NTNU – Trondheim
Norwegian University of
Science and Technology

Base Station Security Experiments Using USRP

Torjus Bryne Retterstøl

Master of Science in Communication Technology
Submission date: June 2015
Supervisor: Stig Frode Mjølsnes, ITEM

Norwegian University of Science and Technology
Department of Telematics

Title: Base Station Security Experiments Using USRP

Student: Torjus Bryne Retterstøl

Problem description:

A Universal Software Radio Peripheral (USRP) is software-defined radio experimentation device. In particular, mobile network base stations can be built with a USRP connected to a computer that runs the open-source Unix software OpenBTS. Previous work at the department are Ref.[1,2]. This master thesis work will investigate potential passive and active attacks using base station spoofing. First build an IMSI-catcher and find effective modes of operation, for instance by using signal strength, duration and selective jamming. Second, use the experience gained to analyse the IMSI-catcher data collected by Aftenposten (mm.aftenposten.no/mobilspionasje/). Third, find a method to measure the security configuration of operating base-stations (Airprobe). Fourth, try to enhance the attack experiment with communication eavesdropping functionality. Finally, make a proposal for the content of a base station security lab for wireless security (TTM4137) students where they can use their own smartphones in the experimental activities.

[1] Glendrange, Hove and Hvideberg: Decoding GSM. Master thesis, Department of Telematics, NTNU, June 2010.
[2] Maxim Suraev: Denial-of-service attack resilience of the GSM access network. Master thesis, Department of Telematics, NTNU June 27, 2011.

Responsible professor: Stig Frode Mjølsnes

Supervisor: Stig Frode Mjølsnes

Abstract

With a coverage of over 90% of the world's population, the cellular technology standard, GSM, is used by millions all over the world every day. The standard is known to have several security weaknesses. One of the weaknesses is that there is no authentication of the network. IMSI-catchers exploit this weakness to perform various attacks.

The largest Norwegian newspaper, Aftenposten, searched for IMSI-catchers in Oslo in December 2014. The newspaper used two different methods in the search. The conclusion of Aftenposten was that they "most likely" found several IMSI-catchers in Oslo.

In this thesis, IMSI-catchers are studied. An IMSI-catcher is built and configured with an Universal Software Radio Peripheral (USRP) and OpenBTS. Two attacks were performed in an experiment with the IMSI-catcher. The first attack presented is a DoS attack aimed at subscribers of specific operators. The other attack presented is a selective jamming attack, aimed at a specific subscriber. In both the attacks, IMSIs were caught. Both types of attacks were successful. It was found that the effectiveness of the IMSI-catcher depends on the signal strength from the nearby base stations. The experiments indicate that for the proposed IMSI-catcher to be effective, it should be operating and be in the vicinity of the targeted cellphones for several minutes.

Additionally, the investigations made by Aftenposten are analyzed and discussed in this thesis. A technical analysis is performed on all the data Aftenposten acquired in Oslo in December 2014 and the major anomalies found by Aftenposten are discussed in details. From the analysis, it was found that it is possible that Aftenposten observed at least one IMSI-catcher during the investigations. The first articles published by Aftenposten in December 2014 were likely based on misinterpretations of the data the newspaper acquired. It was also discovered a possible bug in the measuring equipment used by Aftenposten. Some of the anomalies discovered by Aftenposten might have been due to misconfigurations of the networks in Oslo.

Sammendrag

Mobiletelefonistandarden GSM dekker over 90 % av verdens befolkning, og er brukt av millioner hver eneste dag. Standarden er kjent for å ha flere sikkerhetshull. Et av disse er at det ikke er autentisering av nettverket. IMSI-catchere utnytter denne svakheten til å utføre flere ulike typer angrep.

Norges største avis, Aftenposten, søkte i desember 2014 etter IMSI-catchere i Oslo. To ulike metoder ble brukt av avisen i søket. Aftenposten konkluderte med at de "høyst sannsynlig" fant flere IMSI-catchere i Oslo.

I denne oppgaven er IMSI-catchere studert. En IMSI-catcher er bygget og konfigurert med en USRP og OpenBTS. To angrep ble utført i et eksperiment med IMSI-catcheren. Et tjenestenektangrep rettet mot alle abonnenter av spesifikke teleoperatører er først presentert. Det andre angrepet er et selektivt tjenestenektangrepangrep rettet mot én abonnent. IMSIer ble fanget i begge angrepene. Begge angrepene viste seg å være suksessfulle. Fra eksperimentene ble det funnet at effektiviteten til IMSI-catcheren er avhengig av signalstyrken fra basestasjoner i nærheten. Eksperimentene indikerer at IMSI-catcheren bør være på, og i nærheten av mobiltelefonene som er målet for angrepet i flere minutter.

I tillegg har undersøkelsene Aftenposten utførte blitt analysert og diskutert i denne oppgaven. En teknisk analyse er utført på alle dataene Aftenposten innhentet i desember 2014. Fra analysen ble det funnet at det er mulig at Aftenposten observerte minst én IMSI-catcher i Oslo under søket. De første artiklene som var publisert av Aftenposten i desember 2014 var sannsynligvis basert på feiltolkninger av dataene Aftenposten innhentet. I tillegg ble det oppdaget en mulig feil i et av måleutstyrene Aftenposten brukte. Noen av avvikene Aftenposten fant kan ha vært på grunn av feilkonfigurasjoner av nettverkene i Oslo.

Preface

This is the final report of the work with the Master's thesis in Information Security in the 10^{th} semester of my Master of Science degree in Communication Technology at the Norwegian University of Science and Technology.

I would like to thank my supervisor and responsible Professor Stig Frode Mjølsnes for much valued guidance and discussions.

I would also like to thank Per Anders Johansen, Andreas Bakke Foss and Fredrik Hager-Thoresen from Aftenposten for providing me with unpublished data and documents, and for lending me the CryptoPhone.

Contents

List of Figures

List of Tables

List of Acronyms

2G Second Generation Wireless Telephone Technology.

3G Third Generation Wireless Telephone Technology.

4G Fourth Generation Wireless Telephone Technology.

ADC analog to digital converter.

AGCH Access Grant Channel.

AP Application Processor.

ARFCN Absolute Radio-Frequency Channel Number.

AuC Authentication Centre.

AV authentication vector.

BA BCCH Allocation.

BCC Base Transition Station Color Code.

BCCH Broadcast Control Channel.

BCH Broadcast Channels.

BP Baseband Processor.

BSC Base Station Controller.

BSIC Base Station Identity Code.

BTS Base Tranceiver Station.

CCCH Common Control Channels.

CCH Common Channels.

CI Cell Identity.

CLI command line interface.

CRH CELL_RESELECT_HYSTERISIS.

CRO CELL_RESELECT_OFFSET.

DAC digital to analog converter.

DCCH Dedicated Control Channels.

DCH Dedicated Channels.

DCS Digital Cellular Service.

DoS denial-of-service.

DSC Downlink Signalling Failure Counter.

EIR Equipment Identity Register.

ETSI European Telecommunications Standards Institute.

FACCH Fast Associated Control Channel.

FCCH Frequency Correction Channel.

FDMA frequency-division multiple access.

GPS Global Positioning System.

GSM Global System for Mobile Communications.

GUI graphical user-interface.

HLR Home Location Register.

HN home network.

HNI Home Network Identity.

IMEI International Mobile station Equipment Identity.

IMSI International Mobile Subscriber Identity.

ITU International Telecommunication Union.

LA Location Area.

LAC Location Area Code.

LAI Location Area Identity.

LTE Long-Term Evolution.

MCC Mobile Country Code.

ME Mobile Equipment.

MIC message integrity code.

MITM man-in-the-middle.

MNC Mobile Network Code.

MS Mobile Station.

MSC Mobile Switching Centre.

MSIN Mobile Subscriber Identity Number.

MSISDN Mobile Station International ISDN Number.

NCC Network Color Code.

NIST National Institute of Standards and Technology.

Nkom the Norwegian National Communication-Authority.

NSM The Norwegian Security Authority.

NTNU Norwegian University of Science and Technology.

OS Operating System.

PCH Paging Channel.

PLMN Public Land Mobile Network.

PST The Norwegian Police Security Service.

PSTN Public Switched Telephone Network.

PT PENALTY_TIME.

RACH Random Access Channel.

RF Radio Frequency.

Rx Reception.

RxL Received Signal Strength.

SACCH Slow Associated Control Channel.

SCH Synchronization Channel.

SDCCH Standalone Dedicated Control Channel.

SDR Software-defined radio.

SIM Subscriber Identity Module.

SMS Short Message Service.

SN serving network.

SNR serial number.

SoLSA Support of Localized Service Area.

SQL Structured Query Language.

SRES Subscriber Result.

SS7 Signalling System no. 7.

T3212 Periodic Location Updating Timer.

TAC Type Allocation Code.

TCH Traffic Channels.

TCH/F Full Rate Traffic Channel.

TCH/H Half Rate Traffic Channel.

TDMA time-division multiple access.

TMSI Temporary Mobile Subscriber Identity.

TO TEMPORARY_OFFSET.

Tx Transmission.

UHD USRP Hardware Driver Repository.

UI user-interface.

UiO University of Oslo.

UMTS Universial Mobile telecommunication System.

USRP Universal Software Radio Peripheral.

VLR Visitor Location Register.

VM Virtual Machine.

VOIP Voice over IP.

XRES Expected Result.

Chapter 1
Introduction

1.1 Motivation

With a coverage of over 90% of the world's population, the over 20 years old technology Global System for Mobile Communications (GSM) is still highly relevant. The technology is used by millions all over the world every day, even though it is known to have several weaknesses. One of the weaknesses of GSM is that there is no authentication of the networks. Thus, it is possible spoof legitimate networks without the users of the technology being able to know.

IMSI-catchers are devices that are used to perform active man-in-the-middle (MITM) attacks against GSM systems. IMSI-catchers masquerades themselves as legitimate Base Tranceiver Stations (BTSs). Because there is no authentication of the network in GSM, Mobile Stations (MSs) will not be able to distinguish these BTSs from legitimate BTS. This leads to MSs connecting to these false base stations. The IMSI-catchers can successfully perform several attacks, such as denial-of-service (DoS) and interception of phone calls.

The weakness with no authentication of the network has been known since the introduction of GSM. Since equipment able to communicate with the GSM system were very expensive when the technology was introduced, this was not seen as a significant threat. With the development of Software-defined radios (SDRs) and related open-source software such as OpenBTS, Airprobe and OsmocomBB, this threat has increased. In 2010 Chris Paget demonstrated the possibility of creating an IMSI-catcher by the use of a SDR and OpenBTS[1]. The IMSI-catcher proposed by Paget was a very cheap device, costing approximately 1500 USD.

In December 2014, the largest Norwegian newspaper Aftenposten published a series of articles where they claimed to have revealed several IMSI-catchers in Oslo, which showed that this threat still is very relevant. The Norwegian Police Security Service (PST) analyzed Aftenposten's claims, and concluded with that based on the data

acquired by Aftenposten, there were no indications of IMSI-catchers in Oslo.

1.2 Scope and Objectives

A USRP was acquired to experiment with attacks exploiting the weaknesses in GSM. Initially, the goal of the thesis was to experiment with this device, resulting in attacks that could be transformed to lab assignments in a wireless security course at Norwegian University of Science and Technology (NTNU). It was decided to configure the USRP to work as an IMSI-catcher, similar to what was done by Chris Paget in 2010.

Aftenposten published the methods they used in their investigation as well as the data they acquired. The investigation made by Aftenposten was highly relevant, and it was decided to analyse this investigation, by using the knowledge obtained by building an open source IMSI-catcher.

Installation and configuration of hardware and software showed itself to be more time-consuming than planned. A wide technical background of GSM and IMSI-catchers had to be obtained, which was time consuming. In addition, the analysis of the data acquired by Aftenposten was not as straightforward as initially assumed. The full set of data and documentation were not obtained until May 2015.

This led to large changes in the initial problem description. It was not enough time to finish all the tasks that initially were assigned. The IMSI-catcher is not enhanced to intercept traffic in this thesis. A lab assignment was not made either. However, installation tutorials of the different software used in the thesis are appended, and the configuration of the IMSI-catcher is written in a tutorial-like manner, which can be used as a guideline for future lab assignments. Instead of measuring the security configuration of BTSs nearby, the configuration regarding IMSI-catchers is measured since this was more relevant for the rest of the thesis.

1.2.1 Objectives

The focus of this thesis is IMSI-catchers. This thesis aims to provide a thorough technical background of IMSI-catchers and the related parts of GSM. This information is then used to implement and configure an IMSI-catcher and analyze the investigation made by Aftenposten. There are four main objectives in this thesis:

1. Measure configurations of nearby BTSs related to IMSI-catchers with USRP and open source software.

2. Build and configure an IMSI-catcher with USRP and open source software.

3. Experiment with IMSI-catcher attacks and test the effectiveness.

4. Analyze the investigations by Aftenposten, including data acquired and methods used to acquire them.

1.3 Methodology

The research methodology used in the work with this thesis is divided in three phases. First a literature study of IMSI-catchers and the related parts of GSM was performed. The study was based on the GSM specifications published by European Telecommunications Standards Institute (ETSI), scientific textbooks and scientific papers.

The second phase consisted of configuring and experimenting with software and hardware and testing in practical experiments. An IMSI-catcher was built with an USRP and OpenBTS.

The third phase was a technical data analysis. The analysis was based on the knowledge obtained from the literature study and building and experimenting with the IMSI-catcher. The main tools used in the analysis were MYSQL and Google Maps.

1.4 Contributions

This thesis gives a technical study of IMSI-catchers, both theoretical and practical. The main contribution of the thesis is an analysis of the IMSI-catcher investigations Aftenposten performed in Oslo. It has been performed a technical description and analysis of the data Aftenposten acquired, and the methods used to acquire the data. The major anomalies found by Aftenposten are analyzed and explained in details.

Additionally, an open source IMSI-catcher is proposed and tested. A method of obtaining system information messages from BTSs is included.

1.5 Related Work

1.5.1 Open Source IMSI-catcher

There exist several related work to building false BTSs with SDRs. Chris Paget first demonstrated this in 2010[1]. Paget built an IMSI-catcher with a USRP and

OpenBTS, similar to what is done in this thesis. However, this thesis presents a more effectively configured IMSI-catcher than what was demonstrated by Paget in 2010.

Song et al. showed in 2012 an implementation of a false BTS with a SDR[2]. The device was realized with an AM3517 Experiment Kit and a GSM Radio Frequency (RF) device. The GSM protocol stack was implemented on the AM3517 Experiment Kit. The effectiveness was tested in an experiment where both selective jamming and IMSI-catch attack were performed. The topic and goal were similar as in this thesis, but different hardware and software were used.

Hadžialić et al. showed in 2014 an implementation of an IMSI-catcher, realized with an USRP and OpenBTS[3], very similar to the one proposed in this thesis. Hadžialić et al. did not test the device in a practical experiment. The proposed IMSI-catcher in this thesis is tested in experiments. This thesis also provides a much more detailed explanation of how to setup and configure the IMSI-catcher.

Glendrange et al. showed how a rogue BTS could be implemented with the USRP 1 and OpenBTS in 2010[4]. They showed that interception of phone calls between multiple MSs camped on the cell of the same rogue BTS was possible. They did not configure the device to work effectively as an IMSI-catcher, as is done in this thesis.

1.5.2 Analysis of Aftenposten Investigations

Aftenposten and the company they hired, Delma, performed analyses of the data they acquired during their investigations[5, 6]. PST also performed an analysis and published a ”status report” in April 2015[7]. The analysis performed in this thesis is the first independent, technical analysis performed, and aims to give a more detailed technical analysis of the incidents than the other analyses performed.

1.6 Outline

This thesis is divided into 6 chapters. The outline is as follows.

Chapter 2 Presents a general foundation of GSM, including the parts of the standard that are relevant to fully understand the content of this thesis. IMSI-catchers are explained in details.

Chapter 3 Presents data broadcasted by BTSs on the radio interface. The methods used to acquire the data as well as the data are described and discussed.

Chapter 4 Presents an IMSI-catcher made and configured in this thesis, by the use of USRP and OpenBTS. The effectiveness of the IMSI-catcher is tested in a practical experiment.

Chapter 5 Provides an analysis of the investigations made by Aftenposten in Oslo. Both the methods and the data acquired are analysed.

Chapter 6 Presents a conclusion of the work done in this thesis and possible further work.

Chapter 2
GSM

This chapter includes a general background of the parts of the GSM technology that are necessary in order to understand the content of this thesis. A description of IMSI-catchers is included as well as a description of the GSM PLMNs in Norway.

2.1 Overview

Global System for Mobile Communications (GSM) is a cellular technology standard that was developed by European Telecommunications Standards Institute (ETSI). The standard defines a set of protocols and technologies used for communication between a cellular phone and the Public Switched Telephone Network (PSTN). As of today, GSM networks cover more than 90% of the world's population[8]. GSM is a Second Generation Wireless Telephone Technology (2G).

2.2 Cellular Structure

The GSM standard follows the Public Land Mobile Network (PLMN) architecture developed by the International Telecommunication Union (ITU) in 1981[9, 10]. GSM was the first system to ever follow this architecture. Some other systems that today follow it are Universial Mobile telecommunication System (UMTS) and Long-Term Evolution (LTE). The PLMN architecture uses a cellular structure.

In a cellular structure, the coverage of a radio transmitter and receiver in the network, or Base Tranceiver Station (BTS) (see Section 2.3.2), defines a cell. The network is divided into a significant number of cells, where each cell in the same cluster operates on different frequencies. These frequencies can be reused in other clusters. A cluster typically consists of seven neighboring cells.

The cellular structure is illustrated in Figure 2.1. The numbers in the cells indicate the frequency each cell use. The figure is a very simplified cellular structure, as in modern PLMNs the cells have different sizes and shapes based on the needs of the

network. The cells will typically be larger in rural areas and smaller in areas with high population density. The decisions of the structure of the cells in the cellular network are chosen by the PLMNs themselves.

