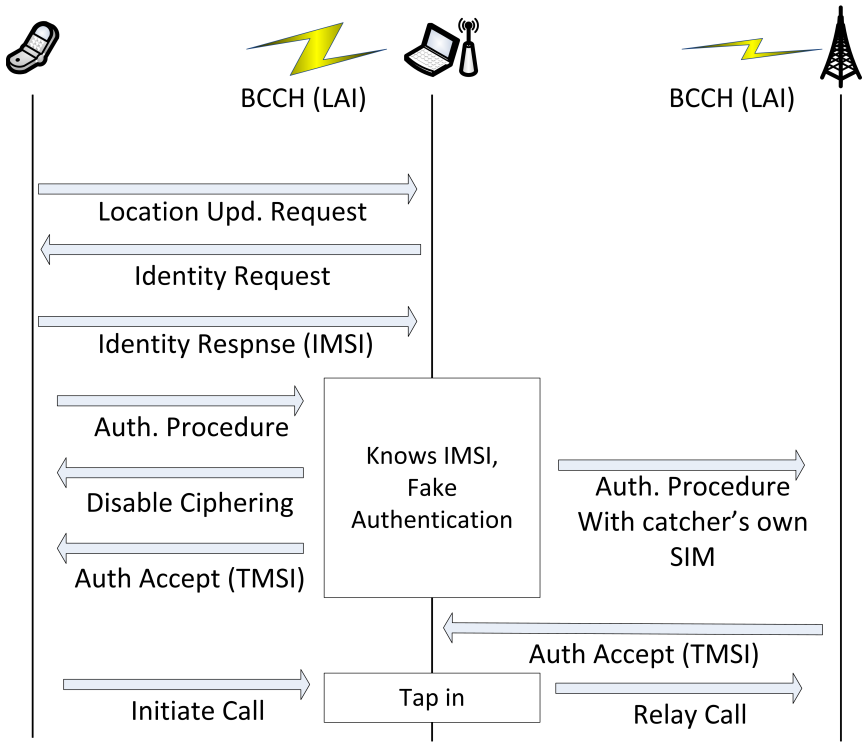


Figure 2.14.: IMSI catching procedure. Adopted and simplified from [11].

catcher itself is connected to the mobile network with its own SIM. If the subscriber now initiates a call, the call can be routed by the catcher into the network and since encryption is turned of it can also be listened to or recorded. The subscriber doesn't notice this privacy breach except in the rare cases where the phone displays that encryption has been turned off. The IMEI is also harvested in a similar fashion if the observed person tries to switch SIM cards on a regular basis [12].

Attacks

When operating a catcher the first and most important step is to actually trick the MS into connecting to the catcher. A lot of phones save the frequency they were tuned to last and upon connecting to the mobile network this is the first frequency they try. Therefore a MS has to be set to 'normal cell selection' mode which means it starts scanning for the best base station available. Three ways of luring a subscriber to the forged cell were presented by Wehrle for the 'Open Source IMSI-catcher' project [28]. The attacks differ on whether the MS already is in normal cell selection mode or not, i.e. it is connected to another BTS.

MS is in normal cell selection mode: The IMSI-catcher has to emulate a cell configuration of the provider the target MS is looking for broadcasting at any frequency. If the MS stumbles upon the frequency it will connect. This is no method with 100% accuracy however chances can be raised by broadcasting with higher power. Some IMSI-catchers even broadcast at a higher power than it would be allowed for normal BTS [31] to make certain to be the strongest base station available to the MS.

MS is already connected to a network: If this is the case then the connection to the current cell needs to be broken. It can be achieved either by jamming the frequency band of the cell the MS is connected to thus forcing the MS into cell selection or by getting the MS to switch the cell to the catcher's. This can be done the following way. In this method the fact is abused that the MS knows its neighbourhood (since it has been broadcasted by the BTS) and does regular quality measurements. The main idea is that the operator of the catcher chooses the frequency of a BTS that is in the neighbourhood of the BTS that the target MS is connected to. This way the operator can make sure the MS know this frequency and has quality measurements associated with it. Furthermore should the chosen BTS, the one that will be replaced by the catcher, have a bad signal to noise ratio (which is why the MS is currently not connected to it). As soon as the catcher starts broadcasting on that frequency, quality measurements will radically improve and the MS will initiate a change of cells to the catcher cell if the quality is above its current cell.

Risks and Irregularities

An IMSI-catcher cannot target an individual subscriber, it always targets an area thus breaching the privacy of uninvolved subjects. Apart from that, a catcher that does not relay calls takes away the possibility for all connected people in the area to initiate calls. Even if the the catcher routes calls into the network, since it only has one SIM card, it can only route a single call. This can be very dangerous because no emergency calls can be submitted in that area during the time of operation which can be as long as five to ten minutes [12].

Another irregularity apart from using no encryption is that people caught in this area cannot be reached on their mobile phones since they are not registered on the main network. As a consequence of the proxy functionality of the IMSI-catcher, when a call is routed into the network the recipient can only see the number the catcher is registered with or 'Number Withheld' however not the original number.

2.4.2. Law Situation in Germany

First reports of an IMSI-catcher used by authorities in Germany dates back to 1997. Until November 2001 35 cases of use were officially confirmed by the Bundesminiterium des Inneren (BMI) [12]. It was used to fight of organised and serious crime like hostage-takings or drug traffic by the Bundeskriminalamt (BKA) and Bundesgrenzschutz (BGS). Attempts have been made by the government to move the catcher out of the legal grey zone and use the 'GA 900' with its capabilities of tapping in to calls for crime prosecution. At that time however the attempt was dismissed.

On 14th of August 2002 with Section §100i of the Strafprozessordnung (Code of Criminal Procedure) a law basis was given to the device. Afterwards on 22nd of August 2006 this section and its accordance with the Grundgesetz (Constitution) was affirmed. The use of an IMSI-Catcher with prior authorisation by a judge does not affect peoples right to privacy nor does it contradict the Datenschutzbestimmungen (Secrecy of Confidential Data) or the Fernmeldegeheimnis (Secrecy of Confidential Communication). In Austria the need for a prior authorisation by a judge was removed in January 2008. During the first four months of 2008, 3800 cases of catcher use were reported in Austria [31].

Gradually, starting with §100i it has become easier for the police and agencies to use electronic surveillance. Although on 2004 it was decided by the Federal Court of Saxony, that electronic surveillance is not to be used in the substantially intimate sphere of private premises, this regulation can be overthrown if linked to the field of serious crimes and terrorism. Section §100a(1) describes that the police merely needs to show certain evidence underpinning a suspicion that a criminal act was committed [22]. This threshold can often be overcome easily, since it is hard for courts to check evidence for sufficiency thoroughly given the short time frame of response. Technically it would even be possible for the authorities to use a catcher without prior authentication by a judge since it is hard

to proof that a catcher was used at a specific point in time. This fact makes is hard to prosecute or even unveil the illegal operation of an IMSI-catcher used by third parties or criminals.

These loose regulations, the hardness of detection together with the fact that third parties can buy or build catchers poses a grave threat to privacy of each individual person.

Chapter 3.

IMSI Catcher Detection

3.1. Framework and Hardware

The following section will give an overview of the OsmocomBB framework and how it works in conjunction with the Motorola C123 mobile phone to enable information harvesting for the IMSI Catcher Detection System (ICDS). OsmocomBB is one of many Open source mobile communications (Osmocom) projects[1]. It implements the software part of a mobile phone. Another project is OpenBSC which implements software for configuring and operating a BSC. OpenBSC was used to realise the Open Source IMSI Catcher [28] and the base station that will be used later to evaluate the performance of the ICDS.

3.1.1. OsmocomBB

OscmocomBB implements the baseband part of GSM as an open source project. Baseband part in this case means that it is an open source software to control the baseband chip inside the mobile phone. The goal is to have, by using compatible hardware, a phone using free software only as opposed proprietary baseband implementations. Therefor the project scope is implementing GSM layer 1-3 as well as hardware drivers for the baseband chipset. A simple user interface on the phone is planned but not yet implemented. At this stage a verbose user interface on the computer is used. This could be beneficial to multiple areas [20]:

- **Security:** The software running on the baseband chips is highly proprietary and closed. The source is often disclosed only to the mobile phone manufacturers using the specific chipset. One cannot be sure that this software does not have bugs that could be exploited and ultimately pose a security risk to the subscriber. History has shown that open source projects are more secure than proprietary solutions since more people can view the source to find issues. If a security threat is found the bug is fixed fast and a patch is released. This could be a great benefit for phone users.

[1] Osmocom, `http://osmocom.org/` [Online; Accessed 04.2012]

- **Education:** Currently knowledge about GSM and its layers on a technical level is not very well spread. An open source implementation as a reference could serve to educate more developers generally interested in the subject of mobile communications and thus improve products and software. Additionally this implementation enables universities to hold practical lab courses and interested individuals to do hands-on experiments.

- **Research:** A free implementation can decouple research on GSM technologies from the industry since key technologies are no longer only available to researchers employed by a specific company. Additionally this way security holes can be uncovered more easily. Modifications to the protocol stack can be deployed and tested in a real environment.

Project Status

At this point layer two and three do not actually run on the phone but rather on a computer to which the phone is connected via a serial cable Layer 1 runs inside the custom firmware on the ME itself, since the procedures involving layer 1 are time critical. This has advantages as well as disadvantages. The disadvantage is that in order to run an application written with OsmocomBB you always have to have a notebook in addition to the phone. The benefit however is that during the development process, the phone does not have to be touched after an initial deployment of the firmware. This means code can be modified, compiled and tested locally without the need of remote debugging. Experimenting is considerably easier this way. This separation however would not work in the original GSM specification, therefore an extra interface layer between layer 1 and 2 had to be implemented to handle messaging between those two. It is called Layer 1 Control, L1CTL.

The current state of the project is, according to a presentation given on the 27th chaos communication congress[1] by Dieter Spaar and Harald Welte, that the network layers 1-3 are fully implemented, SIM cards can be accessed or emulated and GSM cell selection and reselection are working. A3/A8 as well as A5/1 and A/52, Full Rate and Enhanced Full Rate codecs are there, so it is possible to do voice calls with an OsmocomBB application written for that purpose, called `mobile`. It features a terminal/telnet based interface much like Cisco routers however there is no user interface for the phone so far or any implementation for Handovers since neighbourhood measurements were not implemented in the framework at that point. During these calls or during the operation of other programs, it is possible to receive all the frames that are being transmitted via Wireshark from the `osmocon` application.

[1] 27C3 public wiki (Day 3), `http://events.ccc.de/congress/2010/wiki/Welcome` [Online; Accessed 04.2012]

Component	Specification
Band	GSM 900, GSM 1800
Size	$101 \times 45 \times 21$ mm
Weight	86 g
Battery	920mAh Li-Ion battery
Digital Baseband	Texas Instruments Calypso
Analog Basenand	Texas Instruments Iota TWL3025
GSM Transceiver	Texas Instruments Rita TRF6151C

Table 3.1.: Technical specifications for the Motorola C123.