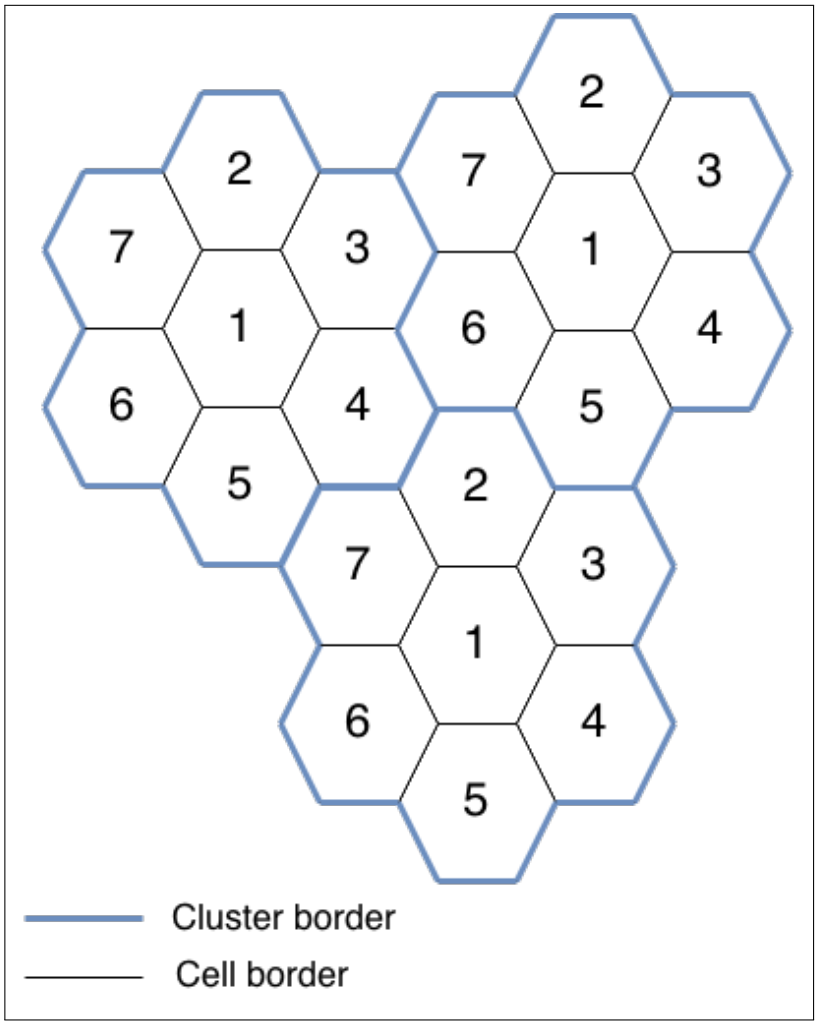


Figure 2.1: Cellular Structure

2.3 GSM Architecture

The architecture of GSM is shown in Figure 2.2. The most important components illustrated in the figure will be described in this section.

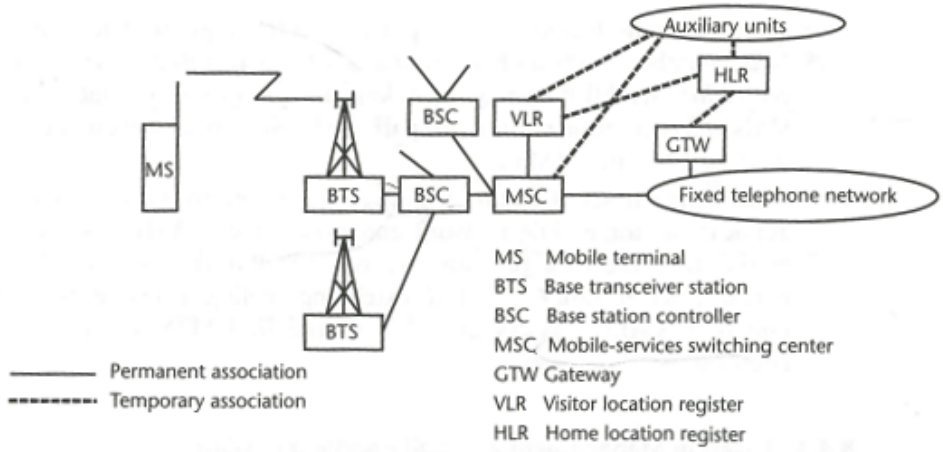


Figure 2.2: Architecture of GSM from [10]

2.3.1 Topology

The topology of a GSM network is illustrated in Figure 2.3.

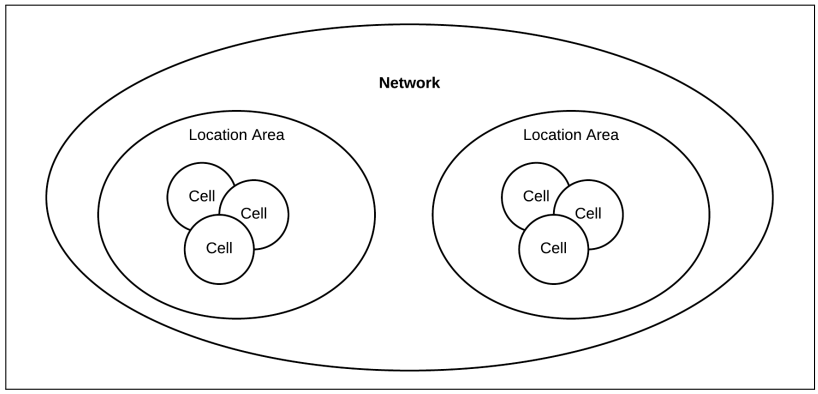


Figure 2.3: Topology of a GSM network

The network in the topology is identified by the Mobile Network Code (MNC), the Location Areas (LAs) are identified by the Location Area Identity (LAI) and the cells are identified by the Cell Identity (CI). The LAI is a concatenation of the Mobile Country Code (MCC), the MNC and the Location Area Code (LAC). The values are described in greater details later in this chapter and are, amongst others, used to locate subscribers.

2.3.2 Components of GSM

The most important components of GSM are described in this section[9, 10].

Mobile Station (MS)

The Mobile Station (MS) is the combination of hardware and software used by a subscriber to communicate with the network. The MS is the combination of a Mobile Equipment (ME) and a Subscriber Identity Module (SIM).

The ME is the physical communication device, while the SIM is a portable smart card that is inserted to a ME, but not restricted to that ME. Modern MEs usually have two processors. One used for applications running on the ME, called the Application Processor (AP), and one processor that performs all radio operations, called the Baseband Processor (BP).

The ME contains an International Mobile station Equipment Identity (IMEI), which is a unique identifier of the ME. The structure of IMEI is shown in Figure 2.4[11]. The Type Allocation Code (TAC) is an eight digit number that uniquely identifies the model and manufacturer of the ME. The serial number (SNR) is six digit and is the serial number of the ME. The spare digit is a check digit calculated by Luhn's formula. The purpose is to mitigate incorrect entries in the Equipment Identity Register (EIR). The spare digit should always be "0" when the IMEI is sent on the network.

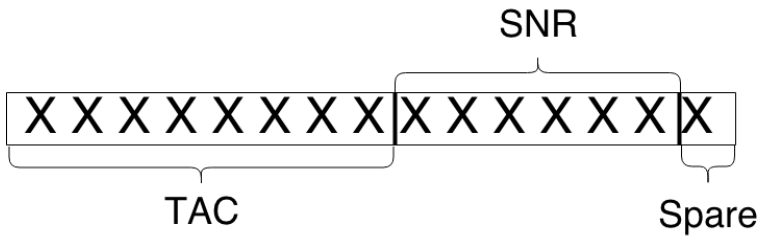


Figure 2.4: The structure of IMEI

Subscriber Identity Module (SIM)

As mentioned earlier, the SIM is a smart card inserted in a ME. The SIM contains two very important parameters, the International Mobile Subscriber Identity (IMSI) and the 128-bit permanent secret key (Ki) used in authentication and encryption described in Section 2.7[12]. The IMSI is a unique identifier of the subscriber in the network. The structure of the IMSI is shown in Figure 2.5.

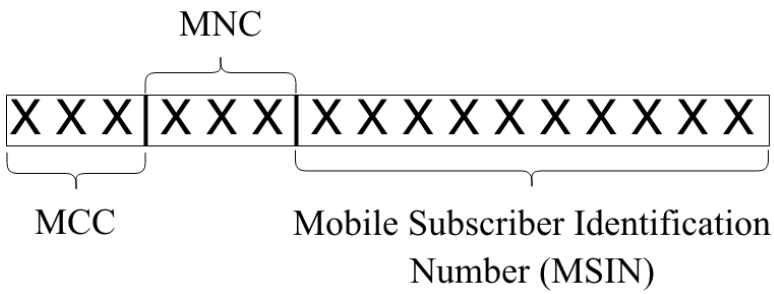


Figure 2.5: The structure of IMSI

While the IMEI identifies the ME, the IMSI identifies the SIM, and thus also the subscriber.

MCC is a three digits unique identifier of the country the SIM belongs to. The MCC of Norway is 242. **MNC** is either a two or three digits unique identifier of the PLMNs within a country. The Mobile Subscriber Identity Number (MSIN) is a number of maximum ten digits that identifies a subscriber within this PLMN.

Base Tranceiver Station (BTS)

The BTS provides the radio interface (the Um interface) in GSM. This is the interface between the MS and the BTS. The BTS transmits and receives signals from the MSs, andit provides multiplexing and encryption. In addition to the Um interface support, the BTS also supports the network interface (the Abis interface) when communicating with the Base Station Controller (BSC). A BTS controls a single cell in GSM and is usually located in the centre of that cell. The cell size is defined by the transmitting power of the BTS.

The BTS is identified by a Base Station Identity Code (BSIC). The BSIC is unique in the cluster and is a 6-bit value, where the first 3 bits are the Network Color Code (NCC) and the 3 next bits are the Base Transition Station Color Code (BCC).

The cell the BTS controls is identified by a 2-byte CI that is generally unique on the network[13]. There are multiple ways of assigning CIs to the different cells of a network[14]. The way the assignment is done is decided by the different PLMN themselves.

Base Station Controller (BSC)

The BSC is directly connected to multiple BTSs and monitors and controls these BTSs through the Abis interface. The number of BTSs connected to a BSC is

operator specific and can be between tens to hundreds. The main tasks of the BSC is to administrate the frequencies of the interconnected BTSs, control the BTSs and provide handover functionality between the BTSs that are connected to the BSC. Each BSC typically controls a single LA. The LA is uniquely identified by the 16-bit LAC within a PLMN.

Mobile Switching Centre (MSC)

The Mobile Switching Centre (MSC) is a telephone switching exchange providing the interface between the cellular network and the PSTN. It is responsible for the routing of calls originating from the PLMN and calls terminating in the PLMN. The MSC controls several BSCs and supports handover between BTSs within these BSCs. It also supports handover between BSCs connected to differenty MSCs.

Home Location Register (HLR)

The Home Location Register (HLR) is a database storing subscriber information. This information includes the Mobile Station International ISDN Number (MSISDN), IMSI, the authentication key of the subscriber, information about supplementary services, the current Visitor Location Register (VLR) of the subscriber and the location of the MS. The location is stored as a combination of the Home Network Identity (HNI) and the LAI the MS is currently located at.

Visitor Location Register (VLR)

The VLR is a database that contains data that are relevant for all the MSs connected to a serving MSC. It contains both permanent data and temporary data. The permanent data are, amongst others, the IMSI, MSISDN, identity of the HLR and authentication key. The Temporary Mobile Subscriber Identity (TMSI) is stored at the VLR. This is a temporary identity of the subscriber used to provide confidentiality of subscribers over the Um interface. It is described in greater details in Section 2.7.3. The VLR also supports the MSC in call establishment, authentication of MSs, forwarding of Short Message Services (SMSs) etc.

Authentication Centre (AuC)

The Authentication Centre (AuC) is connected to the HLR and communicates only with the HLR over a so-called H-interface. It stores secret keys and algorithms used for authentication of the MSs and encryption of traffic on the Um interface.

Equipment Identity Register (EIR)

The EIR stores the IMEIs of all the MEs connected to a network.

2.4 Physical Channels

Both frequency-division multiple access (FDMA) and time-division multiple access (TDMA) are used in GSM[10]. The frequency spectrum used in GSM is divided into carriers of 200 kHz each. This is the FDMA used in GSM. Separate carriers are used for transmission and receiving in the GSM system. The combination of two carriers is called Absolute Radio-Frequency Channel Number (ARFCN), where one of the carriers are used for uplink (from MS to BTS) communication and one is used for downlink communication (from BTS to MS). The calculation of frequencies corresponding to ARFCN n in GSM 900 is shown in Equation 2.1. Similar calculations exists for all the GSM bands. Each of the carriers are time divided into eight TDMA timeslots, which together is called a TDMA frame. The duration of each timeslot is 0.577 ms, and the duration of a frame is 4.615 ms.

$$f_{uplink} = 890.0 + 0.2 \cdot n \tag{2.1a}$$

$$f_{downlink} = f_{uplink} + 45 \tag{2.1b}$$

2.5 Logical Channels

The information sent over the Um interface in GSM are sent on logical channels. The logical channels are organized on the TDMA multiframe, which is 26 TDMA frames. One logical channel may occupy some or all timeslots in the multiframe. It is a hierarchy of channels in GSM, shown in figure Table 2.1. The two types of logical channels in GSM are Common Channels (CCH) and Dedicated Channels (DCH).

Table 2.1 Logical channel hierarchy in GSM

CCH					
BCH			CCCH		
FCCH	SCH	BCCH	PCH	RACH	AGCH

(a) Hierarchy of Common Channels

DCH				
DCCH			TCH	
SDCCH	SACCH	FACCH	TCH/F	TCH/H

(b) Hierarchy of Dedicated Channels

2.5.1 Common Channels (CCH)

There are two types of CCH in GSM, the Broadcast Channels (BCH) and the Common Control Channels (CCCH).

Broadcast Channels (BCH)

The three types of BCH are Frequency Correction Channel (FCCH), Synchronization Channel (SCH) and Broadcast Control Channel (BCCH). FCCH is used for frequency correction. SCH is used for frame synchronization. BCCH is used to broadcast system parameters in system information messages. The system information messages contain information about the cell and the network such as CI, LAC, MNC and MCC. The system information messages also contain parameters used for cell and network optimization, such as CELL_RESELECT_OFFSET (CRO), PENALTY_TIME (PT), TEMPORARY_OFFSET (TO), that are relevant for cell selection and reselection. Cell selection and reselection are described in Section 2.6. The system information messages that are relevant for this thesis are described in Table 2.2.

Table 2.2 System Information Messages in GSM

Message	Content
SI Type 1	Hopping related information, such as this cell's ARFCNs. Information of control of RACH.
SI Type 2	ARFCNs of neighbors (BA List). Information of control of RACH.
SI Type 2bis	Extended neighbor list. Information of control of RACH. Optional.
SI Type 2ter	Extended neighbor list. Optional.
SI Type 2 Quarter	3G neighbor cell information. Optional.
SI Type 3	LAI, CID, and other various information about cell. Cell selection parameters. Information of control of RACH.
SI Type 4	LAI, CID, and other various information about cell. Information of control of RACH.

Common Control Channel (CCCH)

There are three types of CCCH, the Paging Channel (PCH), the Random Access Channel (RACH) and the Access Grant Channel (AGCH). The PCH is used to page MSs. This is used to inform the MS that it is about to receive incomming traffic. The paging messages are sent to all the BTSs in the LA the MS is located. The RACH is used uplink, from the MS to the BTS. It is typically used to inform the

network that the MS is about to initiate a call or send a text message. The AGCH is used to set up a connection between the MS and the BTS.

2.5.2 Dedicated Channels (DCH)

There are two types of DCH in GSM, Dedicated Control Channels (DCCH) and Traffic Channels (TCH)

Dedicated Control Channels (DCCH)

The three types of DCCH are Standalone Dedicated Control Channel (SDCCH), Slow Associated Control Channel (SACCH) and Fast Associated Control Channel (FACCH). The SDCCH is used for exchange of signaling information between the MS and the BTS related to call establishment, location updating, and other management functions. SMS is also sent on the SDCCH. The SACCH is used for timing advance and power control on the downlink. On the uplink, the channel is used for transfer of field strength measurements. The FACCH is always associated with a TCH and is used to transmit urgent signaling messages.

Traffic Channels (TCH)

There are two types of TCH, Half Rate Traffic Channel (TCH/H) and Full Rate Traffic Channel (TCH/F). TCH/H occupies one timeslot every second frame, while TCH/F occupies every timeslot in a frame.

2.6 Idle Mode

The idle mode in GSM is the state of the MS when it is switched on, but does not have a DCH allocated. This is for instance when the MS is switched on, but is not in a call or sending or receiving SMSs messages. When in idle mode, the MS needs to choose an appropriate cell to camp on in order to to communicate with a GSM PLMN[15, 16].

2.6.1 Cell Camping

The MS has to camp on a cell and tune to the control channels of that cell. Cell camping makes it possible for the MS to receive system information and paging messages on the PCH from the PLMN. By camping on a cell, it is possible for the MS to initiate outgoing calls and receive incoming calls.

There are five constraints that have to be satisfied for an MS to camp on a cell:

1. The cell should be associated with the selected PLMN. The MNC and the MCC broadcasted by the cell should be identical as the values for the selected PLMN.

2. The cell should not be barred. The PLMN can choose to not allow MS to camp on a particular cell. In these cases, the cell is barred.

3. The cell should not be in a LA that is forbidden for roaming.

4. When communicating with the cell, the radio path loss between MS and BTS should be below a certain threshold.

5. The cell should not be a Support of Localized Service Area (SoLSA) exclusive cell that the MS is not subscribing to. SoLSA is a mechanism that can provide special tariffs or service features for certain subscribers. It will not be discussed in greater details in this thesis, but more information can be found at [17].

2.6.2 Selection and Reselection

Selection and reselection are procedures that are performed while the MS is in idle mode. These procedures ensure that the MS camps on a cell where it can reliably decode the data on the downlink, and there is a high probability that the uplink traffic will reach the BTS. Cell selection is the cell camping procedure performed immediately after a MS is turned on, while reselection is performed continuously in idle mode.

Criteria for Selection and Reselection

Cell selection and reselection are determined by two criterias calculated by the ME, based on values broadcasted by the BTSs in system information messages over the BCCH.