3.1.2. Motorola C123

Since the general idea behind OsmocomBB was to become a vendor independent open source GSM implementation for everyone to use, there were certain requirements the targeted hardware would have to meet. For the consumer side requirements these were having a low price and a good availability. This criterion rules out do-it-yourself (DIY) approaches since the number of produced devices would be low and thus costly or a significant technical knowledge would be expected from all users to assemble the hardware. For the developer side this would also mean implementing a lot on the lower levels of analog logic. Therefore the Motorola C123 was chosen, an old, very cheap phone that is well spread. It has the advantage of being very simple on the hardware side since it is based on the well documented Texas Instruments Calypso Chipset [15]. Table 3.1 shows an overview of the main specifications for the phone. The OsmocomBB framework should work well or with small adjustments for any phone that share the same components. Figure 3.1 an image of the Motorola C123 circuit board with the components mentioned before. Another reason for choosing this hardware platform was that during the start of the OsmocomBB project an open source implementation of GSM layer 1 was already available on Sourceforge (TSM30 Project) that could be used as a reference. At this point the original project has been removed from the Sourceforge site.

In order to use the Motorola C123 in combination with the OsmocomBB framework the custom firmware implementing layer 1 and L1CTL has to be flashed onto the board. This has to be done using a RS332 serial cable that is connected to the 2.5 mm audio jack. The audio jack of the Motorola C123 and other Calypso based mobile phones typically have a 3.3 V serial port on their audio jacks. These cables are normally referred to as T191 unlock cables A variety of stores around the internet sell the cables ready made for about \$10-\$15[1]. One must be careful when using the PC's serial port to communicate with the phone though. Since the phone's serial operates at 3.3 V and is internally connected to

[1] FoneFunShop, `http://www.fonefunshop.co.uk/cable_picker/773_Motorola_T191_W220_W375_OSMOCOM_etc._USB_Unlock_Cable.html` [Online; Accessed 04.2012]

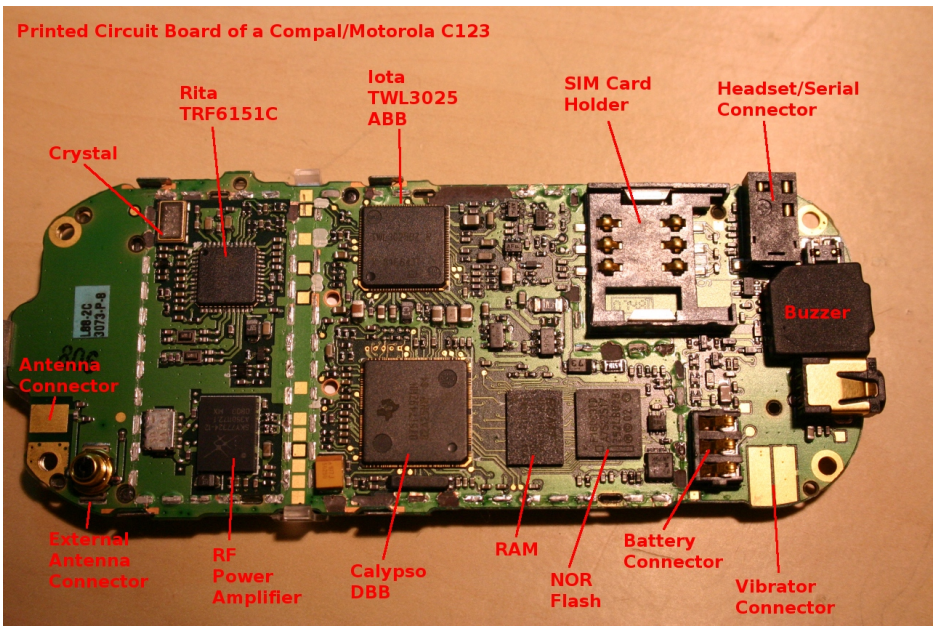


Figure 3.1.: Circuit board of the Motorola C123 with its components [21].

the 2.8 V IO-pins of the baseband processor, directly connecting it to the computers 12 V serial port will destroy the hardware. Therefore it is recommended to use a USB serial cable. Schematics for such an unlock cable, along with a few instructions on how to build one are given in Appendix A.3.

Another issue is virtualisation. The bootloader and the firmware can fail to be deployed correctly if a virtual machine is used as development system. This is because the protocol used by Motorola to do the actual flashing process is *very* time critical and thus timeouts can occur that are caused by the overhead the virtual machine imposes on the hardware/software communication.

OsmocomBB and ICDS

The setup that is used for the ICDS project can be seen in Figure 3.2. It was build and tested in a Xubuntu 11.10 environment [1] which is a more lightweight variant of the popular Debian based Ubuntu Linux distribution. The process of acquiring, compiling and running the OsmocomBB framework itself in this environment is explained in Appendix A.1. As can be seen in the diagram, layer 1 of the OsmocomBB GSM stack runs on the phone. It is connected via a serial cable to the computer running the ICDS. On the computer side the `osmocon` program provides a general interface to the phone. `Osmocon` is

[1] Xubuntu, `http://xubuntu.org/` [Online; Accessed 04.2012]

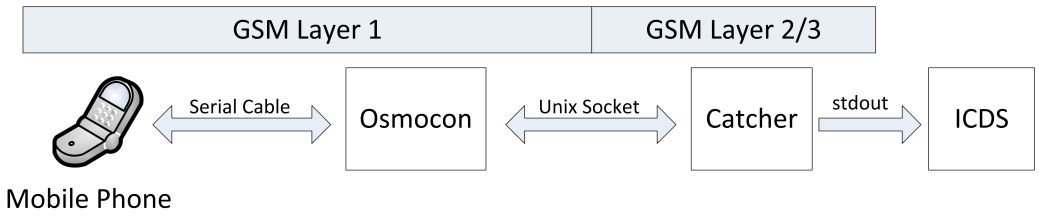


Figure 3.2.: Interaction of the OsmocomBB components with the ICDS software.

also used to download the firmware to the Motorola C123. Other software can communicate with `osmocon` and subsequently with the phone using unix sockets.

`Catcher` is a modified version of the `cell_log` program by Andreas Eversberg that interfaces with `osmocon` to harvest information from BTSs and forward it to the ICDS. It can be seen as a layer 3 program that scans through available frequencies and reads information from the BCCH whenever one such channel is available on the frequency at hand. The forwarding is done directly via `stdout` since it runs as a child process of the ICDS. The functionality of `catcher` will be explained in detail in Section 3.2.1 while the implementation and operation of the ICDS will be discussed in Section 3.3.

3.2. Procedure

The main goal of the ICDS is to reach a conclusion on whether it is safe to initiate a phone call or not, in other words if the base station our mobile phone will connect to is trustworthy. As mentioned before as soon as a subscriber connects to an IMSI Catcher it automatically gives up information on his/her location. Therefore this project will use a passive approach on information harvesting, meaning we will only use information that is broadcasted or freely available as to not give up any hints of the ICDS being active.

To that end a four-step process is taken. First the information is gathered. This process is explained in detail in Section 3.2.1. After information on the surrounding BTSs is ready in the ICDS, a set of checks is evaluated on each base station individually, with each yielding a specific result for the station. These checks are called *rules* and discussed further along with the next two steps in Section 3.2.2. Afterwards the results the rules yielded for each base station have to be aggregated into one single result for each BTS. At last, after every BTS has its evaluation it can be decided whether to tell the subscriber it is safe to initiate a phone call or not.

3.2.1. Information Gathering

As explained in Section 2.3.2 every base station has an associated BCCH where information about the station and its network is spread. BCCH frames are always sent inside a

TC	System Information Type
0	Type 1
1	Type 2
2,6	Type 3
3,7	Type 4
4,5	Any (optional)

Table 3.2.: Type Codes and the corresponding System Information Types [10].

51-Multiframe. After the MS has synchronised using the values on the FCCH and SCH it can determine which kind of information is hosted inside the BCCH message. These so called System Information Messages originate at the BSC and are produced for each BTS individually and then periodically broadcasted. Since all the required information would not fit inside a single frame there are different kinds of System Information Messages that are distinguished by their Type Code (TC) and host different kinds of information. The type can be extracted using the Frame Number (FN) of the frame the message is sent in [10]:

$$\text{TC} = (\text{FN div } 51) \bmod 8$$

Table 3.2 shows how the TCs can be mapped on those types. For this project the System Information Type 1-4 are of interest because these are available to all MSs that tune in to the particular BCCH of the respective BTS without actively connecting to it.

The information contained inside the System Information Messages is harvested via the `catcher` program. `Catcher` is implemented inside the OsmocomBB framework and connects over the `osmocon` application to the Motorola C123. At first a sweep scan is done over all the ARFCNs to measure their reception levels in order to determine where base stations and thus BCCHs are located. Afterwards `catcher` tunes the phone to those specific frequencies where a BTS was found

At each such frequency it waits until all the System Information Messages are gathered and extracts parameters where possible. The parameters along with the raw data are forwarded to the main ICDS application for further evaluation. Examples for all the System Information Messages used, along with an interpretation are located in Appendix C. As long as scanning mode is active all the available stations are scanned repeatedly and changes in the BTSs will continuously update the data model inside the ICDS software. The parameters harvested are:

- Country: The interpreted country code the base station is broadcasting.
- Provider: The interpreted provider code the base station is broadcasting.
- ARFCN: The ARFCN on which the base station is located.

- rxlev: Receiving strength in db. This parameter is measured by the Motorola C123 and not part of the System Information Messages. Even small changes in the location can have a large impact on this parameter due to shadowing and reflection. However it can be used in certain cases as will be discussed in Section 3.2.3.

- BSIC: Because of frequency reuse in a cellular network it is possible that two different base stations can sent at the same ARFCN. In order for the MS to keep these apart the Base Station Identification Code (BSIC) is also broadcasted. It consists of a Network Color Code (NCC) identifying the provider, so the MS can filter out messages that it does not need beforehand and the Base Station Color Code (BCC) that must be unique for a given provider over all base station in a large area.

- LAC: This is the last part of the LAI (that consists of MCC + MNC + Location Area Code (LAC)) and is a hierarchical identifier for a given base station. The hierarchy is provider wide, meaning two different providers may use LACs with a completely different numbering system. The LAC is used by the provider to tell the ME that it entered a new area and has to announce itself.

- Cell ID: The Cell ID is a globally unique identifier for the cell the MS is connected to.

- Neighbouring Cells: Each base station keeps a list of other base stations in the perimeter for the MS to scan and determine if there is a BTS with a better reception in the area.

- Encryption: The encryption algorithm used to encrypt the voice data.

Note that there are different formats for the Neighbouring Cell List since the original number of 17 bytes could only present a bit mask for 124 neighbouring ARFCNs. This works for the 900 MHz band, but for the extended 900 MHz and the 1800 MHz band the System Information Type 2bis and System Information Type 2ter have to be harvested additionally to construct the Neighbouring Cell List.

Encryption cannot actually be read passively from a base station since the encryption algorithm is determined when a connection is established (finish paragraph on encryption when feature is finished).

3.2.2. Information Evaluation

Each base station is evaluated the moment the data completely arrived at the ICDS application. Additionally when a new BTS has been found and added all formerly discovered stations are also re-evaluated since new discoveries can have an impact on the rules that evaluate the context surrounding an old base station.

Rule	Functionality
Provider Known	Checks whether the provider is in a list of known providers.
Country/Provider Map	Checks whether the given provider is a valid provider for the given country.
LAC/Provider Map	Checks whether the LAC of the station is in the normal LAC range for that provider given the area.
ARFCN/Provider Map	Checks whether the ARFCN is in the officially registered range of the provider.
Encryption Algorithm	Checks which encryption algorithm is used.

Table 3.3.: Configuration Rules implemented inside the ICDS.

As mentioned above, evaluation is done based on constructs called rules. Each rule represents one check that can be performed on a base station and yields a result based on its findings. A *Critical* result means that the base station evaluated has a critical configuration error or critical settings that are not found on normal base stations, e.g. unknown provider names or encryption that is turned off. This station should not be trusted.

If a *Warning* status is yielded the BTS at hand has some concerning features but it could not be said whether it really is an IMSI catcher or sheer coincidence. An example would be a base station having a neighbouring cell list of which none of the cells therein have actually been found up to that point. The list could either be a fake or it could simply be coincidence that the scan has not found any. They could have been out of range for example.

In some cases a rule cannot yield a finding. That is when the state is explicitly set to *Ignore* so the evaluator knows that this rule should have no influence on the final outcome. This is the case for example when trying to find whether the base station uses encryption or not and no other subscriber connects until a set timeout is reached.

If everything went as expected, *Ok* is returned.

These rules can be divided into two different categories depending on how they work and which situations they are tailored to. Most of the rules are parametrised so they can be tweaked to different environments and standards.

The first set of rules called *Configuration Rules* targets the base station itself. Rules in this category are meant to check parameters that concern the BTS for integrity and configuration mistakes that could have been made by an IMSI catcher operator. An overview of which Configuration Rules are currently implemented inside the ICDS is given in Table 3.3. Since there is no official listing or rule how the LAC is derived the LAC/Provider Mapping Rule needs knowledge of the area in which the ICDS is used. The ICDS itself

Rule	Functionality
LAC Median Deviation	Checks whether the LAC of the given BTS deviates more than a certain threshold from the median LAC of that provider.
Pure Neighbourhoods	Checks whether all found stations in the Neighbouring Cell List share the same provider.
Neighbourhood Structure	Checks the structure of the Neighbouring Cell List for certain patterns.
Fully Discovered Nbhds.	Checks whether all the cells in the Neighbouring Cell List have actually been found.
Cell ID Uniqueness	Checks whether there are other cells with the same Cell ID.
LAC Change	Checks whether the LAC changes in the course of a scan
rx Change	Checks whether the reception level changed significantly during the course of a scan

Table 3.4.: Context Rules implemented inside the ICDS.

can be used to gather that knowledge but it has to be done prior to using the rule for base station evaluation. The ARFCN range each provider has registered in Germany can be looked up at the website of the Bundesnetzagentur[1] which is needed for the ARFCN /Provider Mapping Rule.

The second set of rules is called *Context Rules*. As the name suggests these rules serve the purpose of checking how well a given BTS fits into its neighbourhood. Table 3.4 shows which rules have been implemented. The Neighbourhood Structure Rule will be explained in a bit more detail in the next section. For the LAC the median was chosen over the average since if an extreme value (ill configured IMSI catcher) exists it would have a too strong impact on the average to which all the BTS are compared. It could even have such a strong effect on the average that legitimate base stations would fall below the threshold and be recognised as catchers.

Neighbourhood Structure

The neighbourhood structure is the graph that is described by the Neighbouring Cell List located in the System Inforamtion 2/bis/ter constructs. Figure 3.3 shows an example of

[1] Bundesnetzagentur Vergabeverfahren,
`http://www.bundesnetzagentur.de/cln_1911/DE/Sachgebiete/Telekommunikation/RegulierungTelekommunikation/Frequenzordnung/OeffentlicherMobilfunk/VergabeVerfahrenDrahtlosNetzzugang/vergabeVerfahrenDrahtlosNetzzugang_node.html` [Online, Accessed 04.2012]

the neighbourhood graphs at the Technische Fakultät of the University of Freiburg[1]. It can be seen that for each provider, the neighbourhood forms an isolated, nearly fully connected subgraph. The bordering white nodes have not yet been discovered therefore they have no outgoing edges. This could be the case because they are too far away for the Motorola to receive or because of signal damping due to shadowing and reflection effects. In the ICDS the aspect of isolated subgraphs for neighbourhoods is captured inside the *Pure Neighbourhoods Rule*. An interesting fact is that one node inside the E-Plus subgraph on the upper right is marked red. This is because it is the BTS of the universities own GSM network. It was set up to be in a E-Plus neighbourhood but is not consistent with the E-Plus nodes surrounding it. Therefore it is marked by the ICDS.

Some of the attacks discussed in Section 2.4.1 imply a certain structure of the neighbourhood graph. Since the IMSI catcher tries keep MSs that have connected from switching back to a normal cell the neighbourhood list of such a catcher cell would either be empty or would only host neighbour cells that have a lower reception than itself. An empty neighbourhood list is represented in the graph by a node that has been discovered and has no outgoing edges. Figure 3.4 shows a simplified regular neighbourhood graph compared to a graph with two catcher nodes inside. In this case catcher C chose the attack where it replaces a previously existent BTS whereas catcher D opened up a new cell. Replacing has several advantages, one being already integrated in the neighbourhood of other nodes and thus being able to catch subscribers by handover. For catcher D it is the other way around, it has only outgoing edges. This means that this cell is not known by any other node of the same provider (of course the catchers provider is fake!). Nevertheless it has some outgoing edges to nodes with significantly less transmission strength to not stick out too much as a completely isolated node. Combinations of these two approaches are also possible. These thoughts are basically what is captured inside the *Neighbourhood Structure Rule*.

Base Station Evaluation

As mentioned at the beginning, all the rules are evaluated for each base station. Aggregation of these rule results into a single result is done by modules called *Evaluators*. Currently there are three different evaluators implemented inside the ICDS, with varying degrees of customisability.

- Conservative Evaluator: This is a worst-case evaluator. It iterates over all the rule findings and yields the most concerning finding as its result. By default this evaluator is enabled in the system.
- Weighted Evaluator: Using this evaluator the user can give a weight to each rule. This way rules that are more important to the user can have a higher impact on overall evaluation.

[1] Georges Koehler Allee, Freiburg

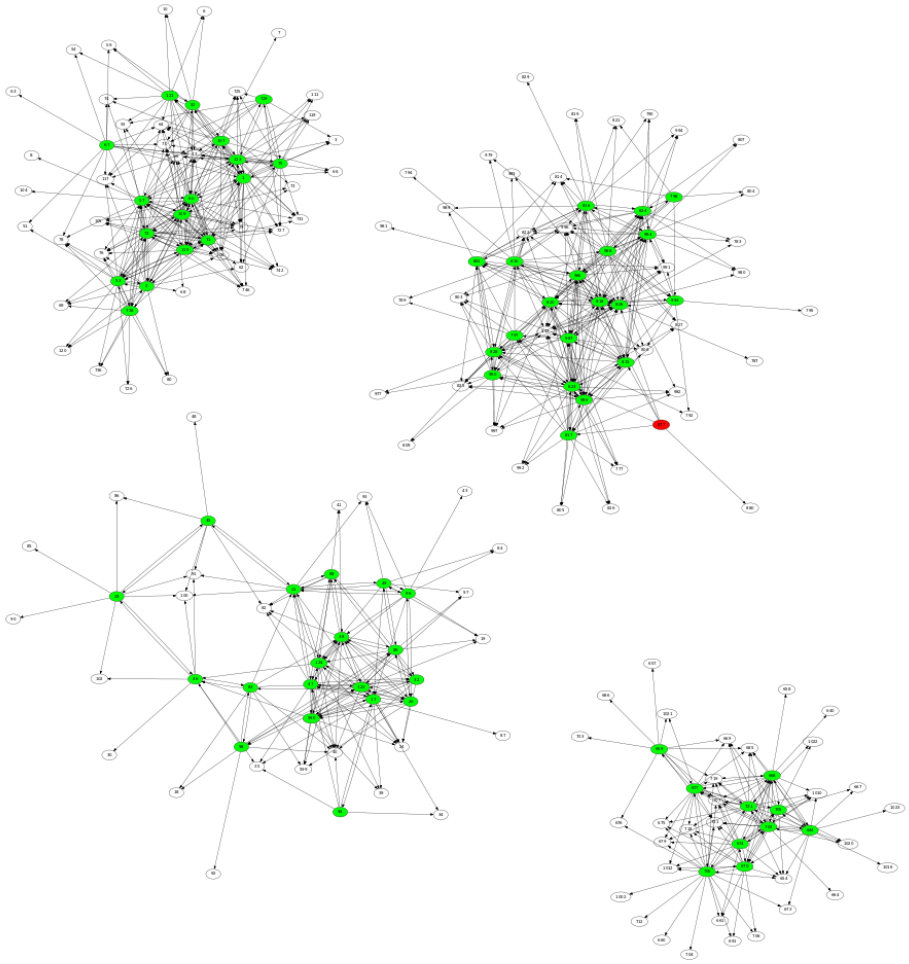
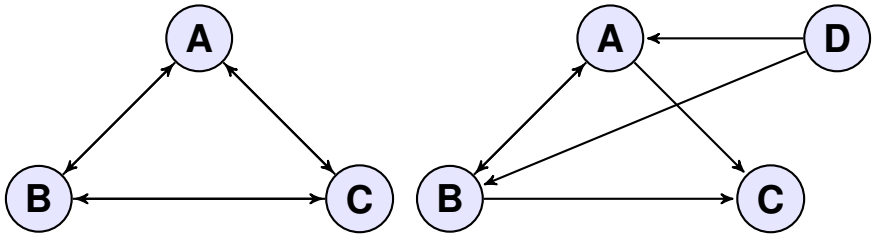


Figure 3.3.: Base stations and their neighbourhood connections at the Technische Fakultät.