- C1 - the path loss criterion parameter
- C2 - the reselection criterion

Cell Selection

The MS keeps track of an average of the signal strength of BTSs operating on some monitored frequencies. There are two ways to determine what frequencies that should be monitored, *normal cell selection* and *stored list cell selection*. Normal cell selection should be used when the MS does not know whether GSM 900 or Digital Cellular Service (DCS) 1800 is used, which is the case in Norway.

In normal cell selection, the MS has to search through all possible ARFCNs to find a suitable cell to camp on, that is 174 for GSM 900 and 374 for DCS 1800. C1 are calculated for the 6 cells with the strongest Received Signal Strength (RxL).

In stored cell selection, the BCCH Allocation (BA) list broadcasted by the last BTS the MS camped on is used. The BA list is a list of ARFCNs neighbors use. The neighbors are BTSs nearby. The BA list is broadcasted in the system information messages.

Cell selection using this BA list can only be used when the MS is switched off and switched on in the same location, as the list only contains BCCH carriers close to the last BTS the MS camped on. C1 values are calculated for the 6 cells with strongest RxL in the BA list. If stored cell selection is not successful, the MS will perform normal cell selection.

The goal of the selection procedure is to camp on a suitable cell. The MS will select the cell that satisfies the constraints in Section 2.6.1 and has the largest C1 value amongst the cells that are monitored.

The C1 parameter is calculated in the following way by the MS:

$$\mathrm{C1} = (A - \max(B, 0)) \tag{2.2}$$

where
A: Received Level Average - RXLEV_ACCESS_MIN
B: MS_TXPWR_MAX_CCH - P
RXLEV_ACCESS_MIN: Minimum received level at the MS required for access to the system. This value is chosen and broadcasted by the BTS. It is a 6-bit value. The range is linear, where 0 means less than -110 dBm and 63 means greater than -48 dBm.
MS_TXPWR_MAX_CCH: Maximum Transmission (Tx) power level an MS may use when accessing the network. This value is broadcasted by the BTS.
P: Maximum Radio Frequency (RF) output power of the MS.
All the values are measured in dBm.

Cell Reselection

The reselection procedure is performed continuously by the MS in idle mode. The MS reads BCCH information every 5 second to calculate the average of the RxL for the 6 strongest non-serving cells in the BA list broadcasted by the serving cell, in addition to the serving cell. This information is then used to calculate C1 and C2 as described in Equation 2.2 and Equation 2.3. The following five events can trigger a cell reselection:

1. C1 parameter indicates that the cell path loss has become too high. The cell path loss is too high when the C1 parameter is a negative value for 5 or more seconds.

2. There is downlink signaling failure. A downlink signaling failure happens when the value of the Downlink Signalling Failure Counter (DSC) is less than or equal to zero. The value of the DSC is broadcasted by the BTS and is chosen by the PLMN. Whenever the MS successfully decodes a message on the PCH, the DSC is increased by one. If the decoding is not successful, the DSC is decreased by 4[16].

3. The current serving cell has been barred.

4. Another cell in the same LA has a higher C2 value than the current serving cell for at least 5 seconds and a cell reselection has not been performed in the last 15 seconds, or another cell in another LA has a C2 value at least CELL_RESELECT_HYSTERISIS (CRH)[1] dBm greater than the current serving cell for at least 5 seconds.

5. The MS unsuccessfully tries to perform a random access attempt to the cell a number of times.

The reselection criterion C2 is defined by:

$$\text{C2} = \begin{cases} \text{C1} + \text{CRO} - \text{TO} * \text{H(PT - T)} & \text{PT} \neq 11111 \\ \text{C1} - \text{CRO} & \text{PT} = 11111 \end{cases} \tag{2.3}$$

where
For non-serving cells:

$$H(x) = \begin{cases} 0 & x < 0 \\ 1 & x \geq 0 \end{cases} \tag{2.4}$$

For serving cells:

$$H(x) = 0 \tag{2.5}$$

CRO: A positive or negative offset used to encourage or discourage MSs to reselect to that cell. The value can be set in the range [0,63] in 2 dBm steps, e.g. 0=0 dBm,

[1] CRH is a value that prevents a MS to repeatedly change between multiple LAs because the MS is positioned between the LAs. The value is measured in dBm.

1=2 dBm etc.
PT: When a cell is put in the list of strongest carriers, a timer is started at the MS. This timer expires after PT and during this time, C2 is given a negative offset. This prevents a fast moving MS from selecting the cell. The PT value can be set to a value in the range [0,31] where each step represents 20 seconds, i.e. 0 = 20 sec, 1 = 40 sec etc. PT value of 31 indicates that the TO should be ignored and C2 = C1 - CRO.
TO: The amount of negative offset given to C2 when the time not yet has reached PT. The value is defined as a number in the range [0,7], where 0 to 6 represents 0 to 60 dBm, and 7 represents infinity.

All values are measured in dBm. CRO, PT and TO are broadcasted by the BTS in system information messages on the BCCH. They are not mandatory values, and if they are not set, then C2 = C1. The mapping between the broadcasted values and the values used in the calculation of C1 and C2 is done by the ME.

2.7 Security Features in GSM

The three most important security features in GSM are as follows[18]:

1. Authentication of the subscriber.

2. Subscriber identity confidentiality by the use of temporary identities, TMSIs.

3. Encryption of radio link providing communication confidentiality.

2.7.1 Authentication in GSM

The purpose of the authentication in GSM is to make unauthorized use impossible. In addition, authentication implies that subscribers are protected against impersonation. The authentication procedure is also used to set the ciphering key used for confidentiality[18, 19]. The network is not authenticated in GSM, which is a security issue that will be discussed later.

There are four events that trigger an authentication procedure. It will be triggered when subscriber related information is changed in the VLR or HLR, for instance due to a location update. It is also triggered when the MS accesses a service, for example initiating a call. The third trigger of the authentication procedure is when the MS

first accesses the network after being turned on. The fourth trigger is if there is a cipher key sequence number mismatch.

Location Update

A location update is the most common trigger for an authentication procedure. Location updating is the action taken by the MS to provide location information to the PLMN[20]. The location update procedure is triggered when the MS reselects to a cell with a different LAI than the previous cell the MS was camped on, or when a MS manually reselects to a new cell.

The location update procedure is also triggered when the Periodic Location Updating Timer (T3212) is expired. The T3212 timer is a value broadcasted by the BTS in the system information messages and is used for network optimization. The minimum value of this timer is one decihour (6 minutes) while the maximum value is 255 decihours. Every time an MS reselects to a cell with a different LAI than the previous cell, the T3212 timer will be reset. Whenever the MS reselects to a cell with the same LAI as the previous cell, the timer value will be set to the remainder of the previous timer modulo the new T3212 timer broadcasted in the new cell[15]. The location update procedure is illustrated in Figure 2.6.

Authentication Procedure

The authentication procedure in GSM checks whether the subscriber has access to the permanent secret key Ki or not. If the subscriber can prove that she has access to this key, the subscriber is authenticated. The secret key is stored only in the SIM and the AuC and never moved. The full authentication procedure triggered by a location update is illustrated in Figure 2.6.

Authentication in GSM involves several components, the SIM, the VLR, the MSC and the HLR/AuC. The authentication is performed as challenge-response. When the authentication procedure is initiated, the MS must provide the network with its TMSI or IMSI, so that the network knows which subscriber should be authenticated.

The MS will first provide the TMSI to the MSC. The MSC forwards the TMSI to the VLR. If the TMSI is not stored in the VLR, the network will request and receive the IMSI from the MS. The MSC/VLR then sends the IMSI of the subscriber to the HLR. The HLR forwards the IMSI to the AuC.

The AuC generates a random 128-bit number called RAND. RAND and the Ki corresponding to the IMSI are used as input parameters in the authentication function, A3, and the session key derivation function A8. These two functions are implemented at the AuC and the SIM.

The A3 function produces a 32-bit value, Expected Result (XRES). The A8 function produces the ciphering key, Kc. RAND, Kc and XRES are then sent to the MSC. The MSC forwards the RAND value to the MS.

The SIM in the MS then performs the same procedures as the AuC did, i.e. the A3 and A8 function. The output of the A3 function performed at the SIM, Subscriber Result (SRES), is sent to the MSC. The MSC then checks if SRES=XRES. If the two values are identical, the subscriber is authenticated and the subscribers TMSI is encrypted with Kc and sent to the MS. The Kc is then used for encryption of further communication between the MS and the BTS.

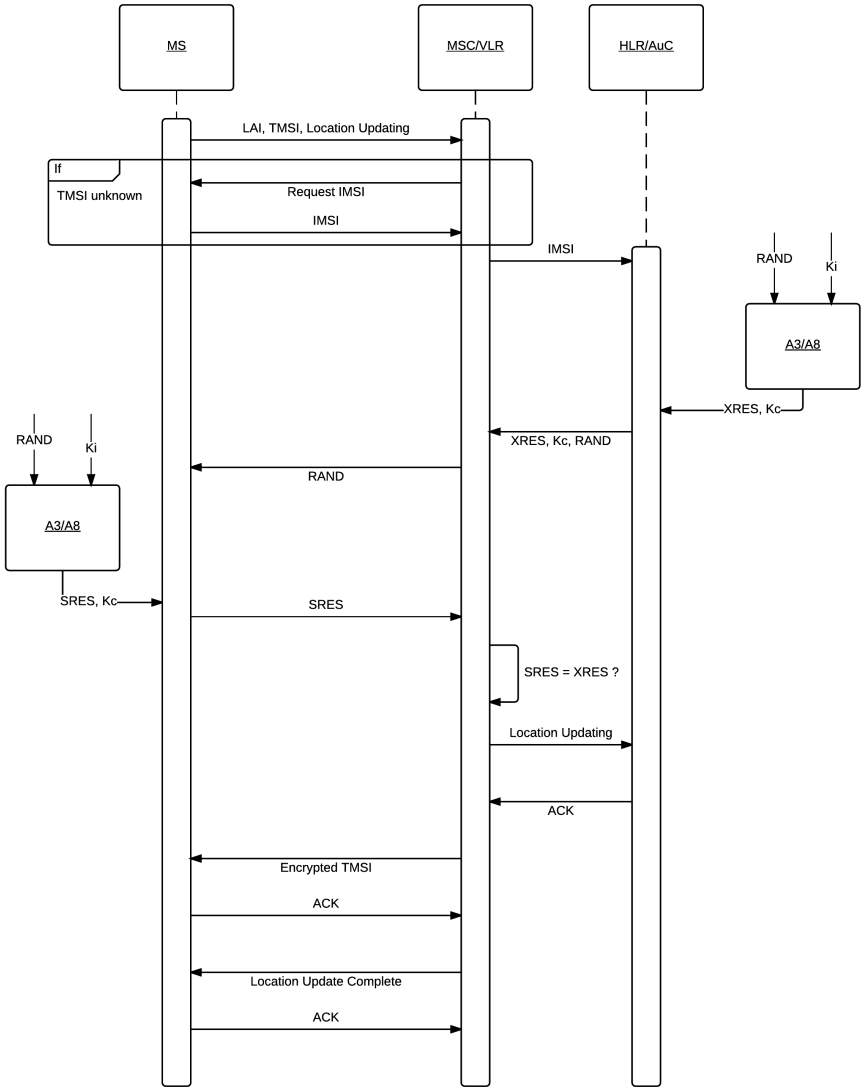


Figure 2.6: Message sequence chart of location update in GSM.

2.7.2 Encryption in GSM

The GSM standard provides methods for encrypting the Um interface in GSM. The other interfaces in GSM are not encrypted. Thus end-to-end encryption does not exist in GSM.

The secret key used for encryption of the Um interface, Kc, is generated as a byproduct of the authentication procedure. The key is 64-bit and is changed every time an authentication procedure is performed.

There exist three different stream ciphers used for encryption of the Um interface that are standardized in GSM, A5/1, A5/2 and A5/3. A5/1 was the first encryption algorithm in GSM. As the standard became popular, another weaker algorithm was needed to get global export licenses for the GSM equipment. A5/2 was developed for that purpose.

Both A5/1 and A5/2 were confidential, only known to the manufacturers of the GSM equipment. Since they are implemented in all SIMs, reverse engineering was possible. The two algorithms were reverse engineered in 1999[21]. There exist ciphertext-only attacks that break the A5/2 encryption in milliseconds[22]. In 2010, a practical attack against A5/1 was described. The attack could be performed with the tool *Kraken*, which computed the session key, Kc, by the use of rainbow tables[23].

A5/3 is an adaption of a variation of the KASUMI block cipher used in UMTS. The KASUMI cipher uses 128-bit keys while the A5/3 uses 63-bit keys. There does not exist practical attacks against the GSM A5/3 cipher today.

2.7.3 Subscriber Confidentiality in GSM

As the IMSI is unique for each subscriber, an attacker could track subscribers if their IMSI were sent in plaintext on the Um interface. GSM mitigates such an attack by the use of TMSIs. TMSIs are temporal identities for each subscriber that often are changed. The IMSI should only be sent when it is necessary, such as the first time the MS registers to the network. In all other cases, the TMSI should be sent over the Um interface. The size of the TMSI is four bytes.

2.7.4 Security Weaknesses in GSM

There are several weaknesses in GSM that could be exploited by attackers[12]. The list below describes the biggest weaknesses.

- No authentication of the network. False BTS, or IMSI-catcher attacks are possible. These kind of attacks are described in Section 2.9.

- Sensitive information such as keys used for encryption over Um interface are sent unencrypted and unauthenticated over Signalling System no. 7 (SS7) [24].

- Some security algorithms are confidential. Security through obscurity is a violation of Kerckhoffs principle[25] and is considered a bad practice in information security, advised against by for instance National Institute of Standards and Technology (NIST)[26].

- The size of the keys used for encryption are short enough that it is possible to retrieve them by performing brute-force or rainbow table attacks.

2.8 UMTS Interoperability

UMTS is a Third Generation Wireless Telephone Technology (3G) standard, and a successor of GSM. In order to enhance the network coverage of the UMTS system, it was decided to implement GSM interoperability[27]. GSM BTSs can be used within the UMTS network. Thus, it is possible to perform a specific IMSI-catcher attack against UMTS. For this reason, only the parts that are needed to understand the attack are included in this section.

2.8.1 Security Features in UMTS

UMTS fixed some of the flaws related to GSM security. The following features were added:

- Mutual authentication is used in UMTS, which means that the network is authenticated by the MS.

- Message integrity code (MIC) is used in the authentication procedure, ensuring integrity.

- KASUMI cipher used with a key size of 128-bits. When GSM BTSs are used, the keys are halved.

2.8.2 Athentication in UMTS with GSM Interoperability

Authentication in UMTS is more complicated than in GSM since authentication of the network is included. The A3 and A8 functions in GSM are replaced with five functions in UMTS, the authentication functions f_1 and f_2, and the key generating function f_3, f_4 and f_5.

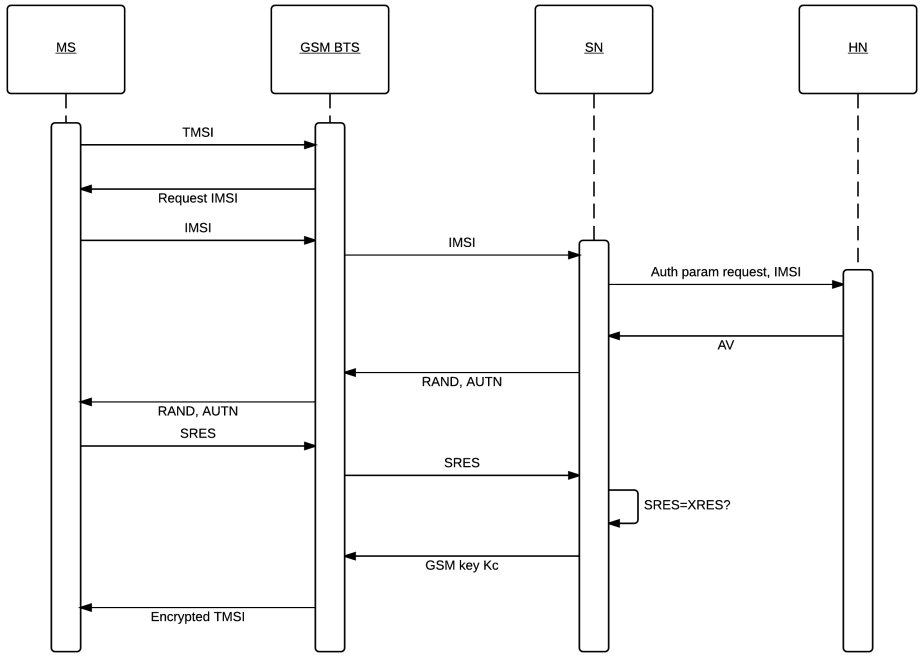


Figure 2.7: Message sequence chart of authentication in UMTS with GSM BTS.

Figure 2.7 shows the authentication procedure in UMTS with a GSM BTS. The MS send its TMSI to the BTS. The BTS may request IMSI from the MS. The IMSI is sent to the serving network (SN), which forwards it to the home network (HN). The HN answers with the authentication vector (AV), which is calculated from the key K and a 128-bit random value RAND. The AV consists of a concatination RAND, the integrity key KI, the ciphering key CK, XRES and the authentication token AUTN. RAND and AUTN are sent to the GSM BTS, which forwards the values to the MS. The MS computes SRES based on RAND and AUTN and sends it to the SN. The SN checks whether SRES equals XRES or not. If it does, MS is authenticated, and TMSI is sent encrypted.

2.9 IMSI-Catchers

IMSI-catchers are devices used to perform active man-in-the-middle (MITM) attacks against GSM. An IMSI-catcher is a false BTS. The device behaves as a BTS, but is not part of the infrastructure of a real PLMN. It broadcasts messages that are interpreted as legitimate GSM messages, and the device operates on a frequency allocated for GSM that MSs can interpret. IMSI-catchers exploit the fact that there is no authentication of the network in GSM. MSs will simply camp on the cell that broadcast correct MCC and MNC values and satisfies the conditions described in Section 2.6, whether it is a legitimate cell or not.

An IMSI-catcher was first described, and patented in Europe by Rohde & Schwarz in 1993[28]. The simplest form of IMSI-catchers are simply able to read the IMSI of MSs nearby, hence the name. More advanced forms are able to perform active MITM attacks to intercept phone calls and text messages. There are several uses for IMSI-catchers today. IMSI-catchers can for instance be used to track individuals, perform denial-of-service (DoS) attacks[29][2], deliver spam text messages, attack the BP on MEs[30] and intercept calls and text messages of individuals.

Figure 2.8: The IMSI-catcher Stingray II, produced by Harris Corp. The image is from [31].

Figure 2.8 shows an image of an IMSI-catcher produced by Harris Corp. called "Stingray". It is widely used by law enforcement in the USA[32]. The Stingray is sold in two versions, the Stingray and the Stingray II. In 2008, the original Stingray was

sold for 75,000 USD while the Stingray II was sold for 148,000 USD[33].

2.9.1 Catching IMSIs

As described earlier, the simplest form of IMSI-catchers simply catches IMSIs. By catching IMSIs, it is possible to track the location of individuals and log which individuals that are present at a location at a given time.

IMSIs can be requested over the SDCCH. The SDCCH is usually initiated by an authentication procedure, for instance by a location update initiated by the MS. An IMSI-catcher can also request IMEIs on the SDCCH in the same way as requesting IMSIs. These messages are, however, not included in the message sequence charts in this section. A SDCCH can also be initiated by paging the MS, but to do this, an attacker would need to know the TMSI or the IMSI of the MS.

The message sequence chart in Figure 2.9 explains how a simple IMSI-catcher is catching IMSIs. The MS initiates a location update procedure with the IMSI-catcher. The IMSI-catcher requests the IMSI of the MS, and then sends a location update reject message. The IMSI-catcher has obtained the IMSI and the MS reselects to a valid cell nearby.

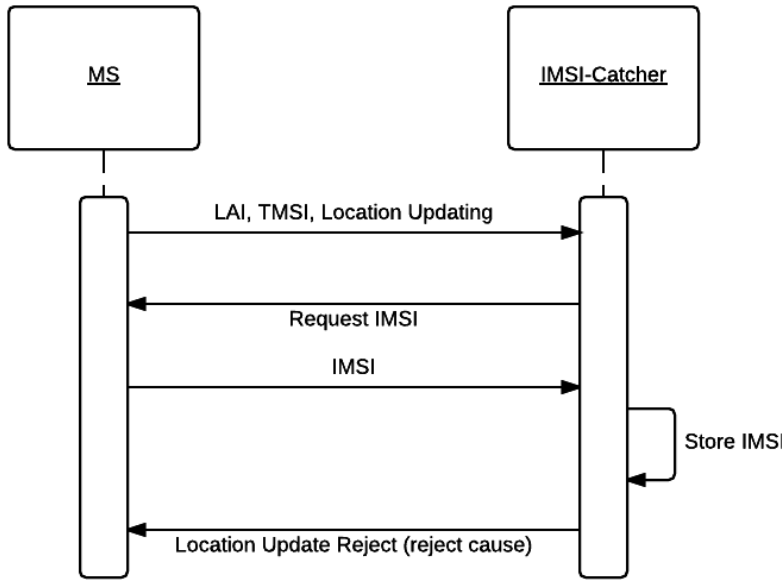


Figure 2.9: Message sequence chart of catching IMSIs with IMSI-catcher

2.9.2 Denial of Service

By allowing MSs to camp on the IMSI-catcher without relaying calls and text messages to a PLMN, the IMSI-catcher performs a DoS attack against the MSs that camps on the cell. The MSs will not have any service, even though the ME will tell the user it is connected to its home network.

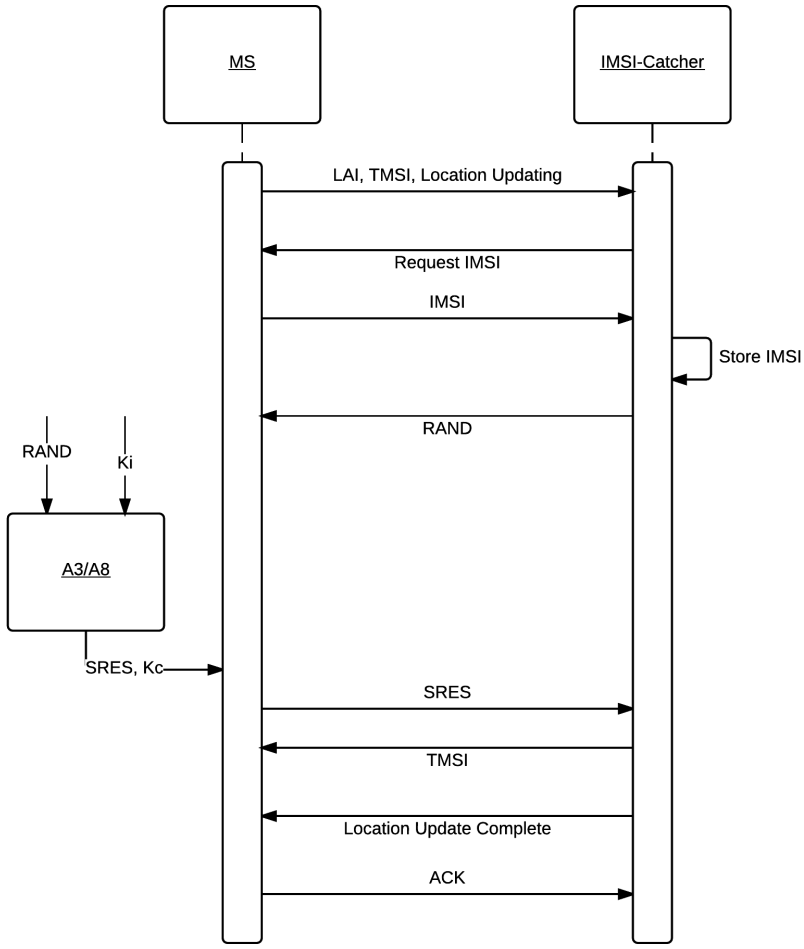


Figure 2.10: Message sequence chart of denial-of-service attack with an IMSI-catcher

The message sequence chart in Figure 2.10 explains how it works. The MS initiates a location updating procedure. The IMSI-catcher requests the IMSI from the MS. It replies to the IMSI with RAND. The MS calculates Kc and SRES and distributes it

to the IMSI-catcher. The IMSI-catcher responds with a TMSI. As far as the MS is concerned, it is now camping on a legitimate cell.

DoS attacks can be performed by using the same LAC as the surrounding legitimate cells. As long as the MS camps on the cell of the IMSI-catcher, the service of the MS is denied. However, in this case, the IMSI of the MS is not caught immediately, since a location update procedure is not performed.

2.9.3 Interception of Traffic

More sophisticated attacks performed by IMSI-catchers is to relay calls and text messages to the real network, and thus being able to intercept all traffic. It is a full MITM attack where the IMSI-catcher will act as a BTS towards a legitimate MS and a MS towards a legitimate BTS. This section describes two different ways to perform this kind of attack in GSM and one way in UMTS.

Intercepting with Ciphering Suppression

One possible way of intercepting phone calls and text messages by the use of IMSI-catchers is to forward all authentication data to and from the MS and ensure that encryption is turned off between the MS and the IMSI-catcher, and between the IMSI-catcher and the BTS. The message sequence chart in Figure 2.11 illustrates how it works[34].

Depending on the configuration of the network, this method will not always work. Some networks do not allow A5/0, no encryption on Um interface, to be used. Thus in these networks the location updating and authentication procedure will fail when the IMSI-catcher responds with *Ciphering Mode Complete (fault)*.

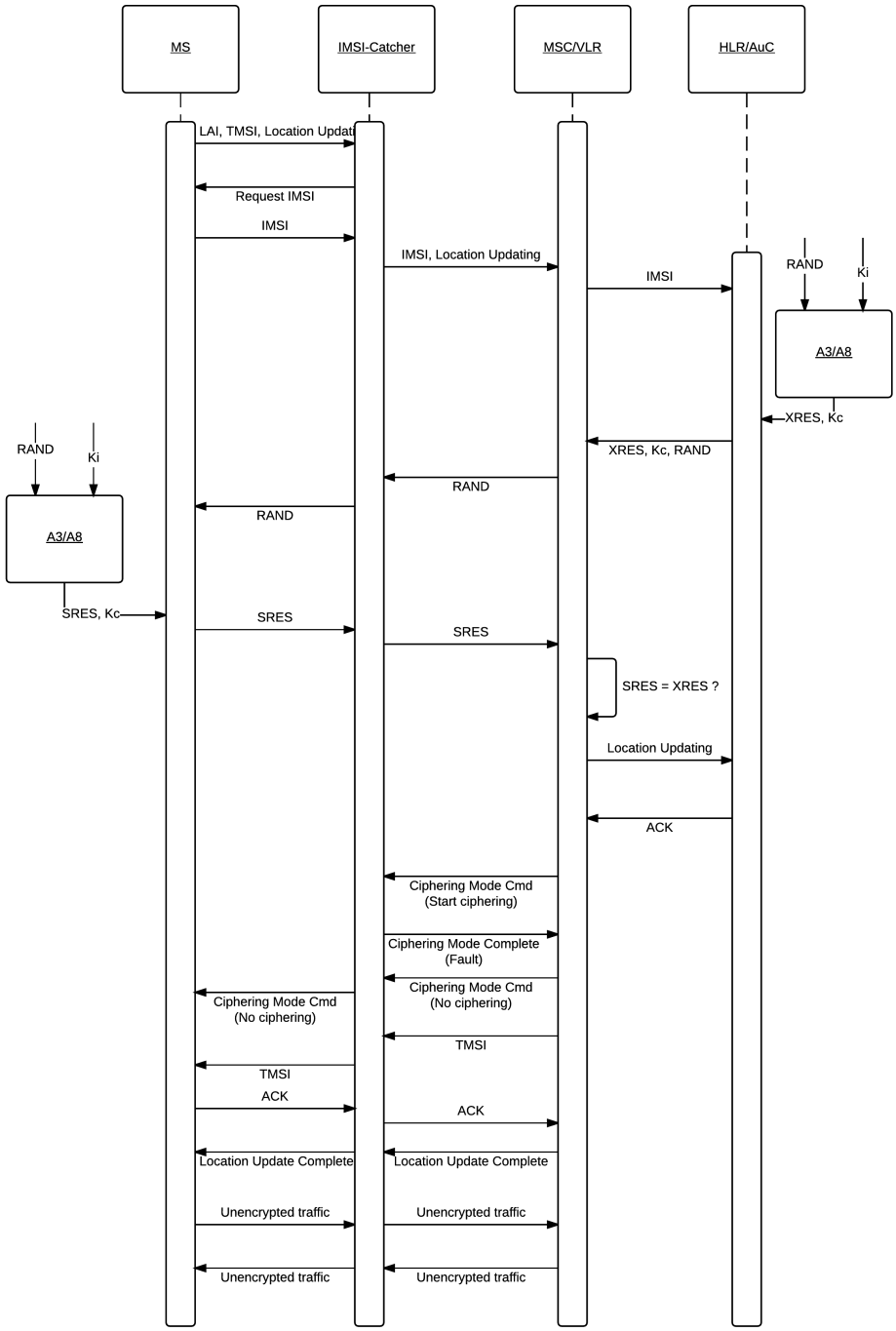


Figure 2.11: Message sequence chart of interception of calls and text messages by suppressing encryption with an IMSI-catcher

This attack would not succeed in Norway. Pönsgen found in [35] that the Norwegian networks only support A5/1 or A/3 encryption. A5/0 is not supported in Norwegian networks.

Intercepting with SIM-card at the IMSI-catcher

Another possible way to intercept phone calls and text messages with an IMSI-catcher is to use the IMSI-catcher with a SIM-card[36]. The IMSI-catcher turns off encryption on the Um interface between the MS and the IMSI-catcher. Calls and text messages originating from the MS are then forwarded onto the network by the IMSI-catcher, encrypted under Kc of the SIM-card of the IMSI-catcher.

In this mode, the originating phone number will be different from the phone number of the MS. The originating phone number will be the phone number of the SIM-card in the IMSI-catcher. However, it is possible for the IMSI-catcher to turn off originating phone number, such that for a receiver of a call, the phone number will be unknown.

This method can only be used to intercept phone calls and text messages originating from the MS. Incoming calls cannot be intercepted with this method because the subscriber has no connection to the PLMN. The message sequence chart in Figure 2.12 illustrates how the attack works. It is only possible to intercept one MS at the time since a regular connection is established with the SIM card of the IMSI-catcher.

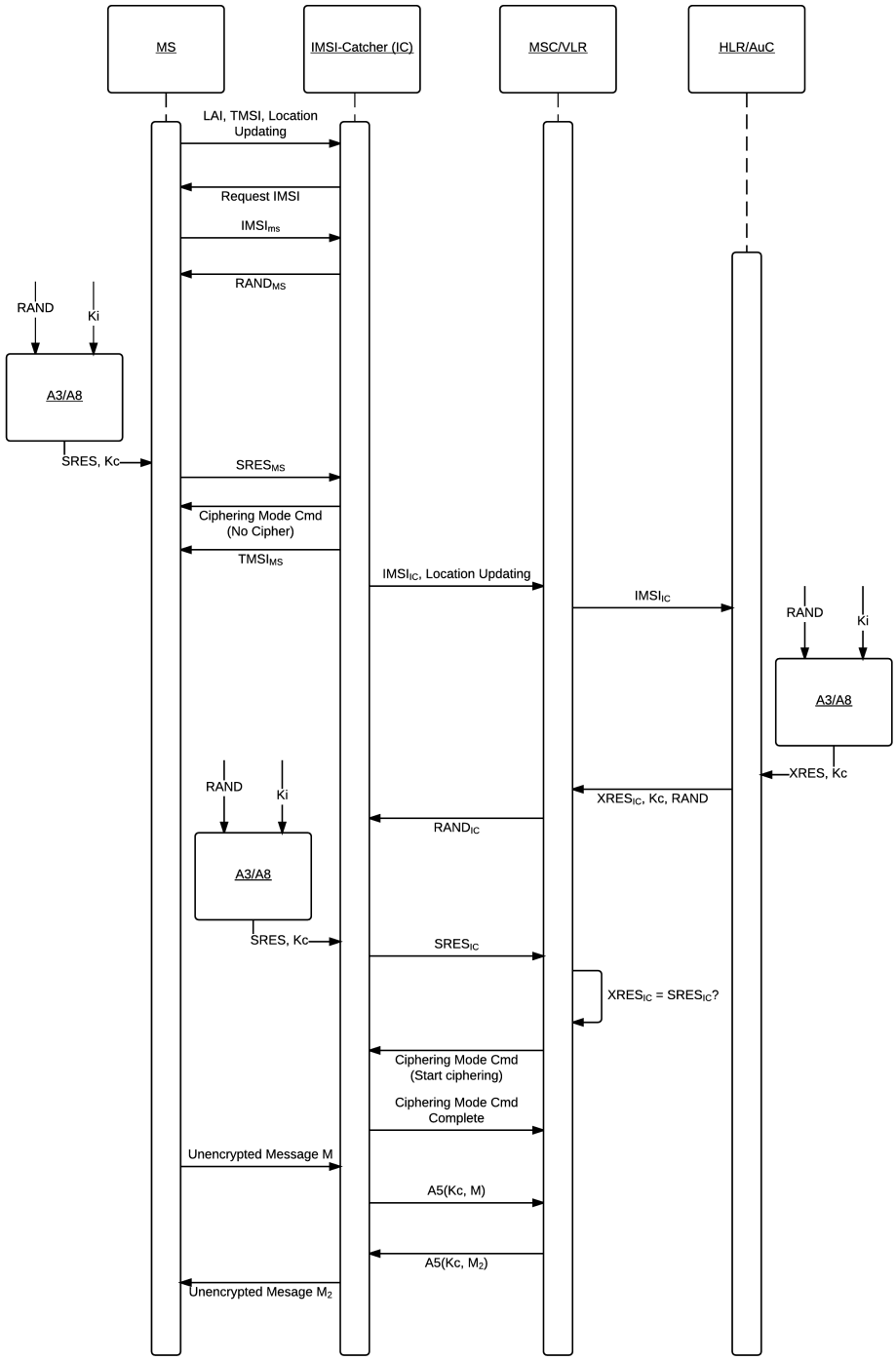
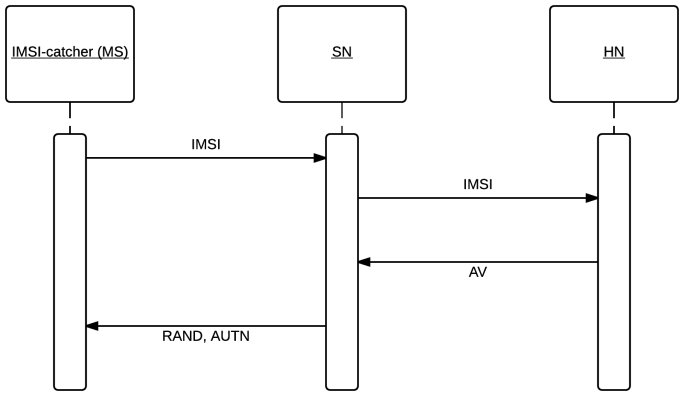


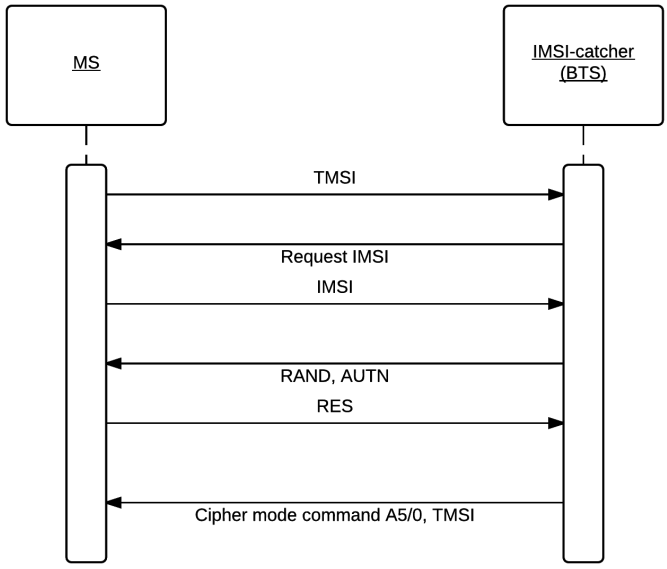
Figure 2.12: Message sequence chart of interception of calls and text messages by using a SIM-card at the IMSI-catcher

UMTS Attack

Mutual authentication is used in UMTS. The network is thereby authenticated in UMTS. The interception and DoS IMSI-catcher attacks described so far are not successful in UMTS.