(a) Normal neighbourhood (b) Tainted neighbourhood

Figure 3.4.: Comparison between a normal neighbourhood subgraph and a tainted one.

- Grouped Evaluator: With this evaluator rules can be grouped together. Inside each group the result for the group is found by majority vote whereas the final result is conservatively found by comparing all the group results.

The different kinds of evaluators can be used to tweak the whole system more to a specific environment or purpose, if specific rules or groups of rules are given more weight. After a finding has been determined for each station, all the results are again aggregated into a final result. The overall result depends on which mode the ICDS is used it. If it is used as analysis tool the final result will be a conservatively aggregated result over all the stations in the list. If the ICDS is run in user mode, which is the mode an end user would use the system, the ICDS looks up the provider the user has provided, filter out the base station with the best reception for that provider and yield its evaluation as final evaluation. This reflects the fact that a subscriber cannot choose the BTS it connects to but the ME will rather connect to the best base station available for its given provider.

3.2.3. Forged Parameters

All of the parameters that have been looked at in this project so far are parameters that can directly be set by the operator of the BTS or IMSI catcher. This is a major problem since how can an IMSI catcher be found that sends exactly the same information as a regular base station? To further investigate this issue we will analyse based on the three attack types presented in Section 2.4.1 which parameters can be forged and which cannot.

For all three attack types presented it is possible to find a parameter configuration that does not raise suspicion, if the operator chooses a compatible ARFCN, etc. for the mimicked provider. However if the IMSI catcher does not have a different LAC it will not notice that a subscriber has just connected to it, as long as the subscriber stays passive.

The Neighbouring Cell List is a bit different. Since the catcher wants to keep lured subscribers it will normally have an empty list or a list pointing only to BTSs that have a lower reception level. Both of these cases can be detected. However the operator *may* also choose to set a list consistent with the neighbouring cells. This would lower the chances of success for the catcher but also make it blend better in its environment and thus harder to detect.

A sure criterion is the absence of an encryption algorithm which is needed by the catcher to record and monitor phone calls. The main problem here is that it cannot be guaranteed that this parameter can be harvested. Since this is a semi passive approach to harvesting it needs another subscriber to connect to the base station in question during the time the ICDS is scanning it. Also if the IMSI catcher is only set up to do localisation, the encryption can be enabled.

For the Cell ID there are basically two possibilities depending on which attack is used. The first possibility is that the IMSI catcher replaces a formerly existent cell and the second one is that it opens up a new cell. In the second case parameters can be chosen in a

consistent way although a new Cell ID has to be chosen, as the Cell ID needs to be unique. In the first case all parameters can be copied from the original cell. Both possibilities can be resolved by adding outside knowledge to the ICDS thus circumventing the problem of other parameters being forged. This is done by rules called *Database Rules*.

Database Rules

There are to different rules that each handles one of these cases. The first case is the easier of both. We know that the catcher cell has a new Cell ID that has not been there before. Therefore the *Cell ID Databse Rule* has two different means to exploit this fact:

- A database of Cell IDs can be learned by the ICDS beforehand. This can be used to detect new Cell IDs that have not been seen before.
- A commercial Cell ID databse can be used to compare against the Cell IDs found by the ICDS. A web service also offered by most providers of Cell ID databases.

The three largest Cell ID databases are the two commercial ones by Ericson[1] and combain[2] as well as the free alternative OpenCellID[3] [29]. Ericson and combain have trial modes, where the first 1000 requests are free for developers afterwards a subscription or a fee per request must be paid. Another free alternative with a large coverage is Google Mobile Maps, that also offers a web service where CellIDs and their respecitve LAIs can be checked against their database to obtain localisation information (or simply check if they are part of the database). By adding this information new cells can be identified.

The second where an existing cell is replaced is a bit more complicated since its parameters are an exact copy of the old cell. Attacking by replacing a cell works in a way that the cell with the worst reception is targeted. That way when the IMSI catcher finished replacing it, the reception goes up a significant amount and the mobile phone will initiate a handover to that cell. The difference in reception can be used to identify this kind of attack. In general the reception cannot be well used as a parameter because shadowing and reflection can substantially change the reception from one moment to the other. However when reception intervals are logged for a fixed location like an office and important calls made from that specific location can be protected against this kind of attack. To that end the ICDS can monitor reception levels to build up databases with information about the reception intervals of the particular cells in different locations. The*Location Area Databse Rule* then checks if reception levels differ significantly for a given location. If no database has been build beforehand but the ICDS is stationary the *rx Level Rule* can watch the reception level during the course of a scan and ensure that no change occured suddenly.

[1] Ericson Labs, `https://labs.ericsson.com/apis/mobile-location/` [Online; Accessed 04.2012]

[2] Mobile Positioning Solutions, `http://location-api.com/` [Online; Accessed 04.2012]

[3] OpenCellID, `http://www.opencellid.org/` [Online; Accessed 04.2012]

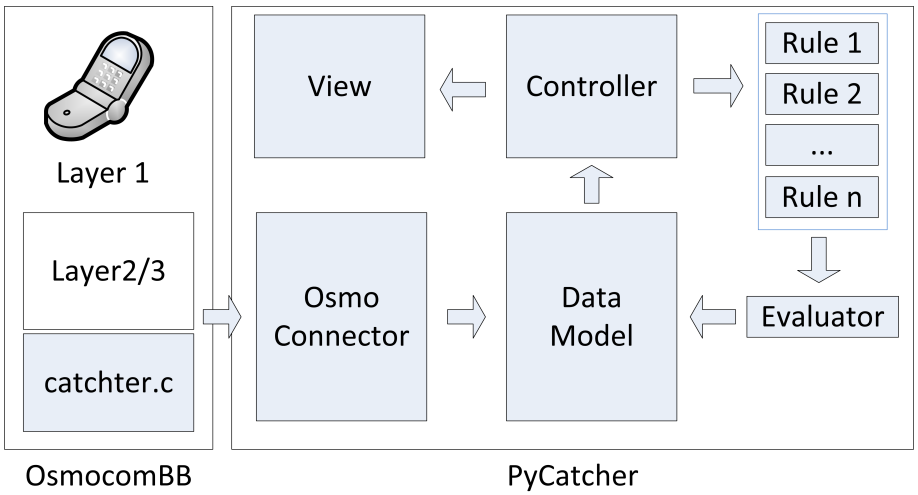


Figure 3.5.: System architecture of the ICDS. The arrows indicate the flow of data.

3.3. IMSI Catcher Detection System

This section will discuss some technical aspects of the ICDS software itself. The first section focuses on architectural aspects and how the architecture can be extended whereas the second and third section will then explain how to configure and operate the application.

3.3.1. Implemetation

Figure 3.5 shows a diagram describing the system architecture, the modules in light blue have been implemented for this project. The application consists of two main parts. One part, the `catcher`, is implemented inside the OscmocomBB framework, the other part, `PyCatcher`, is a Python application that uses `catcher` to harvest information and evaluate it afterwards. Since the way `catcher` works has already been described in Section 3.2.1 this section will focus on the Python application part.

As mentioned before layer 1 of the GSM stack is implemented in the firmware running on the Motorola C123. Layer 2 and 3 are implemented on the computer and are used by the `catcher` software to harvest information from the BCCH.

The `PyCatcher` application was designed with a Model View Controller (MVC) approach in mind to make it easy to implement new functionality. The MVC pattern is used to separate the data model of an application from the logic as well as from the way it is presented to the user. That way each of the different components can be exchanged without affecting the other two. An additional module has been added, the `OsmoConnector` that is loaded by the controller and spawns `catcher` as a child process. It takes the out-

```
dictionary = {
        "key_1": value_1,                 #single value
        "key_2": [value_2,value_3]        #value range
}
```

Figure 3.6.: Configuration Dictionary in the settings file.

put back in and transforms it into an object oriented representation of the discovered base stations. These are then handed over and update the data model. This way it can be ensured that only coherent and complete information is incorporated in the data model. Another benefit is that the parsing module is isolated from the main program logic.

The `Controller` is the main part of the program and instantiates all the other modules. It loads data from the model, triggers the evaluation and sends the results to the view to be displayed. As discussed before there are several rules that can be evaluated for each base station. These rules are stored within the controller and can be enabled or disabled by using the view that relays new rule configurations back to the controller to be applied. Whenever a new evaluation is requested the controller evaluates the active rules and gives the results to the active evaluator, afterwards the results are send to the view for display to the user. Note that all the structures used are view independent, this way the current view could easily be exchanged with a web interface for example.

The `View` in this project consists of a GTK3 window with several forms for user input. It is bound to the controller using PyGTK. Details on the `View` and how to use it will be explained in Section 3.3.3.

Rules and Evaluators were designed in a plugin fashion, since these are the main points where the program can be enhanced and new ideas can be realised. Implementing a new rule or a new evaluator works by extending the rule or evaluator base class and implementing one method inside that derived class that contains the actual logic. After that they only need to be added to the list of included evaluators and rules inside the `Controller`. Appendix B.1 gives an example of how this can be done.

3.3.2. Configuration

The configuration of the system is done in the file `settings.py`. All configuration is done with python dictionaries, where each module has its own dictionary inside which it can have an arbitrary number of parameters with their respective values. Figure 3.6 shows an example with the two common cases used for parameters in this project.

The file consists of three main sections. The first one contains parameters that are needed for the correct operation of the ICDS system and have to be edited:

- `Device_settings`: The setting for the mobile phone that is used. In case the

Motorola C123 is used, this section does not need to be edited.

- `Osmocom_lib`: The path to the folder that contains the OsmocomBB framework.
- `Commands`: This is only to be edited when a newer version of the framework is used and the folder structure has changed since the release used in this project.s

The second and last sections are parameters for the different rules and evaluators. A completely documented configuration file with all the rules and evaluator parameters can be found in Appendix B.2. The file is read in as a python file. This way python code can also be used to change settings dynamically depending on the environment or how the ICDS is started.

3.3.3. Operation

The ICDS main application has to be started with root privileges since it needs to work with Unix sockets and open up connections to the Motorola C123. This should be done by starting up the `main` class that initialises everything else.

```
1 sudo python /path-to-project/Src/PyCatcher/src/main.py
```

After a brief loading time the main window shown in Figure 3.7 should appear if a valid configuration is set up.

The different elements shown in the main window are:

1. Firmware Loader: This button is used to load the OsmoconBB firmware onto the Motorola C123. For this to work, the mobile phone must be connected correctly to the computer and available on the configured `tty` interface. After pressing the button on-screen instructions will lead the user through the process of flashing.
2. Scanner: This starts the `catcher` subprocess in the background and fills the data model with information on the discovered base stations. During this process the Base Station List (11) and the Base Station Graph (13) will also be populated in realtime. Re-evaluation on all base stations is done for every new BTS that has been found.
3. Filter Window: This brings up the window shown in Figure 3.8(a), where different view filters for the Base Station List and the Base Station Graph can be set. Note that these filters do not modify the underlying data model or the behaviour of the scanner, the manipulate merely the view. Hidden base stations will be scanned and added to the data model independent from the filters set, so they can be viewed at a later point if necessary. Available filters are:
   - Provider Filter: Takes a comma separated white list of providers that should be shown.