(a) Step 2



(b) Step 3

Figure 2.13: IMSI-catcher attack in UMTS

As described in Section 2.8, UMTS supports the use of GSM BTSs. This makes it possible to perform an attack with an IMSI-catcher or a false GSM BTS described by Meyer et al. in 2004[27].

The attack consists of three steps. First the TMSI or the IMSI of the target has to be found. Then the IMSI-catcher impersonates the victim towards a legitimate BTS. The attacker will then receive AUTN and RAND from the network. Subsequently, the attacker will masquerade as a GSM BTS and send AUTN and RAND to the victim, which then will compute SRES. The IMSI-catcher will then turn off encryption, and forward messages to the legitimate network by the use of a SIM card at the IMSI-catcher.

The first step of the attack can be performed identically as the attack shown in Figure 2.9. Message sequence charts describing the second and third step are illustrated in Figure 2.13.

2.9.4 Characteristic Operations

There are several characteristic operations that are typically performed by IMSI-catchers in order to be as efficient as possible[37][3]. Some of them are described below.

Spoofing a PLMN

An IMSI-catcher will typically spoof a real PLMN. It does this by broadcasting the same MNC and MCC as the real PLMN it want to spoof. The MSs that camps on the cell of the IMSI-catcher will get no indications that they are not connected to a legitimate BTS. It will appear as if the MS camps on a cell that belongs to the PLMN the SIM subscribes to.

Selecting an ARFCN

The IMSI-catcher needs to choose what ARFCN to operate on. The ARFCN should be one that is used in the country the IMSI-catcher is used. For instance, in Norway, the IMSI-catcher should choose an ARFCN that is in GSM 900 or DCS 1800.

Aditionally, the chosen ARFCN should be unused by BTSs nearby, to increase signal quality and avoid interference with legitimate BTSs nearby. The most effective choice for an IMSI-catcher is however not to choose a random unused ARFCN. As described in Section 2.6, BTSs broadcast a list of ARFCNs that neighbor BTSs operate on, the BA list. The MSs use this list in the reselection procedure. Thus the ARFCN that the IMSI-catcher operates on should appear in this list for MSs to relect to it. The most effective choice of an ARFCN for an IMSI-catcher would thus be to choose

an ARFCN that is broadcasted as a neighbor from the closest legitimate BTS and that is not used by the PLMN or the legitimate BTS operating on the ARFCN does not have reception at the location of the IMSI-catcher.

Another tactic used by IMSI-catchers is to use a random unused ARFCN and use a jammer to jam all downlink frequencies. MSs will then perform a cell selection procedure, and possibly search through all possible ARFCNs assigned to the chosen PLMN. This way the IMSI-catcher may be found, and MSs will select to the cell if the C1 value is large. The use of a jammer might be easier to detect since the users may be aware of the signaling loss while the jammer is used.

Jam 3G and 4G

Some MSs can be configured to prefer 3G and Fourth Generation Wireless Telephone Technology (4G) connection over 2G. This means that the MSs with this configuration would camp on 3G or 4G cells if possible in the area. The IMSI-catcher would thus not be able to perform attacks against these MSs as they would not reselect to the cell of the IMSI-catcher, since the IMSI-catcher operates on a 2G network.

To mitigate this and enhance the attack, an attacker could jam all 3G and 4G frequencies in a close vicinity of the IMSI-catcher. All the MSs nearby would then move down to 2G, and would be able to camp on the cell of the IMSI-catcher.

Increase C2 Value

Since the C2 value calculated at the MS is used to decide if an MS should reselect or not, the value could be increased by the IMSI-catcher in order to force MSs to reselect to the cell. Transmitting with high power increases the RxL at the MSs, and will thus increase the C2 value. The IMSI-catcher could also broadcast a large CRO value, which directly increases the C2 value.

Forcing Location Update

In order to catch IMSIs, intercept traffic and jam traffic, MSs have to perform an authentication procedure on the cell of the IMSI-catcher. As described in Section 2.7.1, the most common way of triggering an authentication procedure is by a location updating procedure. The easiest way for an IMSI-catcher to catch IMSIs and enable interception is to make sure that MSs camps on the cell of the IMSI-catcher and initiates location updating procedures.

The most effective way of forcing a location update is for the IMSI-catcher to use a different LAC than the nearby, legitimate BTSs. The MSs reselecting to the cell of the IMSI-catcher will in these cases perform a location update procedure immediately, such that the IMSI-catcher can request their IMSIs.

Another trick an IMSI-catcher can use to force location update is to set the T3212 to a small value, preferably the smallest, i.e. 6 minutes. This is not as effective as using a different LAC, since the MSs have to be camped on the cell of the IMSI for such a long time that the timer expires for the location update procedure to be triggered.

Encryption

If the IMSI-catcher performs an interception attack, it can turn off encryption, by setting the cipher to A5/0, to get messages in plaintext. More sophisticated IMSI-catchers might turn on A5/1 or A5/2 encryption, and decrypt the ciphertext with attacks such as the ones described in Section 2.7.2.

Forcing MSs to Camp

If an attacker performs a DoS-attack or interception with an IMSI-catcher, she would want the MSs to camp on the cell for as long as possible. Increasing the C2 value, as described above, is one technique that would work. Another is to broadcast the maximum value of the CRH, 14 dBm[16]. A large CRH would make it harder for an MS to reselect to a new cell, as the new cell would need to have a C2 value 14 dBm greater than the cell of the IMSI-catcher.

2.9.5 IMSI-Catcher-Catchers

There exist several devices and software with the goal of detecting IMSI-catcers. The open source software project OsmocomBB[2] have implemented an IMSI-catcher-catcher in their BP firmware, running on Motorola C123 or V171 handsets. There also exist some Android applications that aims to detect IMSI-catchers, such as the AIMSICD project[3] and SnoopSnitch[4]. Dabroeski et al. proposed an IMSI-catcher-catcher for Android devices in 2014[37]. The GSMK CryptoPhone, a device running a modified Android, providing end-to-end encryption, also has an IMSI-catcher-catcher implementation in the so-called BP firewall. The device is explained in more details in Chapter 5.

The mentioned devices and software uses a similar approach to catching IMSI-catchers. A set of rules are implemented and violations of these cause alarms to be raised. The rules are mainly based on the information obtained from system information messages. For instance will a small T3212 and empty BA-list cause alarms to be raised. Alarms will also be raised when A5/0 encryption is detected.

[2] http://bb.osmocom.org/trac/
[3] https://secupwn.github.io/Android-IMSI-Catcher-Detector/
[4] https://opensource.srlabs.de/projects/snoopsnitch

AIMSICD and the application proposed in [37] compares the CI and LAC to public CI databases, such as OpenCellID[5], and raises alarms if the CI and LAC is not in the databases for the given location. As these public CI databases are based on user uploads, many CIs and LACs are not in the databases, thus many false alarms will be raised. These applications can only detect IMSI-catchers configured to spoof the operator of the SIM inserted in the ME the software is installed on.

The Network Guard takes a slightly different approach, described in more details in Chapter 5. This device logs information from cell selection and reselection procedures, and can monitor the networks of multiple PLMNs simultaneously. Various algorithms can be performed on the acquired data to detect anomalies. The device is described as very expensive by Aftenposten[5]. Pönsgen proposed in 2015 a method of obtaining the same data as the Network Guard acquires with a manipulation of the open source OsmoComBB BP firmware[35]. It runs on very cheap MEs, such as the Motorola C123. Pönsgen did not implement the algorithms used to detect anomalies.

In [37], the authors proposed a method of catching IMSI-catchers with a stationary device, looking for changes and anomalies amongst the cells it can observe.

2.10 GSM PLMNs in Norway

There are currently two GSM PLMNs in Norway, Telenor and NetCom. Until 2015, there were three PLMNs, Telenor, NetCom and Network Norway. In July 2014, TeliaSonera, NetCom's parent company, bought Tele2. Tele2 owned Network Norway. Thus, TeliaSonera acquired Network Norway as well[38]. The frequencies of Network Norway were then sold to ICE, a mobile broadband provider.

2.10.1 MNCs in Norway

Table 2.3 shows the MNCs of the PLMNs in Norway. The table includes the MNC that was used by Network Norway.

Table 2.3 MNC of the PLMNs in Norway.

PLMN	**MNC**
Telenor	01
NetCom	02
Network Norway	05

[5] http://opencellid.org/

2.10.2 GSM Frequency Allocations in Norway

There are two frequency bands allocated GSM in Norway. The 900 band (GSM 900) and the 1800 band (DCS 1800). The two PLMNs in Norway are allocated frequencies on both these bands[39]. ICE are also allocated some of the frequencies, but they do not have a GSM network currently operating on their allocated frequencies. Network Norway was allocated these frequencies until 2015.

Table 2.4 GSM frequency allocations in norwegian land territory

	900 Frequency Band (MHz)		**1800 Frequency Band (MHz)**	
PLMN	**Uplink**	**Downlink**	**Uplink**	**Downlink**
Telenor	899.9 - 915	944.9 - 960	1725 - 1745	1820 - 1840
NetCom	885.1 - 899.9	930.1 - 944.9	1745 - 1765	1840 - 1860
ICE	880 - 885.1	925 - 930.1	1730 - 1750	1825 - 1845

Chapter 3
BTS Configuration

The system information messages broadcasted by BTSs of the two PLMNs in Norway on the BCCH were sniffed and logged in this thesis. This chapter presents the method of obtaining the messages. The parameters related to IMSI-catchers are presented and discussed at the end of this chapter.

3.1 Experimental Setup

This section describes the setup that was used to intercept and decode system information messages sent from BTSs nearby. The following hardware and software were used:

- Macbook Pro Early 2011, OSX Yosemite v. 10.10.1 with VirtualBox v. 4.3.20 installed.
- Virtual Machine (VM) with KaliLinux 1.1.0 with GNU Radio and Airprobe installed.
- Universal Software Radio Peripheral (USRP) N200 with a SBX 400-4400 MHz Rev 5.1 daughter board, two VERT900 antennas, GPSDO Kit for USRP N200 series and a Global Positioning System (GPS) antenna.

3.1.1 USRP N200

The USRP N200 is a fully functional radio device that, when connected to a computer, is a Software-defined radio (SDR). A SDR is a radio that is controlled by software running on a computer[40]. The software performs the signal processing, in contradiction to conventional radios where the hardware performs the signal processing. Depending on what frequencies the radio is able to transmit and receive on, the SDR can listen to and transmit all kinds of radio signals by writing software that enables

it. A SDR may, for instance, be able to listen and transmit FM radio, listen on GPS data and be used to open garage doors.

The USRP N200 is a device of the USRP family, that in total consists of 10 different SDR devices. The devices are manufactured and developed by Ettus Research[1] which is a daughter company of National Instruments. Ettus Research is at the time of writing the world's leading supplier of SDRs[41].

Figure 3.1: The USRP N200

Out of the box, the USRP N200 is equipped with a motherboard. The motherboard has a dual 100 MS/s, 14-bit analog to digital converter (ADC) and a dual 400 MS/s, 16-bit digital to analog converter (DAC). Figure 3.1 is an image of the front side of the USRP N200. The device has an Ethernet interface used for high-speed connection between the computer running the software and the USRP.

In order to be able to receive or transmit signals, a daughter board has to be installed on the motherboard. The daughter board provides the RF front end and distributes radio signals to and from the ADC and DAC. There exist multiple daughter boards for the N200. The difference between these daughter boards is the frequency they can transmit and receive on.

Since the 900 MHz and 1800 MHz frequency bands are allocated GSM in Norway, a daughter board able to transmit and receive on these frequency bands was needed. The SBX 400-4400 MHz daughter board was chosen and installed. This daughter board has the capabilities to transmit and receive on all the frequencies in the range

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

400 - 4400 MHz. Two VERT900 antennas were installed to the daughter board to enhance the Tx power of the radio. These antennas can transmit and receive in the frequency ranges 824 - 960 MHz and 1710 - 1990 MHz.

The internal clock of the USRP N200 is fixed to 100 MHz. As described in Chapter 2, TDMA is used in GSM. The system is very clock sensitive, and a USRP with a just a slightly inaccurate clock could have troubles receiving and transmitting GSM signals. For this reason, a GPS clock was installed on the device. A GPSDO kit was installed to the motherboard and connected to a GPS antenna. The GPSDO kit works as a reference clock for the internal 100 MHz clock. The GPS clock provides an accuracy of 0.01 ppm.

The complete USRP N200 with GPS clock, antennas and daughter board is shown in Figure 3.2.

3.1.2 GNU Radio

GNU Radio is an open source development toolkit that provides signal processing blocks[42]. The development of the software first started in 1998. It can, in combination with external RF hardware, such as the USRP, be used to implement SDRs. The software can be used to write applications that read signal streams or push data onto digital signal streams that are then transmitted with the external RF hardware.

GNU Radio provides decoders, vocoders, filters and many other elements. These elements are called ”blocks” and they can be connected to each other through a graphical user-interface (GUI). Blocks can be edited and added by writing code in Python or C++. GNU Radio comes out of the box with several tools, such as a simple spectrum analyzer and a simple signal generator.

A tutorial on how GNU Radio can be installed on Kali Linux is appended in Appendix A.

3.1.3 Airprobe

Airprobe is a tool used to analyze the Um interface of GSM[43]. The development of the tool ended in 2010. Some conflicts with the new version of libraries the software depends on arises because the tool is not updated for these versions. The installation process of the software can thus be complicated. For this reason, a tutorial on how to download and install Airprobe is appended in Appendix B.

There are three subprojects of Airprobe, **acquisition**, **demodulation** and **analysis**.

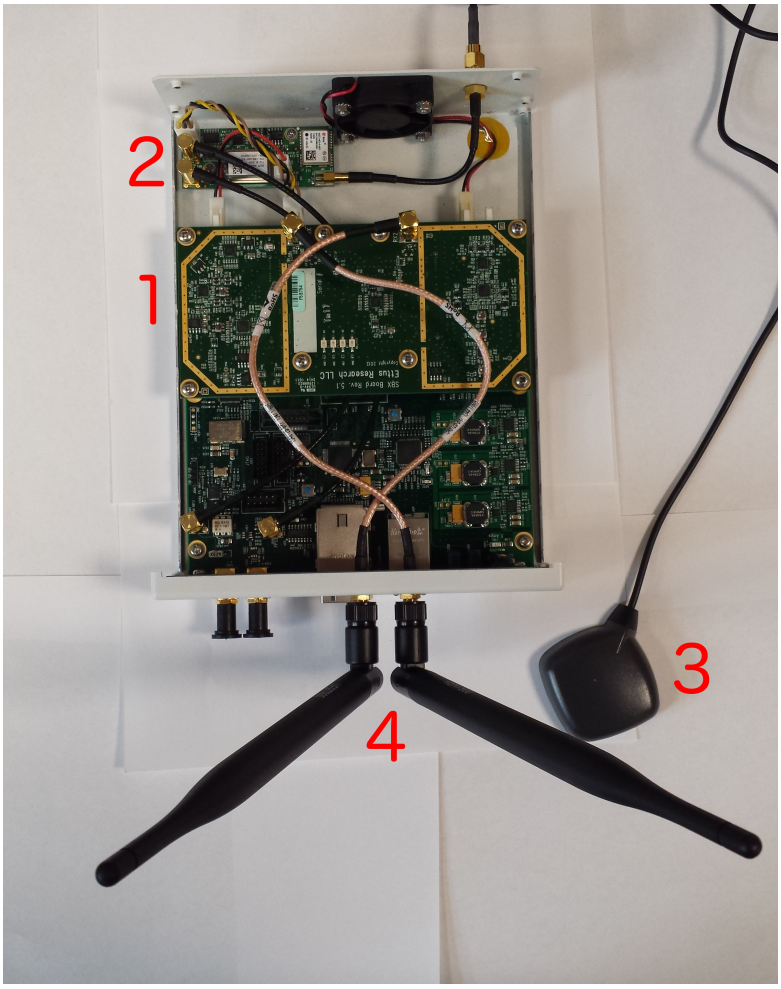


Figure 3.2: The USRP N200 with daughter board, GPSDO kit, GPS antenna and two VERT900 antennas installed. In the figure, 1 is the daughter board installed on top of the motherboard, 2 is the GPSDO kit, 3 is the GPS antenna connected to the GPSDO kit and 4 is the two VERT900 antennas.

- **Acquisition**: Contains everything that has to do with receiving and digitizing the Um interface. This part is hardware dependent. It is written for USRP and RTL-SDR hardware.

- **Demodulation**: Contains everything that is needed to make bits out the signal captured by acquisition. This part is not hardware dependent.

- **Analysis**: Contains GSM protocol parsing and decoding.

Airprobe inherits code from GNU Radio. Thus GNU Radio has to be installed for Airprobe to work.

3.2 Method of Obtaining Messages

Airprobe was used to read the system information messages broadcasted by the nearby BTSs. This section will describe how the messages were gathered.

3.2.1 Finding BTS

One first need to know what frequency to listen for broadcasted GSM messages to capture data with Airprobe. The frequency nearby BTSs broadcasted on had to be found for both the GSM PLMNs in Norway to observe the configuration of the two different networks.

The experiment was conducted in "Hovedbygget" at Norwegian University of Science and Technology (NTNU) in Trondheim, Norway. The closest BTSs are illustrated in a map in Figure 3.3. The data from the map is from 'finnsenderen.no' which is a service provided by the Norwegian National Communication-Authority (Nkom) that shows the geographical location of BTSs in Norway[44].

The GNU Radio tool *uhd_fft* was used to search for nearby BTSs. The tool is a simple spectrum analyzer that is provided out of the box for GNU Radio. It displays the spectrum at a given frequency. It is a narrow band spectrum analyzer, i.e. the tool is only able to display the frequency spectrum of 1 MHz at the time.

Finding Telenor BTS

To find Telenor's BTS with largest RxL nearby, all downlink frequencies that are allocated Telenor had to be observed with the frequency spectrum analyzer tool, *uhd_fft*. The frequencies allocated the different PLMNs in Norway were shown in Section 2.10.2.

Since the tool only displays the spectrum for 1 MHz at the time, the tool has to be run several times with steps of 1 MHz from 945 MHz to 960 MHz. Listing 3.1 shows this procedure.

Figure 3.3: Map over the closest GSM BTSs to the location of the experiment. 'N' represents NetCom BTS, 'T' represents Telenor BTS and 'X' represents the location of where the experiment was conducted. Edited map from http://www.finnsenderen.no/[44].

Listing 3.1: Searching for Telenor BTSs with GNU Radio

```
$ uhd_fft -f 945M
$ uhd_fft -f 946M
$ uhd_fft -f 947M
...
$ uhd_fft -f 960M
```

Figure 3.4 shows the output of *uhd_fft -f 947M*, i.e. the frequency spectrum at 947 MHz. The red arrows points at spikes in the spectrum analyzer that represents nearby BTS. The BTS with the best reception of all the observed BTSs was chosen. This was the BTS broadcasting on 947 MHz. This frequency corresponds to ARFCN 60. The RxL from this BTS was approximately -50 dBm.

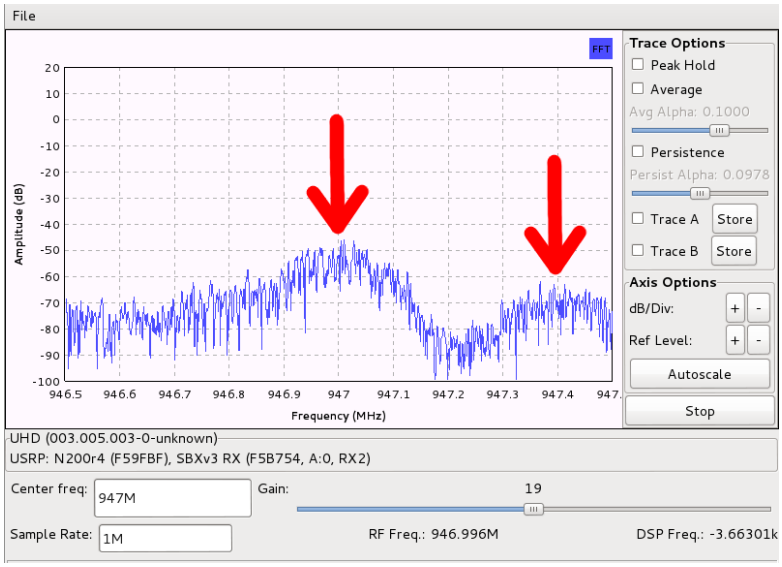


Figure 3.4: Output from *uhd_fft -f 947M*.

Finding NetCom BTS

The method of finding the NetCom BTS with the best reception was the same as described for Telenor. The *uhd_fft* tool was used to search through NetCom's allocated downlink frequencies in the 900 band, i.e. 930 - 945 MHz, as shown in Listing 3.2.

Listing 3.2: Searching for NetCom BTSs with GNU Radio

```
$ uhd_fft -f 930M
$ uhd_fft -f 931M
$ uhd_fft -f 932M
...
$ uhd_fft -f 945M
```

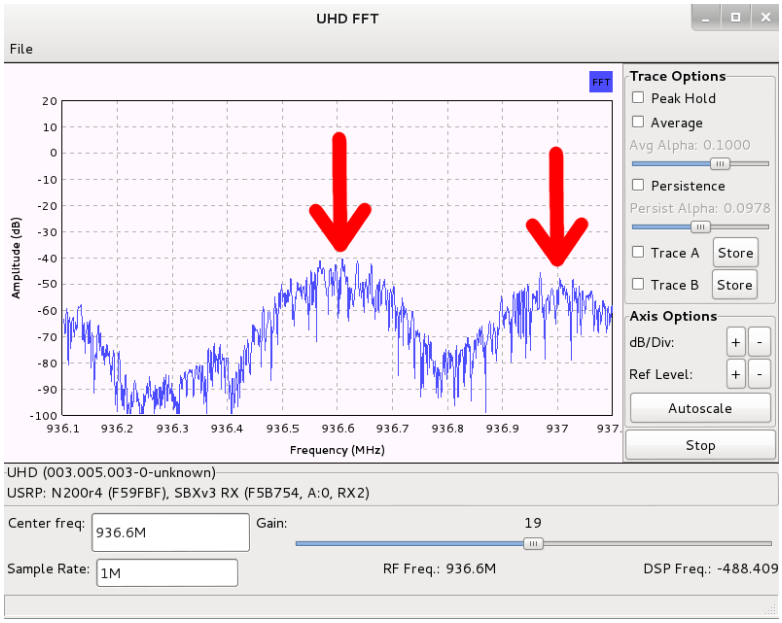


Figure 3.5: Output from *uhd_fft -f 936.6M*.

Figure 3.5 shows the output of *uhd_fft -f 936.6M*. The red arrows points at BTSs observed in this plot, one at 936.6 MHz and one at 937 MHz. The RxL from the one broadcasting on 936.6 MHz was strongest out of all the NetCom BTSs observed, thus it was chosen to listen for NetCom system information messages on this frequency. This frequency corresponds to ARFCN 8. The measured RxL from this BTS was approximately -40 dBm at the location of the experiment, as can be observed from Figure 3.5.

3.2.2 Capturing System Information Messages with Airprobe

The Airprobe tool *gsm_receive_usrp* was used to listen to system information messages sent on BCCH of the frequencies found in Section 3.2.1. This tool is able

to listen to downlink, non-hopping GSM signals. The signals are interpreted, and can be read with Wireshark[2][45].

Listing 3.3 shows how Airprobe was used to listen to system information messages sent by Telenor BTS on frequency 947 MHz. The $-f$ option determines the frequency to listen on. The $-g$ option sets the Reception (Rx) gain.

Listing 3.3: Listening on BTS on frequency 947 MHz with Airprobe.

```
$ ./gsm_receive_usrp.py -f 947M -g 10
```

The messages sent by the BTS can be observed with Wireshark by listening to the *lo (loopback)* interface on the computer that runs the Airprobe tool. The messages are interpreted as a *GSMTAP* protocol.

3.3 BTS Configuration Parameters

In this section, some of the configuration parameters of the nearest BTSs of the two PLMNs in Norway are observed and discussed. The focus is on parameters relevant for IMSI-catchers, such as parameters used in selection and reselection procedures.

The parameters are sent in the system information messages from the BTS. Figure 3.6 shows how system information message type 4 is presented in Wireshark. This message contains the LAI, cell selection parameters and RACH parameters. The information in this section is gathered from system information type 1 to system information type 4 broadcasted on the BCCH.

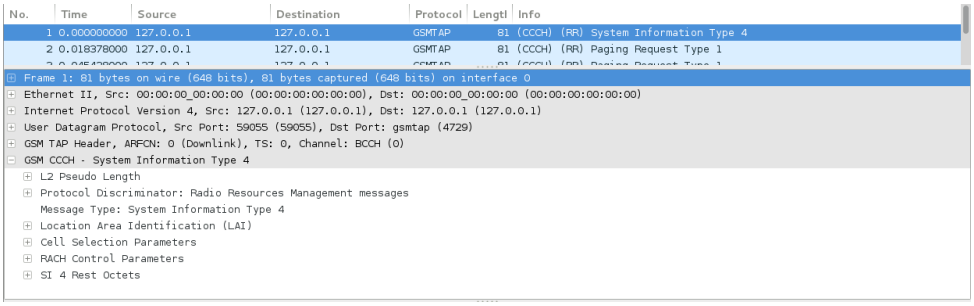


Figure 3.6: System Information Type 4 in Wireshark

3.3.1 Telenor

Table 3.1 shows parameters relevant for this thesis, broadcasted by the Telenor BTS with the best reception at the location the experiment was conducted. The BTS with

[2]http://www.wireshark.com

best reception was the BTS broadcasting on ARFCN 60, as found in Section 3.2.1. The list of ARFCNs tells the MS what ARFCNs this cell uses for slow frequency hopping.

Table 3.1 Parameters broadcasted by Telenor BTS.

Parameter	**Value**
CID	0x407d (16509)
LAI	242/01/12411
MCC	242 (Norway)
MNC	01 (Telenor)
LAC	0x307b (12411)
List of ARFCNs	103 60
CELL_RESELECT_HYSTERISIS	3 (6 dBm)
MS_TXPWR_MAX_CCH	5
RXLEV_ACCESS_MIN	0 (<110 dBm)
CELL_BARR_ACCESS	0 (cell is not barred)
PT	0 (20 s)
TO	0 (0 dB)
CRO	0 (0 dB)
T3212 Timer	40 decihours (4 hours)
BA list	124 123 68 67 66 65 64 62 61 60 59 58 57 56 55 54 53 52 51

3.3.2 NetCom

Table 3.2 shows the parameters broadcasted by the NetCom BTS with the best reception at the location the experiment was conducted. The NetCom BTS with the best reception was the BTS broadcasting on ARFCN 8, as found in Section 3.2.1.

Table 3.2 Parameters broadcasted by NetCom BTS

Parameter	**Value**
CID	0xfc0b (64523)
LAI	242/02/3305
MCC	242 (Norway)
MNC	02 (NetCom)
LAC	0x0ce9 (3305)
List of ARFCNs	38 8
CELL_RESELECT_HYSTERISIS	2 (4 dBm)
MS_TXPWR_MAX_CCH	5
RXLEV_ACCESS_MIN	0 (<110 dBm)
CELL_BARR_ACCESS	0 (cell is not barred)
PT	0 (20 s)
TO	0 (0 dB)
CRO	0 (0 dB)
T3212 Timer	40 decihours (4 hours)
BA list	48 42 41 31 28 26 24 21 16 14 11 10 7 5 4

3.3.3 Discussion

From Table 3.1 and Table 3.2 one can observe the configuration of the BTSs of Telenor and NetCom, and their similarities and differences. The BTSs have different CI and LAC which is normal since they belong to two different PLMNs. Both the cells have two ARFCNs used for slow frequency hopping.

The CRH is different for the BTSs of the two networks. For Telenor's BTS the CRH is set to 3 while for NetCom's BTS, the CRH is set to 2. The CRH difference corresponds to a difference of 2 dBm. This means that for a MS camped on Telenor's cell, a C2 value of a new cell with a different LAC has to be at least 6 dBm greater than the C2 value of the observed cell, for the MS to reselect to the new cell when the cells LAC differs. For NetCom's cell, the value is 4 dBm.

Both the BTSs broadcast RXLEV_ACCESS_MIN value of 0 (<110 dBm). As described in Chapter 2 Section 2.6, this is the smallest possible value, and are used in the calculation of the C1 value. A smaller value of RXLEV_ACCESS_MIN leads to a larger value of C1, which in turn leads to a larger C2 value.

The T3212 is 4 hours for both the BTSs. Thus, a MS camped on one of the cells will

perform a location update procedure if it has been camped on the cell for 4 hours. Since the timer is as large as four hours, IMSI-catchers relying on a small T3212 value could be easy to detect in this area.

CRO, PT and TO are all broadcasted as 0 by the BTSs. This is the case for both the Netcom BTS and the Telenor BTS. This in turn means that C2 = C1 in these cells. Since MS_TXPWR_MAX_CCH and RXLEV_ACCESS_MIN are the same for the two BTSs, the difference in C1 and C2 values produced depends solely on the RxL. Since CRO is not set for neither of the BTSs, an IMSI-catcher using a large CRO value would be very effective at this location. By using a large CRO, the MSs in vicinity of the IMSI-catcher would calculate a much larger C2 value for the IMSI-catcher than the legitimate cells, and thus reselect to the IMSI-catcher.

It can be observed that the list of neighbor ARFCNs, the BA list, is larger for the Telenor BTS than the NetCom BTS. Thus, Telenor probably have more cells than NetCom in the area. Another observation is that one of the ARFCNs used by Telenor's cell appears in the BA list, i.e. ARFCN 60. This is probably a misconfiguration by Telenor. Putting the serving cell in the BA list will not serve any purposes. Since the MS calculates C1 and C2 for the serving cell and the six cells with strongest RxL from the BA list, the serving cell's C1 and C2 values will often be calculated twice. In practice, only five neighbor cells will be considered as possibilities for reselection in these cases, which may reduce the performance of the network.

Many of the values observed in this chapter, such as CRO, TO, CI, LAC, etc., are considered confidential by the Norwegian PLMNs[46, 47, 48, 49].

To configure an IMSI-catcher effectively, one need to know similar information as the information obtained in this chapter.The results from this chapter are used to implement an IMSI-catcher in Chapter 4.

By using the method explained in this chapter, it is also possible to manually detect IMSI-catchers, by comparing the values of the parameters received from all the cells that can be observed in the area to detect anomalies.

Chapter 4
Open Source IMSI-Catcher

An open source IMSI-catcher was made and configured in this thesis. Two different attacks and the effectiveness of the IMSI-catcher were tested in an experiment. This chapter describes the tools used, how the IMSI-catcher was configured in the experiments and results from the experiments. The results are discussed at the end of this chapter.

IMSIs and IMEIs caught are censored as they are sensitive information that should only be known by the subscriber and the PLMN.

4.1 Experimental Setup

This section describes the setup used when conducting the IMSI-catcher experiment. The following hardware and software were used:

- Macbook Pro Early 2011, OSX Yosemite v. 10.10.1 with VirtualBox v. 4.3.20 installed.
- VM with Ubuntu server 12.04.4 installed. OpenBTS, Asterisk, SmQueue and SipAuthServe were installed on this VM.
- VM with KaliLinux 1.1.0. GNURadio and Airprobe were installed on this VM.
- USRP N200 with a SBX 400-4400 MHz Rev 5.1 daughterboard, two VERT900 antennas and GPSDO Kit for USRP N200 Series.
- 31 MSs with various hardware and Operating Systems (OSs).
- One GSMK CryptoPhone 500, Samsung Galaxy S3 with customized firmware and software.

GNU Radio and Airprobe are described in Chapter 3. The GSMK CryptoPhone 500 is described in Chapter 5 Section 5.2.

4.1.1 OpenBTS

OpenBTS is an open source software written in C++ and developed by Range Networks[50]. It is an application running on Unix systems that use a SDR to provide a GSM Um interface. It provides a software implementation of the GSM stack for BTS, and OpenBTS together with a SDR have thus the capabilities to emulate a BTS. In combination with SmQueue[1], SipAutheServe and Asterisk[2], it can be used to place calls and send text messages between MSs connected to the same OpenBTS network. The OpenBTS network is an all-IP network, which means that calls are provided as Voice over IP (VOIP).

The goal of OpenBTS is to provide a new type of cellular network that is much cheaper and easier to deploy and operate than conventional GSM networks, which could be used in rural and remote areas. It can however also be used to create illegitimate GSM networks and IMSI-catchers. This chapter will describe how an IMSI-catcher is made with the use of OpenBTS and USRP.

A guide on how to install OpenBTS, Asterisk, SmQueue and SipAuthServe is appended in Appendix C.

4.2 Setup OpenBTS

After OpenBTS, Asterisk, SmQueue and SipAuthServe have been installed, the USRP is connected to the computer via ethernet and the two devices are on the same subnetwork, the programs can be started with the following commands in the terminal:

Listing 4.1: Starting the programs used for IMSI-catcher.

```
$ sudo start openbts
$ sudo start sipauthserve
$ sudo start smqueue
$ sudo start asterisk
```

OpenBTS comes with a command line interface (CLI) that is used to control the application. The CLI can be opened with following command in the terminal:

Listing 4.2: Opening CLI for OpenBTS.

```
$ sudo /OpenBTS/OpenBTSCLI
```

The user-interface (UI) of the CLI is presented in Figure 4.1.

[1] https://smqueue.com/
[2] http://www.asterisk.org/

Figure 4.1: OpenBTSCLI

The network created with OpenBTS is highly configurable. The configuration can be done by changing values in a database manually or by using the CLI, which is advised. Changing a configuration parameter with the CLI can be done in the following way:

Listing 4.3: Changing a configuration parameter in OpenBTSCLI.

```
$ OpenBTS> config GSM.Identity.MNC 01
```

The example will set the MNC broadcasted by the BTS to 01. All the parameters that can be configured are presented in [51].

Out of the box, the network created with OpenBTS will operate as test network in test country (MNC=01, MCC=001).

4.3 Experiment

The IMSI-catcher experiment was conducted at the same location as the experiment in Chapter 3. Figure 3.3 shows a map of the location of where the experiment was conducted and the closest BTSs.

4.3.1 Overview

The experiment consisted of three parts. They were:

- Spoofing Telenor BTS and perform a DoS attack against Telenor subscribers.

- Spoofing NetCom BTS and perform a DoS attack against NetCom subscribers.

- Spoofing Telenor BTS and perform selective jamming attack against one MS selected from the IMSIs found in the first experiment.

31 students and professors from NTNU participated in the experiment. All of the participants used their own MS. A CryptoPhone 500, subscribed to Telenor, was also used in the experiment. Table 4.1 shows the number of MSs subscribing to which network.

Table 4.1 Distribution of participants on the two networks

Network	**Number of MSs**
Telenor	17
NetCom	15

4.3.2 Configurations

To get as many MSs to reselect to the IMSI-catcher and perform a location update procedure, some configurations on the BTS had to be made:

- Set the MCC to the country of the PLMN we want to spoof.

- Set the MNC to the PLMN we want to spoof.

- Set the LAC to a different value then the LAC of the legitimate cells of the PLMN we want to spoof nearby to force location update requests.

- Operate on an ARFCN broadcasted as a neighbor of the cell of the PLMN we want to spoof with the best reception at the location of the experiment.

- Make C2 value produced by the cell as large as possible. In this experiment, this was done by using maximum Tx power and setting the RXLEV-ACCESS-MIN to 0 (<110 dBm).

4.3.3 Selecting ARFCN

The first step in the experiment was to find suitable ARFCNs for the IMSI-catcher to operate on, one for Telenor and one for NetCom. The chosen ARFCN should be broadcasted in the BA list of the legitimate cells nearby. In addition there should be as little as possible traffic on the frequencies. The frequencies should either not be in use by a BTS, or the BTS operating on the chosen ARFCN should have very little or no reception at the geographical location of the experiment. The IMSI-catcher should not interfere with a real BTS as it would make the IMSI-catcher less effective since there would be noise on the channel. Additionally, the IMSI-catcher could interfere with the operations of the real BTS operating on the ARFCN, such that the PLMN would notice the noise on the channel, and thus the IMSI-catcher.