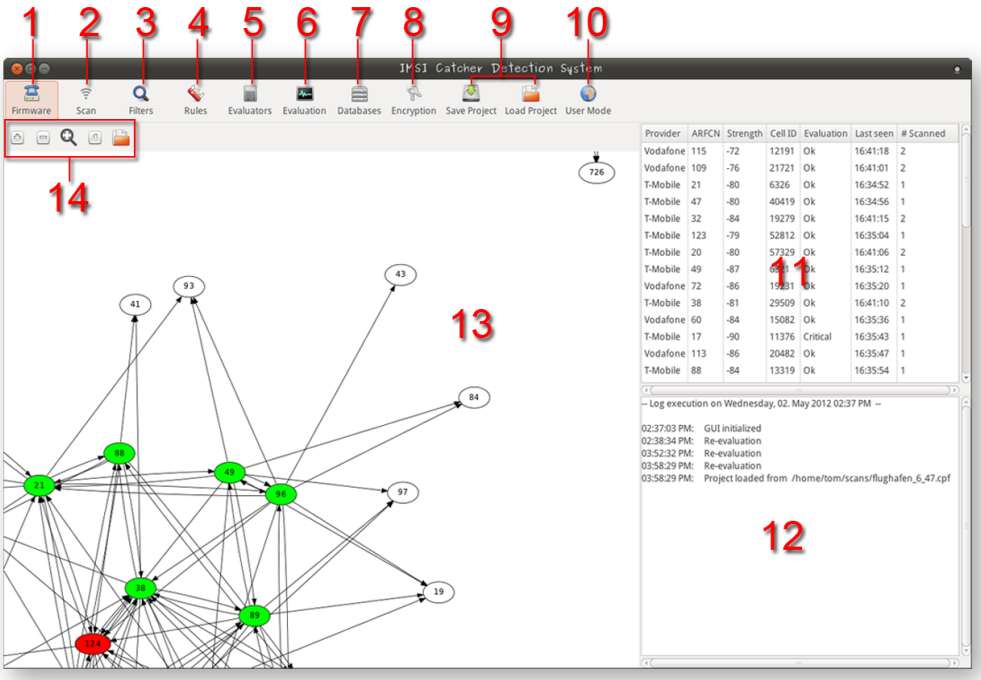


Figure 3.7.: The ICDS main window.

- ARFCN Filter: Takes a range of ARFCNs to be shown.

These two filters can arbitrarily be combined together. Filters are designed the same way as rules and evaluators, a new filter can be implemented by derivation of the base class.

4. Rules Window: All the rules implemented inside the ICDS will be brought up with a check box to enable or disable these rules. Disabling means that they will not be considered for the evaluation of a base station. A screenshot can be seen in Figure 3.8(b).

5. Evaluator Window: This window will let the user choose which evaluator to use for BTS evaluation. Choosing a new evaluator will also trigger a re-evaluation of all the data collected so far.

6. Evaluation: This button brings up a separate window showing only the final evaluation of the scan. The final evaluation shown in this dialog *will* be affected by the filters set. Base stations that are filtered out are not considered.

7. Databases Window: The window shown in Figure 3.8(c) contains settings for all the databases the ICDS uses. These settings are mandatory if the Local Area Database Rule or the CellID Rule is going to be used. It is also possible here to export the current scan as a Comma Separated Value (CSV) file or sqlite database to be used in other programs.

8. Encryption Window: This button brings up a dialog in which an ARFCN or a list of ARFCNs can be scanned to discover which encryption is used by the BTS. A timeout for this operation can also be set here. The longer the timeout the more likely another subscriber will connect to the base station in the given time frame.

9. Save/Load Project: The current state of the application can be saved as or loaded from a `.cpf` file. This enables the user to continue a scan at a later time or to compare different data sets scanned at different points in time or locations with one another.

10. User Mode: The ICDS is ultimately meant to be a tool that can be used by end users to check whether it is safe to initiate a phone call or not. This dialog presents a way the already configured tool could be presented to end users. Only the provider is to be entered and a final evaluation will be returned once the ICDS is done with the process.

11. Base Station List: This list gives an overview of which base stations have been discovered so far along with some distinguishing information including its evaluation. A detailed view of a base station can be brought up by selecting it in the list

and pressing the enter or return key. The report is separated into four main parts, the first being all the harvested parameters, followed by findings the different rules and evaluators yielded and a section with the raw uninterpreted system information data.

12. Log Window: Every important event inside the ICDS is reported in the log together with a time stamp when it occurred.

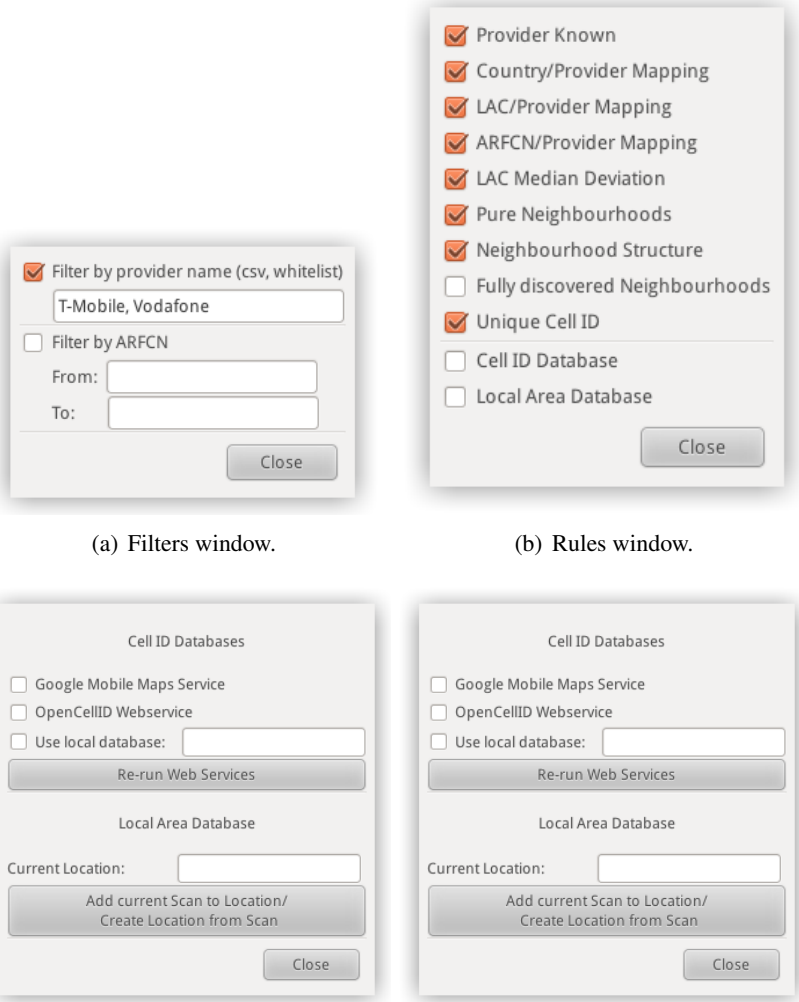
13. Base Station Graph: This graph displays the base station found in the Base Station List (11). A node represents a single BTS and is labelled with its respective ARFCN. An edge from note A to B is drawn if node B occurs in the Neighbouring Cells List of A. Nodes with a white background have only been found inside Neighbouring Cell Lists but not yet by the ICDS scanner itself whereas nodes with a red, yellow or green background have been found and evaluated with the colour representing either a critical, a warning or an ok status respectively.

14. Graph Controls: These are meant to make navigating the graph a bit easier. From left to right the functionality is zoom in, zoom out, fit the whole graph to the viewport and display the graph in original size. Zooming can also be done with the mouse wheel and it is possible to drag the graph around by clicking and holding it with the mouse and then moving it in the desired direction.

The procedure of operation differs depending on the purpose.

Sweep scans: This is the normal mode of operation, scanning and evaluating all base stations in the perimeter. This is also used for gathering various kinds of information to be used for analysis later. At first the firmware needs to be flashed onto the device by pressing (1). After the flashing process is finished the scan can be started by pressing (2). Either before or during the scan (3),(4) and (5) can be used to customise the output or rules that should be considered during evaluation. The scan can be stopped at any time. Resuming the scan will renew the information in the Base Station List. The scan will continue renewing information until it is terminated by the user. The number of times a specific BTS has been scanned is shown in the *Sightings* column of the Base Station List.

CellID Information: CellID information can be obtained through several different means. The Databases window shown in Figure 3.8(c) can be brought up by pressing (7). In the upper part settings concerning the acquisition of CellIDs can be found. The operator has the choice between three different methods which can also be used in combination. *Google Mobile Maps Service* compares the station's CellIDs and LAIs to the ones in the Google database. If they are found they are marked as such and additionally their location information will be set. *OpenCellID Web Service* performs the same task if activated. As of now OpenCellID has a very low coverage compared to Google's service but it has been



(a) Filters window.

(b) Rules window.

(c) Databases window.

(d) Encryption window (not yet implemented).

Figure 3.8.: Dialogs for different settings.

included since it is an open source approach that is actively developed and updated constantly. The *Use Local Databse* feature allows to use a previously build Location Area Database as CellID Database for lookups. For this purpose the location to be used as database has to be entered in the textfield. Offline lookups can be done that way, which are considerably faster that online lookups, the raw data used by the OpenCellID project can also be downloaded and used as a offline version for reference that way. Since these lookups take some time if performed using webservices, this is not done while the scan is taking place, to not delay the acquisition of information from new base stations. Pressing the button below the checkboxes will add the CellID Database information from the selected sources to all the stations currently in the base station list. If more than one service is activated lookups will be done starting with the Google service, if active and using the next one in line only if the previous lookup failed. Having at least one service activated and run on the base station list is a precondition for the CellID Rule to work.

Location Area Database: Having set up the correct location in the *Current Location* field of the databases window and having a valid database for that location are preconditions for the Location Are Database Rule to work. To build up a database for a specific location a sweep scan for this location has to be done. After the sweep scan is finished, the current location has to be set in the dialog and the button for adding/updating the database has to be pressed. If there was no existing database for that location it will be created, otherwise the database will be updated with the new information acquired by the sweep scan. To raise the quality of a Location Area Database it is recommended to do multiple sweep scans and integrate them rather than to only rely on a single scan. This raises the probability that all BTS in the perimeter are found is higher and it solidifies the interval in which the base station signal strength varies.

Scan Encryption: To be implemented . . .

User Mode: To be implemented . . .

Chapter 4.

Evaluation

The following chapter presents the results of some experiments done with the ICDS. Evaluation has been done in different areas to give a complete impression of how the ICDS performs. In the first section some general findings will be described that affect overall performance. Afterwards the test environment and setup of the IMSI catcher is discussed. The last two sections evaluate the ICDS against a configured catcher, first to test the individual rules and second against the attacks that were listed earlier.

4.1. Performance Evaluation

In order to evaluate general performance it has to be considered that the ICDS can be deployed in different environments. To reflect different compositions and densities of base stations form different areas, four distinct data sets will be used for the experiments in this section. The data sets have been taken in areas surrounding the city of Freiburg. Table shows some of data sets' key values.

Apart from nodes from the four public GSM providers E-Plus, T-Mobile, Vodafone and O2, nodes from Deutsche Bahn also occur in these scans. These nodes form a private network used for internal communications by Deutsche Bahn. They are identified by their

Name	Description	Number of BTS	Scan Duration
`cdb`	CBD around the area of Bertholdsbrunnen	54	6:13
`airport`	Airport and university area around Georges Koehler Allee	68	6:25
`ind_park`	Industrial park Haid in Freiburg West, Hausener Weg	53	4:52
`house_area`	Housing area at the rim of Freiburg Zähringen, Thuner Weg	22	3:59

Table 4.1.: Key values of the data sets used for performance tests.

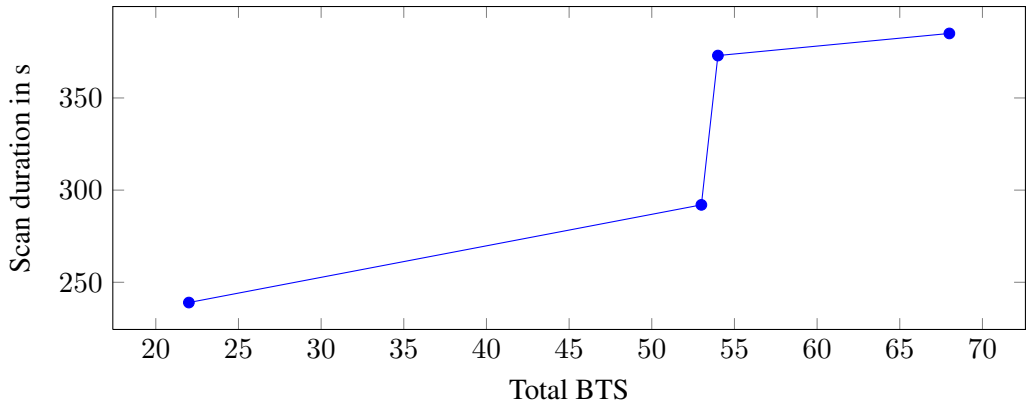


Figure 4.1.: Scan durations for the sample data sets.

broadcast name 'DB Systel GSM-R' and their frequency which is outside the regular bands. Since the distribution of these nodes is very sparse, only one node can be found in each scan they yield a false positive for no neighbouring nodes can be discovered. These nodes are not relevant to subscribers because they are not able to connect to them. Therefore they will be ignored and factored out for the remainder of this evaluation.

4.1.1. Scan Duration

Table 4.1 shows that the times for scans in the Freiburg area can differ by large amounts depending on how many base stations are scanned. Generally said it takes longer the more dense the base station distribution is in the scanned area. This is however not the only factor, as Figure 4.1 visualises. If the scan duration would only depend on the number of base station scanned, a linear growth could be expected.

There is a large increase in scan duration between the `ind_park` and the `cbd` data sets although only one more base station was detected. This jump can be explained considering the context of the scan. The scans were done on a Saturday between 14:00 and 16:00. The Freiburg CBD was crowded at the time of the scan as was the university campus due to an event held there. Contrary to that the industrial park area was very calm, as was the housing area. Whenever the ICDS discovers a BTS it needs to wait until all system information messages are gathered before it can continue scanning for further base stations. In a crowded area reception is far worse due to radio inference therefore it takes longer to accumulate the information needed resulting in increased scanning times.

A crowded area with high density of BTSs could be seen as a worst case for scan duration. Re-evaluation of a base station based on its own parameters thus occurs only every 7 minutes in this worst case. This is an inherent problem to the approach of scanning and updating all base stations and not only monitoring a subset from a single provider. If

	cdb		airport		ind_park		house_area	
	Cov.	Time	Cov.	Time	Cov.	Time	Cov.	Time
Google	1.00	5	0.99	8	1.00	5	1.00	2
OCID	0.57	51	0.58	68	0.58	55	0.41	19

Table 4.2.: Coverage for Google Mobile Maps and OpenCellID on the data sets with the time needed in s for fetching the information.

an IMSI catcher replaces a base station directly after it was scanned, it could take up to 7 minutes until it is discovered. To lessen this threat, if the ICDS is used in user mode, the base station with the strongest reception is scanned again, to eliminate the possibility of having been taken over and not being detected.

4.1.2. Cell ID Databases

The usefulness of the Cell ID Rule is subject to the completeness of the database that is used. That is even more so since a database with a low coverage will yield false positives, e.g. legitimate base stations will be evaluated as being IMSI catchers because they are not found in the database.

The coverage for the OpenCellID database and the Google Mobile Maps service evaluated against the data sets can be seen in Table 4.2. Google Mobile Maps service scored a complete coverage on all the data sets while Open Cell ID could cover about half the nodes in the different sets. The reason the Google service had only a 99% coverage on the `airport` data set is that base station that has not been found was the one operated by the chair of communication systems, therefore it can be factored out. The OpenCellID database is not a good source of information for this project as is shown by its coverage scores. However it must be said that these two services are intended for localisation and thus do not have the demand to yield a complete coverage of all the base stations in the area. Therefore it must be kept in mind when using this rule for analysis that false positives might still be brought forth. What can be said though is that a base station that has been found may only be subject to a type of attack that replaces an existing base station and can thus be investigated more specifically.

Figure 4.2.: Open Source IMSI Catcher.

4.1.3. Encryption Detection Speed

4.2. IMSI Catcher Detection

4.2.1. Open Source IMSI Catcher

The remainder of the rules cannot be tested without an active IMSI catcher. For this purpose the Open Source IMSI Catcher [28] is used.

This project builds up an IMSI catcher using only Open Source systems and freely available hardware so it can basically be used by anybody. On the hardware side a computer running a Linux operating system is used, as well as the Universal Software Radio Peripheral (USRP) as the radio transmitter. The USRP allows the signal processing for radio transmissions to be done in software, therefore it can be used for a multitude of purposes and protocols. Some hardware modifications have to be done to the device to empower it to send and receive data on the frequency bands used for GSM communication. An external clock needs to be used since GSM operations are very time critical.

On the software side GNU Radio[1], OpenBTS[2] and Asterisk[3] are used to achieve the functionality provided by a IMSI catcher. Figure 4.2 shows how these components are chained and used together. The raw data that is received by the USRP is sent to the GNU Radio component which works as a software side interface to the USRP. This data is taken by the OpenBTS software that emulates base station behaviour and has an integrated module simulating a VLR and handing out TMSIs. OpenBTS implements an open source version of the GSM stack with the goal to provide cheap access points to the GSM network in areas with bad coverage. The user accounts are as well as encoding of voice data and recording of calls is handled inside the Asterisk software, basically combining the TRAU, HLR and authentication centre of a real GSM network. Calls are routed from here on to the Voice over IP (VoIP) network of the university.

Since we do not want to actually connect to the IMSI catcher, the Asterisk part and user configuration will be omitted here. The parameters necessary to simulate a GSM cell have to be set inside the `OpenBTS.conf`. Figure 4.3 shows an annotated example for a configuration simulating a T-Mobile cell. `Control.OpenRegistration` is explicitly set to 0 which prevents anyone from connecting to the IMSI catcher since connections are not part of the test and we do not want to interfere with other peoples' communications in the area.

[1] GNU Radio Project Wiki, `http://gnuradio.org/redmine/projects/gnuradio/wiki` [Online; Accessed 05.2012]

[2] OpenBTS Project Wiki, `http://wush.net/trac/rangepublic` [Online; Accessed 05.2012]

[3] Asterisk, `http://www.asterisk.org` [Online; Accessed 05.2012]

```
#Do not let people connect
Control.OpenRegistration 0

#Basic cell parameters
GSM.MCC 262                     GSM.ARFCN 54
GSM.MNC 01                      GSM.ShortName T-Mobile
GSM.LAC 29184
GSM.CI 61858

#Transmission strength ranging from 0 to 23
GSM.PowerAttenDB 20

#Neighbouring cell list, space separated
GSM.Neighbours 69 53 20

#Force location Updates, multiple of 6 minutes
GSM.T3212 1
```

Figure 4.3.: Excerpt of a `OpenBTS.conf`.

4.2.2. Rule Evaluation

4.2.3. Attack Scenarios

Since all the rules have been tested we assume from this point on the IMSI catcher is configured correctly, meaning that parameters like the ARFCN, LAC or provider have been set up in correct and consistent way so the respective rules will not show an alarm. Consistent parameters for the four providers in Germany can be found in Tables 4.3 (a)-(d). Note that the Cell ID can be a arbitrary value as long as it is unique in the area of reception. Cell IDs measured from different base stations do not follow any particular schema.

4.2.4. Long Term Test

(a) T-Mobile

Parameter	Range
Name	T-Mobile
ARFCN	13-49, 81-102, 122-124, 587-611
LAC	21014 / 21015
MCC	262
MNC	01

(b) Vodafone

Parameter	Range
Name	Vodafone
ARFCN	1-12, 50-80, 103-121, 725-751
LAC	793
MCC	262
MNC	02

(c) E-Plus

Parameter	Range
Name	E-Plus
ARFCN	975-999, 777-863
LAC	588 / 138
MCC	262
MNC	03

(d) O2

Parameter	Range
Name	O2
ARFCN	0, 1000-1023, 637-723
LAC	50945
MCC	262
MNC	07

Table 4.3.: Consistent parameter configurations in the Freiburg area for the four German providers.

Chapter 5.

Conclusion

5.1. Future Work

Bibliography

[1] Data link (dl) layer; general aspects. GSM 04.05, http://www.3gpp.org/ftp/Specs/archive/04_series/04.05/0405-802.zip, 1999.

[2] Mobile station - base station system (ms - bss) interface; data link (dl) layer specification. GSM 04.06, http://www.3gpp.org/ftp/Specs/archive/04_series/04.06/0406-840.zip, 1999.

[3] 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.

[4] 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.

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

[6] Multiplexing and multiple access on the radio path. GSM 05.02, http://www.3gpp.org/ftp/Specs/archive/05_series/05.02/0502-8b0.zip, 2003.