The results from the experiment in Chapter 3 were used to decide what ARFCN to operate on. In Chapter 3 the BTSs of Netcom and Telenor with the largest RxL in the geographical position of the experiment were found. In addition the lists of neighbor ARFCNs were obtained. Table 4.2 shows the list of neighbor ARFCNs of the BTSs with the best reception at the location of the experiment.

The frequency spectrum analyzer tool *uhd_fft* provided with GNU Radio was used to search through all the neighbor ARFCNs to find the most suitable ARFCNs to broadcast on. The most suitable ARFCNs are the neighbor ARFCNs with the lowest RxL at the geographical location of the experiment.

Table 4.2 ARFCNs in the BA list of the nearby BTSs

PLMN	**ARFCN of nearest BTS**	**List of neighbors**
NetCom	8	48 42 41 31 28 26 24 21 16 14 11 10 7 5 4
Telenor	60	124 123 68 67 66 65 64 62 61 60 59 58 57 56 55 54 53 52 51

The most suitable ARFCNs in the BA list were:

- ARFCN 56 for Telenor.
- ARFCN 48 for NetCom.

4.3.4 Telenor DoS Attack

When spoofing Telenor, the MCC was set to 242 (Norway), the MNC was set to 01 (Telenor), the short name of the network was set to ”Telenor” and the ARFCN was

set to 56, as found in Section 4.3.3. As found in Chapter 3, the LAC of the nearest Telenor BTS was 12411. The LAC of the IMSI-catcher was thus set to a different value.

Listing 4.4: Spoofing a Telenor BTS with OpenBTS

```
$ OpenBTS> config GSM.Identity.MCC 242
$ OpenBTS> config GSM.Identity.MNC 01
$ OpenBTS> config GSM.Identity.ShortName Telenor
$ OpenBTS> config GSM.Radio.C0 56
$ OpenBTS> config GSM.Identity.LAC 1111
```

In addition, the BTS was configured to accept all location update requests, i.e. let all MSs camp on the cell and thus perform a DoS-attack.

Listing 4.5: Accept all location update requests

```
$ OpenBTS> config Control.LUR.OpenRegistration .*
```

The BTS was also configured to broadcast on maximum power to maximize the C2 value.

Listing 4.6: Configure BTS to transmit on maximum power.

```
$ OpenBTS> power 0
```

Results

The IMSI-catcher was spoofing Telenor for 12 minutes. Figure 4.2 shows the IMSIs that camped on the IMSI-catcher during this time. The IMSIs that are caught can be shown with the *tmsis* command in OpenBTS:

Listing 4.7: Display caught IMSIs in OpenBTS.

```
$ OpenBTS> tmsis
```

This command also shows the IMEI of the MSs that have initiated a location updating procedure.

IMSI	TMSI	IMEI	AUTH	CREATED	ACCESSED	TMSI_ASSIGNED
24201	0xf6fdf		2	10m	71s	1
24201	0x691d3		2	149s	82s	1
24201	0xd961c		2	136s	135s	1
24201	0x2775d		2	160s	159s	1
24201	0x46c92		2	184s	183s	1
24201	0xadbc7		2	214s	192s	1
24201	0xb97b1		2	289s	244s	1
24201	0x64353		2	270s	269s	1
24201	0x74f36		2	11m	293s	1
24201	0xe76e5		2	10m	5m	1
24201	0x5e600		2	5m	5m	1
24201	0x658c8		2	6m	6m	1
24201	0xb5230		2	6m	6m	1
24201	0x61605		1	6m	6m	1
24201	0x111ea		2	10m	8m	1
24201	0x4ad35		2	11m	11m	1

Figure 4.2: IMSIs caught, and MSs camped on the cell when spoofing Telenor. MSINs and IMEIs are censored.

From Figure 4.2 one can observe that 16 IMSIs were caught during the 12 minutes the IMSI-catcher was operating. The 16 MSs reselected and camped on the cell of the IMSI-catcher, which means that their connectivity to the real PLMN was lost and the MSs were denied service.

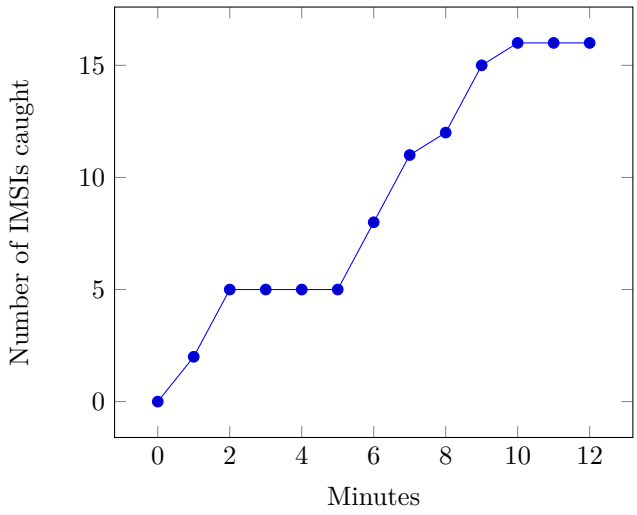


Figure 4.3: Number of MSs camped on the cell and IMSIs caught over time when spoofing Telenor

The ”AUTH” parameter in Figure 4.2 shows if the MS is authenticated or not. ”AUTH” 0 means that the location update request was rejected. ”AUTH” 1 means that the MS is a subscriber in the network and is authenticated. ”AUTH” 2 means

that the MS is not a subscriber, but the location update request is accepted. In this case, the MS is camped on the network, but does not have a phone number.

In Figure 4.2 one can further observe that all except one of the caught IMSIs had a "AUTH" value of 2. The one with "AUTH" value of 1 is an MS that was added as a subscriber to the network before the experiment was conducted.

Figure 4.3 shows the time it took for the MSs to reselect to the cell of the IMSI-catcher. From the figure, it can be observed that many of the MSs used several minutes to reselect to the cell.

4.3.5 NetCom DoS Attack

Spoofing NetCom was done in the same way as Telenor. The MNC was set to 02 (NetCom), the short name of the network was set to "NetCom" and the ARFCN was set to 48, as found in Section 4.3.3. The LAC of the nearest NetCom BTS was 3305, found in Chapter 3. The IMSI-catcher used the same LAC as in the Telenor experiment, which was different from 3305.

Listing 4.8: Spoofing a NetCom BTS with OpenBTS.

```
$ OpenBTS> config GSM.Identity.MNC 02
$ OpenBTS> config GSM.Identity.ShortName NetCom
$ OpenBTS> config GSM.Radio.C0 48
```

The network accepted all location update requests in this experiment as well, and RXLEV-ACCESS-MIN was set to 0.

Results

The IMSI-catcher was spoofing NetCom for 11 minutes. During this time, 8 IMSIs were caught. The 8 MSs associated to the IMSIs camped on the cell and were thus denied service to the real network. Figure 4.4 shows the MSs that camped on the cell. One can observe that two Swedish IMSIs were caught (MCC 240) and one Polish IMSI was caught (MCC 260). Only three IMSIs had NetCom's MNC 02. One of the caught IMSI had the MNC of Telenor and one had the MNC of Network Norway.

IMSI	TMSI	IMEI	AUTH	CREATED	ACCESSED	TMSI_ASSIGNED
24205	0xb4820		2	103s	101s	1
24007	0x69b18		2	238s	237s	1
24007	0x2a36f		2	6m	269s	1
24201	0x24af9		2	283s	283s	1
24202	0x135e7		2	6m	6m	1
26006	0x3b8c4		2	6m	6m	1
24202	0x76575		2	7m	7m	1
24202	0x4c6aa		2	8m	8m	1

Figure 4.4: IMSIs caught when spoofing NetCom. MSINs and IMEIs are censored.

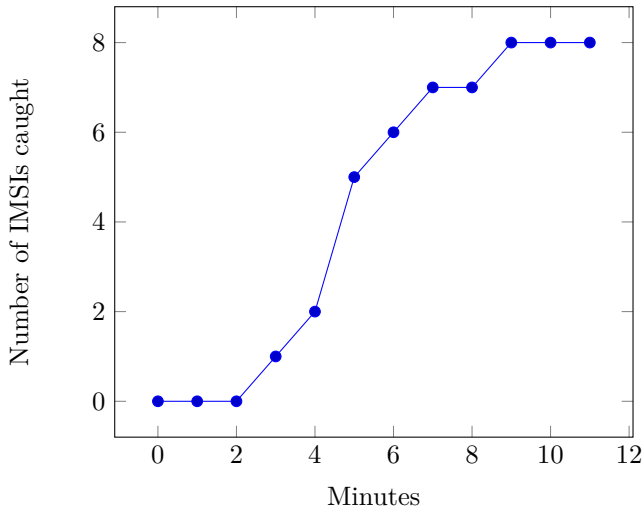


Figure 4.5: Number of MSs camped on the call, and IMSIs caught over time when spoofing NetCom

Figure 4.5 shows the number of IMSIs caught, and thus also the number of MSs camped on the cell, over time.

4.3.6 Selective Jamming

In this experiment, the IMSI-catcher was set to spoof Telenor. The difference between this experiment and the one performed in Section 4.3.4 was that location update request was only accepted for one specific IMSI selected randomly from the IMSIs caught in the first attack in Section 4.3.4. Thus, a selective jamming attack was performed against the MS with the IMSI targeted. All the other MSs that performed location update procedures were rejected, and thus reselected to a legitimate cell nearby.

The IMSI-catcher was configured in the same way as in Section 4.3.4 with one adjustment. The *Control.LUR.OpenRegistration* parameter was set to accept only one specific IMSI.

Listing 4.9: Jamming MSs selectively by IMSI. The MSIN of the IMSI targeted is replaced with x's.

```
$ OpenBTS>
        config Control.LUR.OpenRegistration 24201xxxxxxxxxx
```

IMSI	TMSI	IMEI	AUTH	CREATED	ACCESSED	TMSI_ASSIGNED
24201	0xfc63e		0	62s	62s	0
24201	0xca23e		0	88s	88s	0
24201	0xf4739		1	89s	88s	1
24201	0x25c0e		0	91s	91s	0
24201	0xdeba6		2	100s	98s	1
24201	0x4c204		0	102s	102s	0
24201	0x730da		0	102s	102s	0
24201	0x97339		0	107s	107s	0

Figure 4.6: Selective jamming

From Figure 4.6 one can observe that two MSs was authenticated ("AUTH" = 1 or "AUTH" = 2), and thus camped on the cell. The one MS with "AUTH" = 1 was the same as in Section 4.3.4, and was subscribed to the network. The other MS with "AUTH" = 2 was the one targeted.

The targeted MS performed a location update request and camped on the cell of the IMSI-catcher within seconds. Its connectivity to the real network was lost, and the MS was jammed. The other MSs that initiated a location updating procedure was rejected by the IMSI-catcher. Their IMSI was caught, but the MSs reselected to another, legitimate cell immediately.

4.3.7 CryptoPhone Warnings

The CryptoPhone is a device that, according to the manufacturers, can detect IMSI-catchers[52]. The device is described in details in Chapter 5.

The CryptoPhone reselected to the cell of the IMSI-catcher and camped on the cell when Telenor was spoofed. The baseband firewall in the CryptoPhone gave some warnings shown in Figure 4.7

There are several warnings marked as 'VERY_HIGH'. The baseband firewall of the CryptoPhone was able to determine that the IMSI-catcher broadcasted an empty BA list. This is a clear indication that the MS is camped on a IMSI-catcher. Most legitimate cells broadcast a list of neighbors.

The IMSI-catcher did not perform any attacks on the BP. Nevertheless, the CryptoPhone warned against baseband processor anomalies during the time the CryptoPhone was camped on the IMSI-catcher. These warnings were false positives.

4.4 Discussion

The experiment was conducted in lecture hall H1 at NTNU. The walls in the lecture hall are thick. However, the signal most likely reached some areas outside of the building and other parts inside the building. Thus, some MSs that did not participate

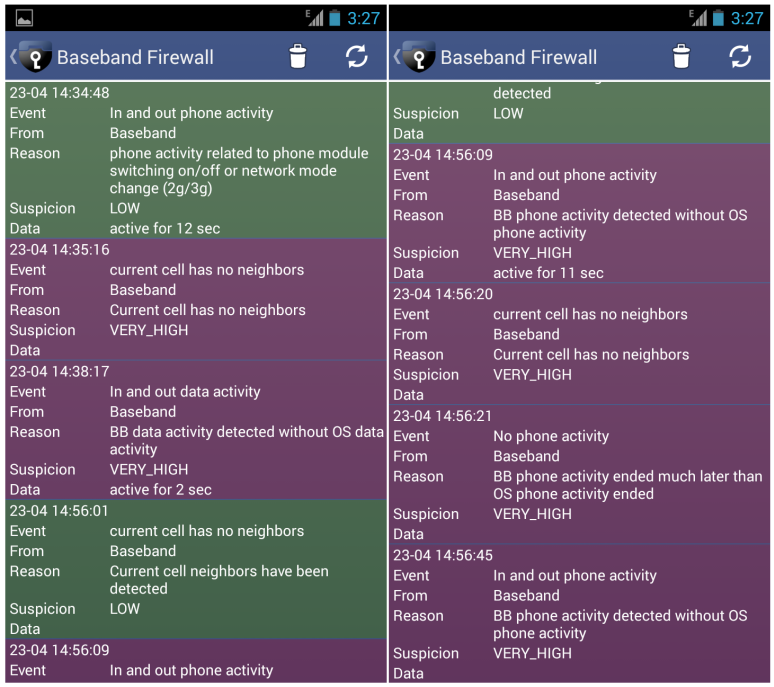


Figure 4.7: Baseband firewall warnings from CryptoPhone during IMSI-catcher experiment.

in the experiment could reselect to the cell provided by the IMSI-catcher. Some of the IMSIs that were caught may originate from MSs that did not participate in the experiment, but accidentally were located nearby. This can explain why two Swedish IMSIs, and one Polish IMSI were caught in the NetCom experiment. None of the participants of the experiment had Swedish or Polish registered SIMs.

From the results in Section 4.3.4 and Section 4.3.5, it can be observed that the IMSI-catcher was more effective when spoofing Telenor than when spoofing NetCom. The C2 value of the IMSI-catcher was thus not large enough for many of the MSs to reselect to the cell of the IMSI-catcher in the NetCom experiment. Even though the CRH for the nearest Telenor cell was higher than the nearest NetCom cell, more MSs reselected to the IMSI-catcher when spoofing Telenor.

In Chapter 3 it was found that C1 = C2 in the cells with the best reception nearby. It was also found that RXLEV_ACCESS_MIN and MS_TXPWR_MAX_CCH were the same for the NetCom and the Telenor cell. Thus, the reason why the IMSI-catcher was more effective when spoofing Telenor was that the Telenor cell with largest RxL in the lecture hall had significantly worse RxL than the NetCom

cell with the largest RxL in the lecture hall.

From Figure 3.4 and Figure 3.5 one can observe that the RxL of the NetCom BTS nearby was approximately -40 dBm and the RxL of the nearest Telenor BTS was approximately -50 dBm. The RxL of the IMSI-catcher was measured to approximately -50 dBm a meter away from the device. Since CRO was not broadcasted by the IMSI-catcher, the C2 value of the cell of the IMSI-catcher would be smaller than C2+CRH of the nearest NetCom cell at the location of the experiment. This can explain why only 3 out of 15 NetCom IMSIs were caught in this experiment.

From Figure 4.5 and Figure 4.3 it can be observed that most MSs used several minutes to reselect to the cell of the IMSI-catcher. This means that for the IMSI-catcher to be effective, it should be operating continously and not in intervals.

The IMSI-catcher proposed in this chapter was able to perform DoS attacks and catch IMSIs and IMEIs. It can also be used to deliver spam text messages to the MSs camped on the cell of the IMSI-catcher. Such text messages can be sent with an originating MSISDN chosen by the attacker.

The effectiveness of the IMSI-catcher proposed in this thesis is determined by the number of MSs that reselect to the cell in a short amount of time. Thus, the effectiveness depends on the C2 value calculated by the MSs in the vicinity of the IMSI-catcher compared to the C2 value of the other, legitimate cells in the area.

The signal strength is the biggest drawback of the IMSI-catcher as a low signal strength results in a low C2 value. The IMSI-catcher is only effective in a small geographical area since the Tx power of the USRP is limited. Signal strength quickly declines when moving away from the IMSI-catcher.

The attacks performed in this chapter illustrate the major security flaw of no mutual authentication in GSM. Effective attacks were performed in this chapter with equipment costing less than 2000 USD.

Chapter 5
Analysis of the Aftenposten Investigations

The largest Norwegian newspaper, Aftenposten, claimed in December 2014 that at least 9 false BTSs or IMSI-catchers were deployed in Oslo[53]. The newspaper published the methods and material that gave reason to believe that they observed IMSI-catchers in Oslo[54].

The methods and data acquired by Aftenposten are discussed and analyzed in this chapter. A summary and discussion of the investigation is included at the end of the chapter. All the figures that represent maps and does not state otherwise are excerpts from Google Maps[1]. MYSQL was used as the main tool in the analysis in this chapter.

5.1 Background

Aftenposten first performed an investigation in Oslo with the German-made ME GSMK CryptoPhone 500. The company that is producing the ME advertises that the ME can detect IMSI-catchers. Aftenposten acquired data that they interpreted as suspicious with the CryptoPhone.

The newspaper wanted to do a more thorough investigation to confirm the results of the investigation with the CryptoPhone. They contacted the Norwegian security company Aeger. Aeger acquired assistance from the Czech company CEPIA, which in turn acquired assistance from the British company Delma MSS. Delma MSS provided the equipment used in the investigations in Oslo. The device used is called Falcon II by CEPIA and Network Guard by Delma. Throughout this thesis, the name Network Guard is used. The device has been used in counter-surveillance investigations all over the world[5].

Four surveys in Oslo were performed with Network Guard, and a large amount of data from the BTSs in Oslo were gathered. Aftenposten concluded that there most

[1] http://maps.google.com/

likely were several IMSI-catchers in Oslo, based on these data and the data acquired with the CryptoPhone[55].