[7] 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.

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

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

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

[11] FEDERRATH, H. Protection in mobile communications.

[12] FOX, D. Der imsi-catcher. *Datenschutz und Datensicherheit 26*, 4 (2002), 212–215.

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

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

[15] HARALD WELTE, S. M. Osmocombb - running your own gsm stack on a phone. `http://events.ccc.de/congress/2010/Fahrplan/attachments/1771_osmocombb-27c3.pdf`, 2010.

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

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

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

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

[20] OSMOCOMBB. Project rationale. `http://bb.osmocom.org/trac/wiki/ProjectRationale`, 2012.

[21] OSMOCOMBB. Project rationale. `http://bb.osmocom.org/trac/wiki/ProjectRationale`, 2012.

[22] SAFFERLING, C. Terror and law. *Journal of International Criminal Justice 4*, 5 (2006), 1152–1165.

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

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

[25] SECURITY, H. Imsi-catcher für 1500 euro im eigenbau. `http://www.heise.de/security/meldung/IMSI-Catcher-fuer-1500-Euro-im-Eigenbau-1048919.html`, 2010.

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

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

[28] WEHRLE, D. Open source imsi catcher.

[29] WIKIPEDIA. Cell id. `http://bb.osmocom.org/trac/wiki/MotorolaC123`, 2012.

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

[31] WIKIPEDIA. Equipment identity register. `http://de.wikipedia.org/wiki/IMSI-Catcher`, 2012.

Appendix A.

OsmocomBB

A.1. Installation

The environment used for this project was a Thinkpad X220 Tablet running Xubuntu Linux 11.10. The instructions should work for any other distribution of the Ubuntu product palette.

1. Build libraries must be installed on the operating system to enable compiling libraries.

```
1 sudo apt-get install libtool shtool autoconf git-core
2 pkg-config make gcc wget
```

2. The GNU Arm cross compiler toolchain needs to be installed so the firmware for the Motorola C123 can be built. It will be added as a repository to `sources` so it can be easily removed if it is not required any more.

```
1 sudo add-apt-repository ppa:bdrung/bsprak
2 sudo apt-get update
3 sudo apt-get install arm-elf-toolchain
```

3. The source code needs to be obtained. This can be either done by checking out the latest version of the framework from the developers, or by using the code on the CD.

```
1 git clone git://git.osmocom.org/osmocom-bb.git
```

4. At this point some firmwares had build errors, therefore we will compile only the firmware for the Calypso board used by the Motorola C123. This constraint might not be necessary if a newer version of the framework is used. In the `src` directory of the OsmocomBB framework the build process can be started.

```
make BOARDS=compal_e88
```

5. If a new version of OsmocomBB is used, the extra code from this project must be included in the build. The two files `catcher.c` and `app_catcher.c` must be moved to `osmocom-bb/src/host/layer23/src/misc` and the `Makefile.am` must be edited to include the new code.

```
bin_PROGRAMS = bcch_scan ... cbch_sniff catcher
catcher_SOURCES = ../common/main.c app_catcher.c
```

A.2. Usage

To use a program written in the framework, the Motorola C123 needs to be flashed with the custom firmware. This can be done with the `osmocon` application.

```
cd src/host/osmocon
sudo ./osmocon -p /dev/ttyUSB0 -m c123xor
 ../../target/firmware/board/compal_e88/layer1.compalram.bin
```

After `osmocon` is started and running any application can be started with root privileges.

```
cd ../layer23/src/misc/
sudo catcher
```

A.3. Serial Cable Schematics

A T191 unlock cable used to connect the Motorola C123 can either be obtained by ordering it from one of the mentioned stores or by building it from scratch. The schematics can be seen in Figure A.1.

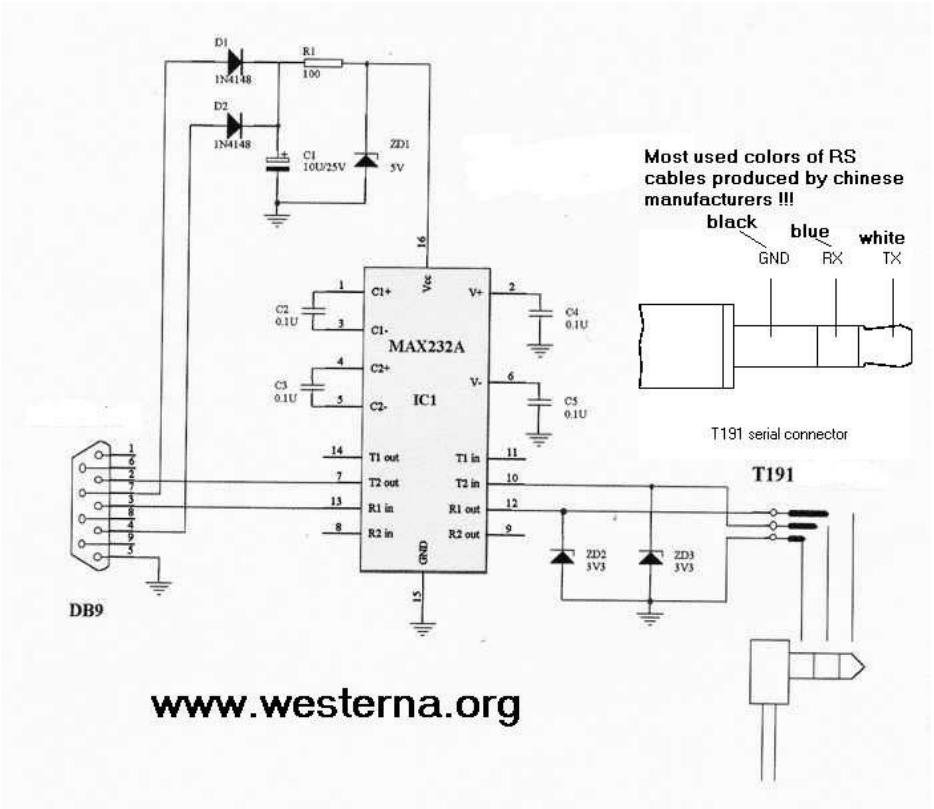


Figure A.1.: Schematics for the T191 unlock cable.

Appendix B.

IMSI Catcher Detection System

B.1. Extextions

B.2. Example Configuration

Appendix C.

System Information

The following pages contain parsed System Information Messages of type 1-4 for reference.

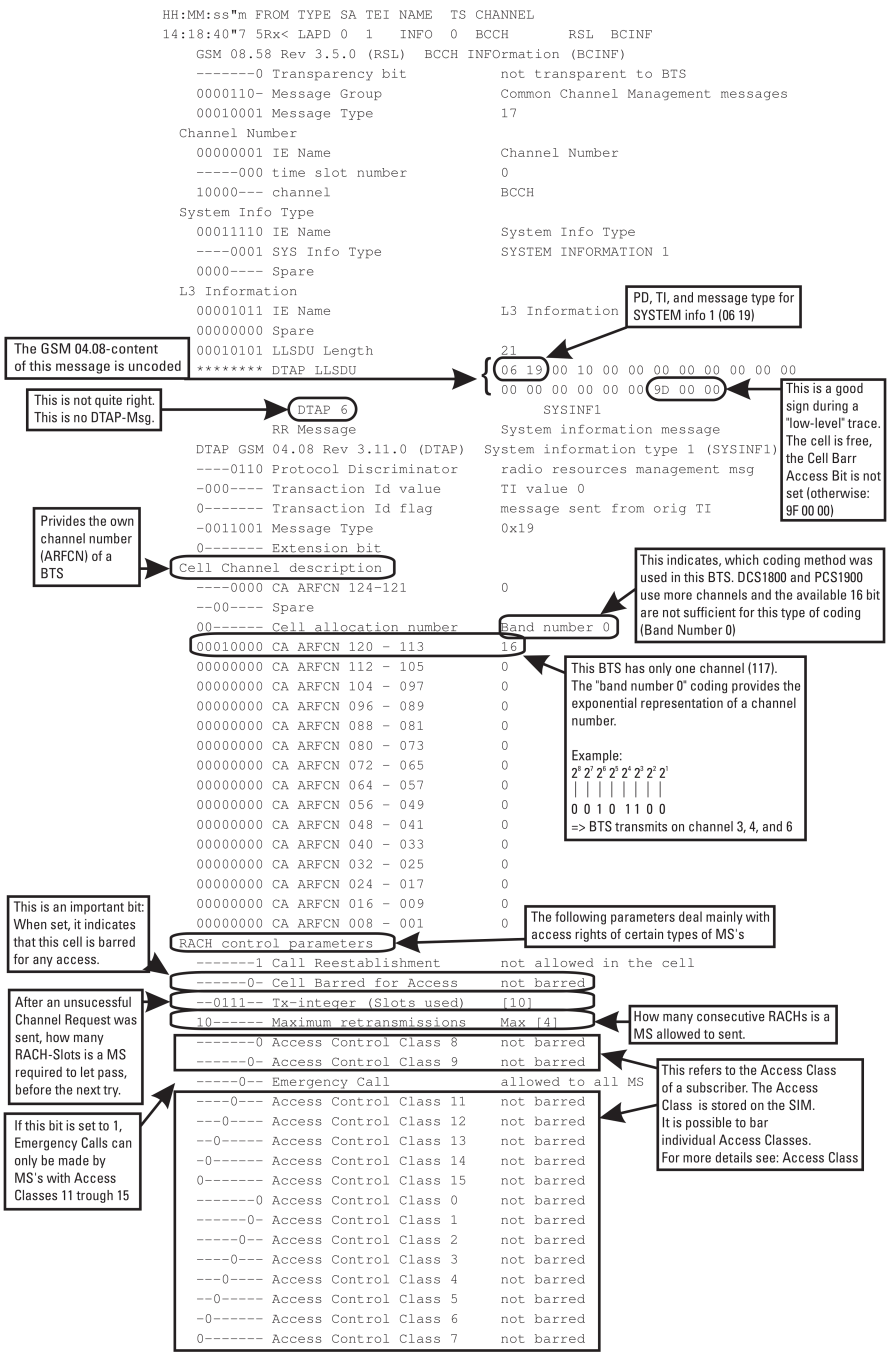


Figure C.1.: System Information 1 Message

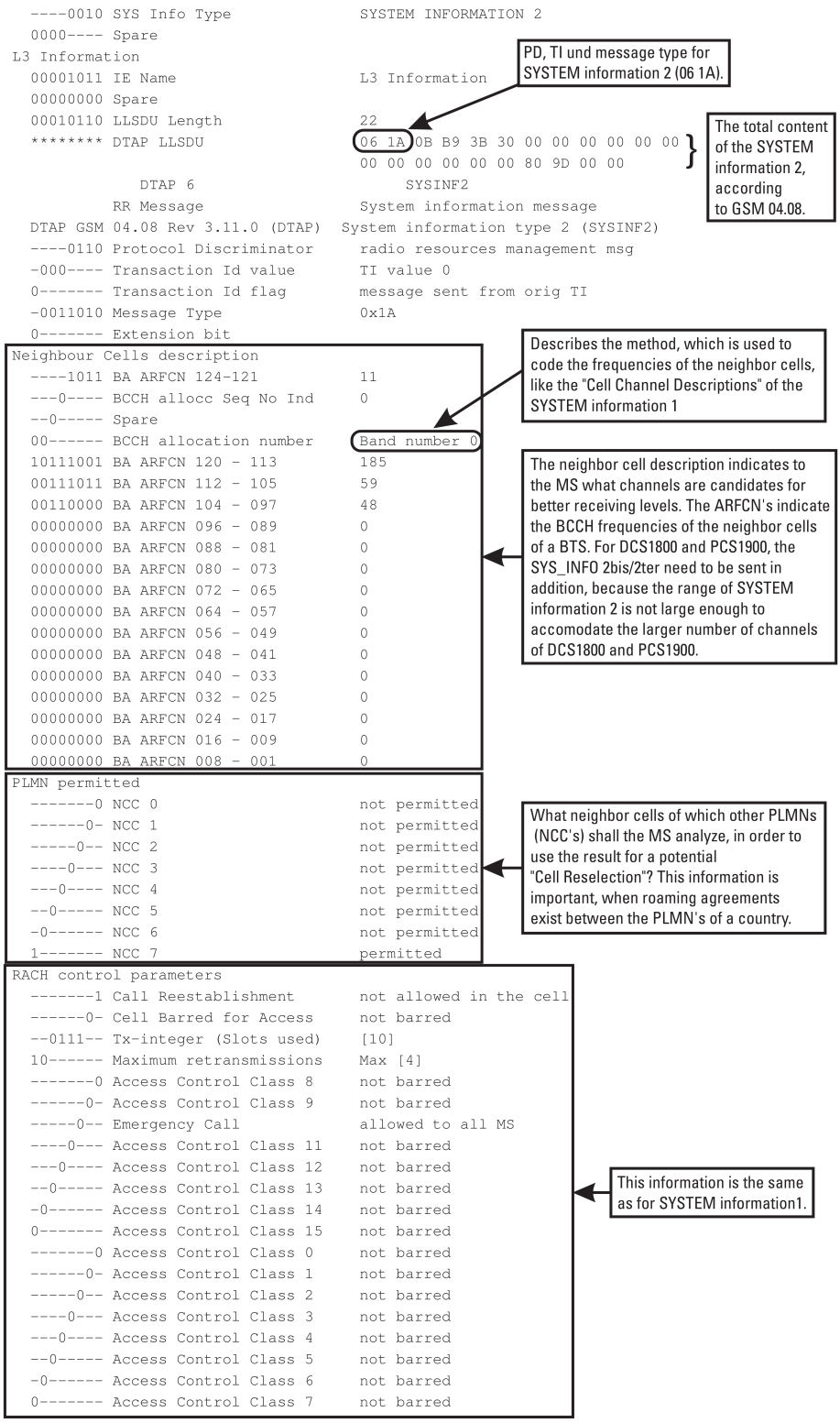


Figure C.2.: System Information 2 Message

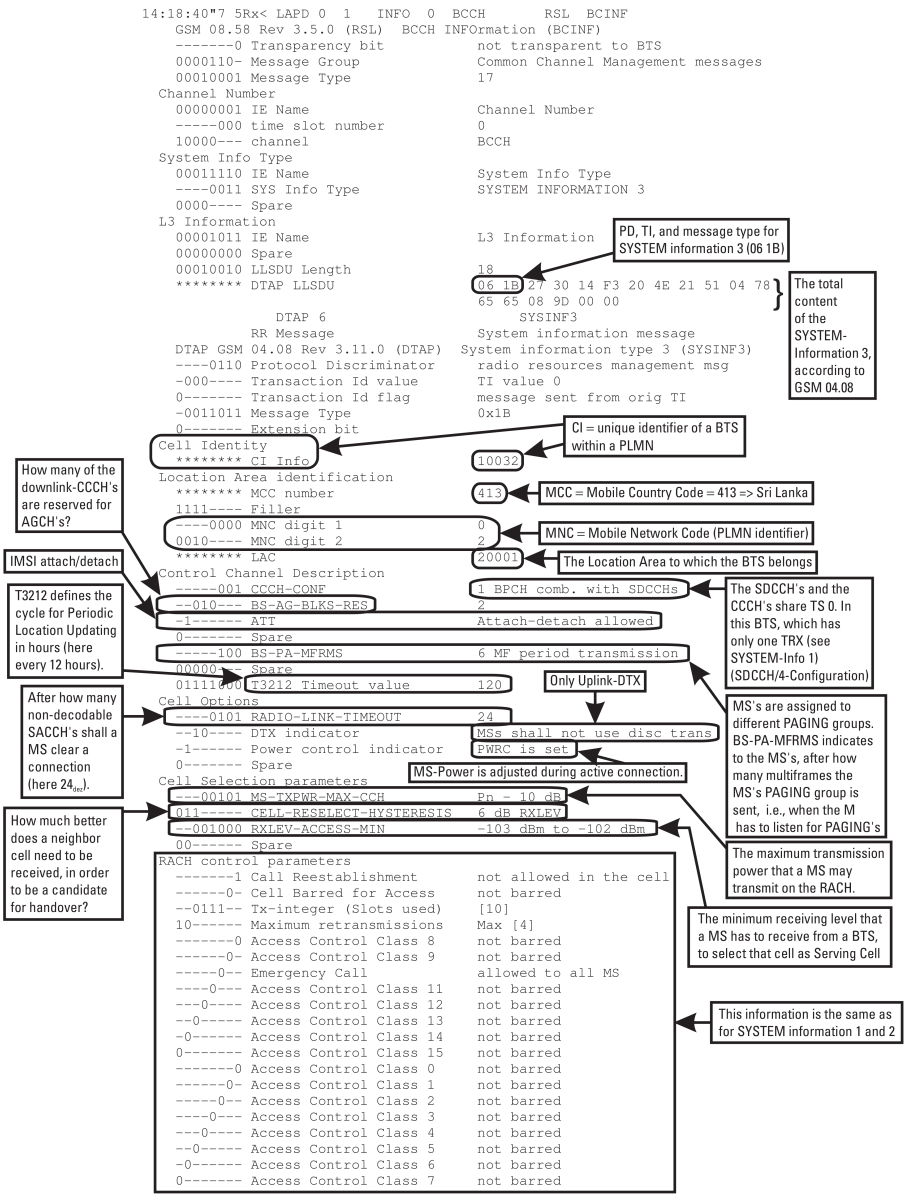


Figure C.3.: System Information 3 Message

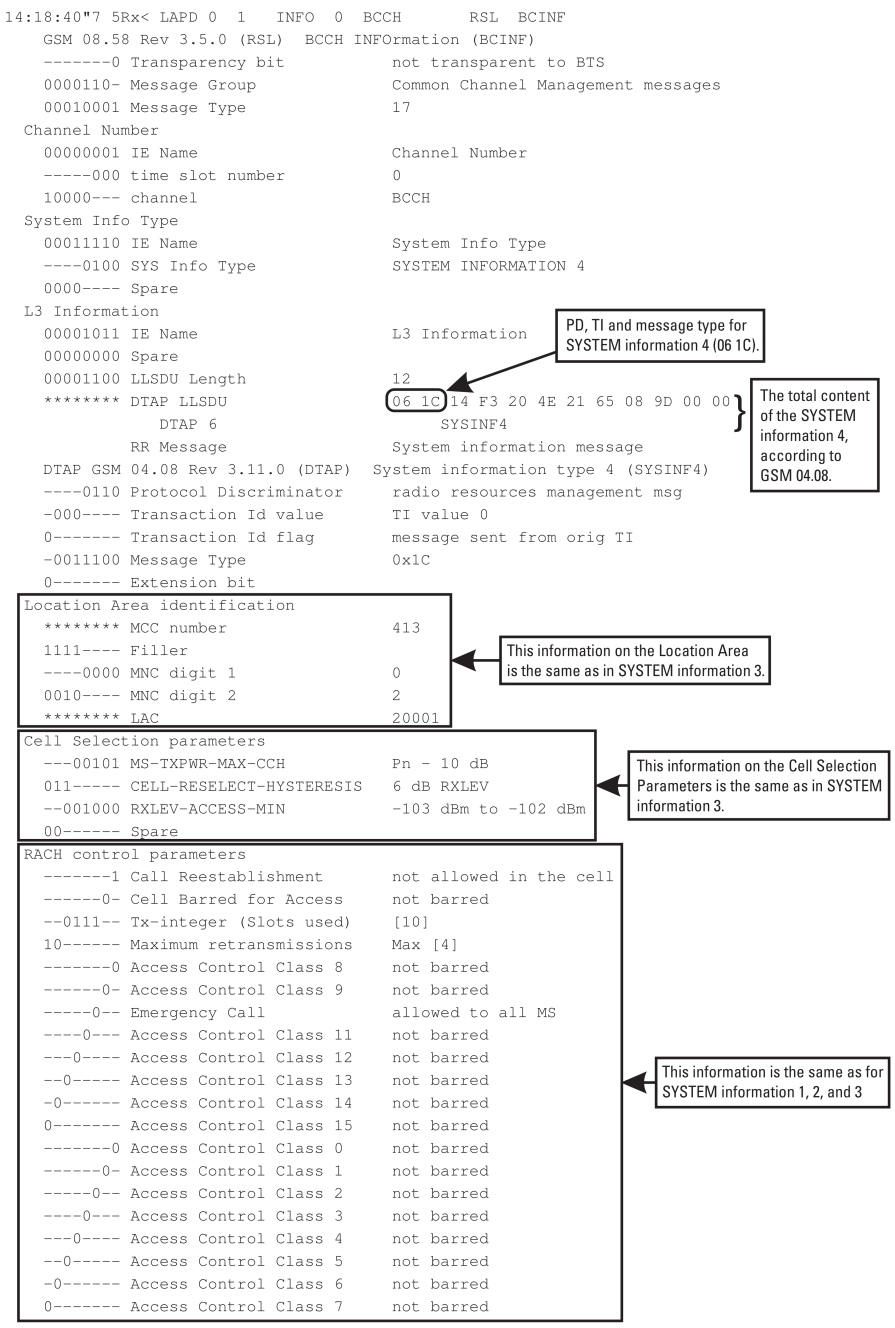


Figure C.4.: System Information 4 Message

Appendix D.
Evaluation Data

D.1. IMSI Catcher Configurations

D.2. ICDS Scans

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