Aftenposten published the first of a series of articles the 12. December 2014[55]. The first articles were based on the data acquired with the CryptoPhone and the two first surveys made with the Network Guard. The newspaper claimed that, amongst others, the Norwegian parliament and the Prime Minister possibly were being surveilled by the use of IMSI-catchers. The articles resulted in a widespread debate, where prominent politicians, The Norwegian Police Security Service (PST), The Norwegian Security Authority (NSM) and other organizations participated. The findings made by Aftenposten resulted in the government providing Nkom with 2 million NOK. The funding was allocated to improving the capacity to detect the use of illegal equipment connected to the PLMNs, such as IMSI-catchers[56].

At the end of March 2015, PST analyzed the data acquired by Aftenposten, compared them to data acquired from the PLMNs and made their own measurements. PST argued that the values in the data Aftenposten gathered were normal and corresponded to the data presented by the PLMNs[7]. They claimed that nothing suggested that Aftenposten had detected IMSI-catchers in Oslo, based on the data Aftenposten had acquired.

5.2 CryptoPhone

5.2.1 About

The *GSMK Cryptophone 500* is a modified *Samsung Galaxy S3*. It provides secure voice messaging and VOIP on any network by the use of end-to-end encryption. The ME is running a modified version of the Android[2] operating system that provides better security than the conventional version of the operating system. Figure 5.1 shows an image of the GSMK CryptoPhone 500.

5.2.2 Baseband Firewall

The CryptoPhone is equipped with what GSMK calls a *baseband firewall*. It is not a real firewall protecting the Baseband Processor (BP), but rather a monitoring program that monitors the debug output from the BP and some of the data sent from the BP to the AP. The baseband firewall can according to GSMK detect anomalies[57]. The baseband firewall is the function that Aftenposten utilized to detect anomalies in the networks in Oslo in the investigation with the CryptoPhone. According to GSMK, the baseband firewall in CryptoPhone can protect the AP from attacks on the BP, such as the attacks presented by Weinmann[30]. The baseband

[2]http://www.android.com/

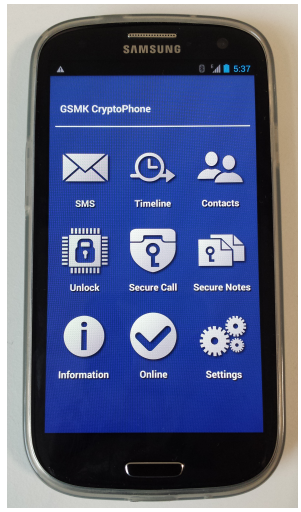


Figure 5.1: The GSMK CryptoPhone 500 used by Aftenposten.

firewall provides two functions, **BP behavior anomaly detection** and **network anomaly detection**.

BP Behavior Anomaly Detection

The BP anomaly detection monitors the interface between the BP and AP and checks if one of the processors behaves suspiciously compared to the other processor. This can be used to check if the BP is under attack, for instance by attackers that try to run code from the BP or exploit vulnerabilities in the BP, such as exploits of memory corruptions. The BP is a non-standard unit, and code needs to be developed specifically for a certain BP to be able to run on that BP. Thus, the BP anomaly detection detects only quite sophisticated attacks, aimed at specific BPs. Many of the warnings given by this function are likely false positives in the sense that legitimate processor operations trigger the warnings[52]. However, a high number of these warnings may indicate that active attacks are being performed. There are six rules in the BP behavior anomaly detection. Violations of these rules cause warnings. The rules are described in Table 5.1.

Table 5.1 Rules used to detect BP anomalies with the CryptoPhone baseband firewall[52].

	Rule
1	When there is BP data activity, there also should be OS data activity.
2	When there is BP phone activity, within some interval there also should be OS phone activity or SMS activity, or within 1s data activity.
3	When there is BP control channel or SMS activity, within a short period there also should be AP data activity / SMS activity.
4	Check that BP data activity ended at the same time when AP data activity ends.
5	Check that baseband phone activity ended at the same time when AP phone activity ended.
6	If an incoming call is off hook, then the user must have answered it.

Network Anomaly Detection

The network anomaly detection is the function that is best suited for IMSI-catcher detection. The baseband firewall monitors some parameters in the system information messages broadcasted from the BTS to the MS and triggers a warning in case of suspicious events. The events that may trigger warnings are described in Table 5.2.

Table 5.2 Events that trigger network anomaly warning with the CryptoPhone baseband firewall[52]. C1 and T3212 are described in more details in Chapter 2.

	Event
1	A5 encryption on the Um interface is not enabled.
2	The cell the MS is camping on does not advertise neighboring cells.
3	Path loss criterion parameter (C1) value is suspiciously large.
4	The Periodic Location Updating Timer (T3212) is suspiciously small.
5	The network operator changes, i.e. the MS is roaming to another PLMN than its home network.
6	The network mode changes, for instance drops from a 3G connection to a 2G connection.

If a high number of these events happen in a short period, GSMK claims that there is likely that there is an IMSI-catcher nearby. Alarms triggered by the baseband firewall are graded from ”NONE” suspicion to ”VERY_HIGH” suspicion.

5.2.3 Data Acquired with the CryptoPhone

Aftenposten traversed the city center of Oslo while using Cryptophone. The logs from the CryptoPhone were stored in Structured Query Language (SQL) format and interpreted by Aftenposten and professor Josef Noll at the University of Oslo (UiO).

The newspaper registered 470 anomalies with ”VERY_HIGH” suspicion with the CryptoPhone. Aftenposten filtered out several warnings that they claimed could be false positives. These could be due to noise from toll plazas, tunnels, bridges, etc. All the alarms triggered with RxL lower than -93 dBm were dismissed. Aftenposten assessed that in total 384 alarms could be possible false positives, and were thus removed from the further investigation. Amongst these were all the alarms triggered by BP anomaly detection rule no. 4 in Table 5.1, as GSMK states this rule results in many false positives[52]. This resulted in 122 alarms that Aftenposten did not find any alternative explanations for. Figure 5.2 shows the locations of where the CryptoPhone warnings were triggered in Oslo.

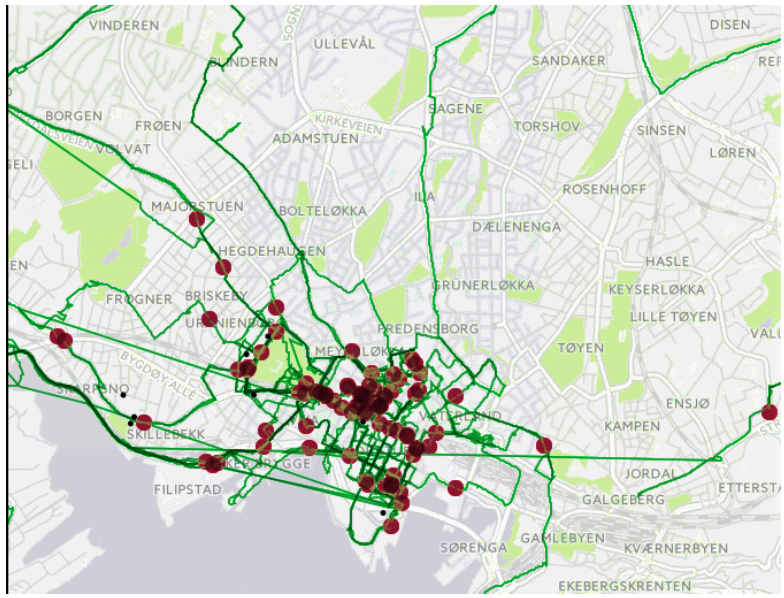


Figure 5.2: Location of CryptoPhone warnings. Modified map from[54]. The red dots represents the majority of the baseband firewall warnings. The green lines represent the route Aftenposten traversed while using the CryptoPhone.

5.2.4 Discussion CryptoPhone Investigations

GSMK claims that the source code of their devices are open source, but the only code they provide on their website is an implementation of VOIP encryption for an old Windows Mobile ME[58]. The implementation of the baseband firewall is not

available on their website. In an email correspondence with GSMK, the source code of the baseband firewall and documentation of the effectiveness of the firewall in terms of detecting IMSI-catchers were requested[59]. The company did not provide the source code, even though they state on their website that all the CryptoPhone products come with full source code for review for anybody. The CryptoPhone products are thus not open source, as the company claims. They did not provide any documentation of the effectiveness of the firewall either. They referred to the incidents in Oslo as proof that the ME can detect IMSI-catchers. The effectiveness of the baseband firewall in CryptoPhone in regards of discovering IMSI-catchers and baseband attacks remains unclear.

GSMK states in the baseband firewall technical briefing[52] that:

> **If you plan to use the BBFW specifically to detect IMSI-Catchers in a specific geographic area**, then it is strongly recommended to focus on the "active connection without ciphering detected" in combination with "no neighbor cells detected" events, especially when a 3G towards 2G network change has happened before them. Other warnings may pop up triggered by specific attack techniques, but not necessarily so. To weed out false positives it is recommended to have a second unit at a different location with a SIM card from the same operator (and, if possible, SIM cards bought at the same store at the same time) and compare the results. If the "no ciphering" warning is displayed simultaneously on both (spatially separated) locations it is likely a network problem (specifically, the network operator's home location register (HLR) having problems with handing out the encryption keys to the base stations due to some error or maintenance). Moving around a suspected IMSI-Catcher's location and verifying whether the warnings can be associated with a specific area is also a good technique to try.

Aftenposten did not use a second unit at a different location as suggested by GSMK.

By performing various SQL queries on the data set acquired with the CryptoPhone, some observations could be made. All of the 122 alarms Aftenposten considered suspicious were triggered by the BP anomaly detection. None of them was triggered by the network anomaly detection, which GSMK state is the most important function in finding IMSI-catchers. Aftenposten did not comment this in the technical description[53]. Since there were no network anomalies amongst the alarms with "VERY_HIGH" suspicion, some observations should be noticed:

1. Encryption was never turned off while the CryptoPhone was used.

2. All the cells the CryptoPhone camped on during the investigation broadcasted neighbor cells.

The CryptoPhone was thus not able to detect any occurrences of these two, very characteristic behavior of IMSI-catchers during the investigations in Oslo.

Figure 5.2 shows the geographical location of all the alarms Aftenposten considered suspicious. The cause of most of these alarms were *"BB data activity detected without OS data activity.* The figure shows that alarms with "VERY_HIGH" suspicion were raised all over Oslo city center.

GSMK were not able to define how often false positives occur, the source code is not open, the warnings were raised all over Oslo, and no network anomalies were observed. Thus, the data acquired from this survey cannot be used to conclude whether IMSI-catchers were deployed in Oslo or not. In addition, Aftenposten did not use a second device at a different location, which was advised by GSMK to rule out some false positives. As there were no "Network Anomaly" warnings, no clear indications of IMSI-catchers were observed during this investigation. All the BP anomalies detected might indicate active attacks, but they might also be false positives. It is unlikely that BP attacks were performed all over Oslo during the investigations.

False negatives may also occur with the CryptoPhone. The ME is not able to detect suspiciously large C2 values, thus IMSI-catchers that broadcast large CRO value will not be detected by the CryptoPhone. The CryptoPhone does not compare the LACs of the cells in the vicinity of the ME to each other. Thus, if an IMSI-catcher chooses a LAC that no other cells in the area use, the CryptoPhone would not be able to detect this. These two operations are very typical for IMSI-catchers.

5.3 Network Guard

5.3.1 About

Network Guard is a device that scans multiple cellular networks by the use of multiple MSs at the same time[60]. It is used for contra espionage purposes in countries all over the world. SIM cards for each network the device is investigating are inserted into the device. In the case in Oslo, these networks were Telenor, Network Norway and NetCom, the PLMNs in Norway at the time. According to the Network Guard documentation[60], Network Guard extracts data from the networks approximately

every four seconds. However, the data acquired in Oslo suggested that it was not so periodic, as the time between measurements ranged from seconds to minutes. The data acquired is subsequently uploaded to a computer that performs various operations on the data.

Network Guard can operate in two different modes, **comparative** and **active**. When the Network Guard device is used in comparative mode, the data extracted from the cellular networks is continuously compared to a reference data set. In the active mode of operation, various algorithms are performed continuously on the data extracted from the networks, without the use of a reference data set. During operation, the Network Guard device will raise alarms indicating that monitoring or interception of traffic is taking place on the cellular network. The alarm is graded from *"LOW"* to *"HIGH"* probability that the network is under attack. According to CEPIA, the Network Guard device is also able to locate the source of the attack equipment to within ten meters[60].

In the investigation in Oslo, only the active mode of operation was used. The data were analyzed against a large database of public maps and multiple sources that Delma and CEPIA have access to. Aftenposten and their experts did not have access to the configuration of the networks, such as the exact location of cells, CIs, LACs, CROs, as this kind of information is not public and seen as confidential by the PLMNs.

5.3.2 Alarms

The Network Guard device raises alarms each time an anomaly is found in the data obtained that appears to be monitoring activity[6]. Table 5.3 shows the possible alarms raised by the device.

Delma graded the various alarms by severity. The different severity gradings of the alarms are explained in Table 5.4.

Table 5.3 Possible alarms raised by Network Guard. Note that alarm 4 and 6 have identical description in the forensic analysis report from Delma[6, 61].

	Alarm	**Explanation**
1	Channel LAC change	LAC has changed on a given channel.
2	Channel Cell Change	Cell ID has changed on a given channel.
3	Cell LAC Change	The LAC has changed on a given cell. The LAC changes, but the cell ID and ARFCN are unchanged.
4	Cell Reselect Change	An abnormal change in the C1 and / or C2 value on the cell.
5	Duplicated cell	The same cell ID is used on multiple networks in the same area.
6	C anomaly	An abnormal change in the C1 and / or C2 value on the cell.
7	Service Denial	The MSs camping on the cell is denied service, i.e. the MSs does not have a the possibilty to place or receive calls or text messages.
8	Neighbor cell suppression	Cell does not publish a neighbor list.
9	Provider Anomaly	The BTS publishes a neighbor list with an ARFCN that is used by another PLMN.

Table 5.4 Explanation of the different alarm gradings in Network Guard[6, 61].

Severity	**Explanation**
”LOW”	Network characteristics which make it easier for undetected monitoring to take place. Probability of network monitoring is slight.
”MEDIUM”	Network characteristics which make it easier for undetected,monitoring to take place. Probability of network monitoring is greater.
”HIGH”	Definite and high probable examples of various forms of monitoring.

5.4 Measurement Details

Aftenposten and their collaborators performed three surveys in December 2014 in Oslo with the Network Guard device. The first was performed 03.12.2014-04.12.2014, the second was performed 10.12.2014-11.12.2014, and the third was performed 22.12.2014. The first two surveys were performed both in the morning and the evening. The third survey the 22.12.2014 was performed from 09.15 to 14.00. Aftenposten did not publish the data they acquired from the last survey.

The data from the two first surveys were published on [53]. The data from the third survey was provided by Aftenposten by email the 14.05.2015. The data was provided in Microsoft Excel format. The data provided by email was manually parsed from Excel format to SQL format to enable thorough analysis.

The 16th and 17th of April, Aftenposten performed their last survey in Oslo. The last survey was a check survey performed at the locations where they detected anomalies in the first surveys. The data from this survey were not released by Aftenposten. This analysis is based on the data from all the surveys performed by Aftenposten in December 2014.

Some surveys were static, and some were mobile. During the static surveys, the Network Guard device was located at the same location for a longer period. During the mobile surveys, the Network Guard was moved, either by car or by foot.

The device operates in ”slots”, one slot for each PLMN it is investigating. In the investigations in Oslo, there were three slots, one for Network Norway, one for Telenor and one for NetCom. The respective SIM cards subscribing to the different PLMNs are inserted into the slots. The Network Guard cycles through the slots. When in a slot, the device performs measurements from all the cells the Network Guard monitors at that time.

Each measurement includes some information gathered from the system information messages, as well as the calculated C1 and C2 values. The Network Guard monitors the serving cell and up to six cells in the BA list with the largest RxL. In general, the Network Guard logs the selection and reselection procedures. The time between the measurements of the different slots differed greatly, from seconds to minutes. The most important data that is logged in each measurement is described in Table 5.5.

Table 5.5 Data logged with each measurement made with the Network Guard device.

Field	Description
ID	Measurement identifier
Date	Date of measurement
Time	Time of measurement
MNC	Mobile Network Code
LAC	Location Area Code
Cell ID	Measured Cell ID
Slot	The slot the measurement is made on
RxL	Received Signal Strength
ARFCN	Absolute Radio Frequency Number
Lat	GPS Latitude of the measurement
Long	GPS Longitude of the measurement
CellType	Either ”S cell”, serving cell, or ”A cell”, adjacent cell. Serving cell is the cell the Network Guard camps on. Adjacent cells are cells from the BA list of the serving cell.
C1	Path Loss Criterion parameter
C2	Reselection Criterion
BSIC	Base station Identity Code
Alarm	If an alarm is raised on the measurement, this field determines the type of alarm.

5.5 Network Observations in Oslo

The investigation with the Network Guard device resulted in a significant amount of data of how the BTSs in Oslo were configured. Several observations of the configuration of the networks in Oslo can be made by analyzing the data. The observations are based on all the data acquired by Aftenposten from the three first surveys, i.e. in total 42109 distinct measurements. The observations made in this section are used in further analysis of the anomalies Aftenposten detected in Section 5.6. The route traversed with the Network Guard device is shown in Figure 5.3.

Figure 5.3: The route traversed with the Network Guard device in Oslo. Modified map from [54].

5.5.1 Overview

Some noteworthy data is presented in Table 5.6. The newspaper observed three LACs in Telenor's network, five in NetCom's network and three in Network Norway's network. The different PLMNs have configured their BTSs differently.

By comparing the observed C2 and C1 values from the data with the reselection criterion equation shown in Equation 2.3 in Chapter 2, it is possible to determine the values of the reselection parameters the BTSs in Oslo broadcasted during the investigation.

It was found that NetCom used the CRO and TO in some cells. Telenor used TO in some cells while Network Norway did not use the cell reselect parameters at all for their BTSs. From the data published by Aftenposten, one can observe that when the TO of a cell is set to 7 (infinity), the C2 value is -1 during PT. This value was used by 77 cells in NetCom's network.

The CRO and TO values were not mentioned by Delma or Aftenposten. Delma mentioned that the differences between C1 and C2 sometimes were 30 dBm on NetCom's network and 20 dBm on Telenor's network, but did not relate them to the actual values of the parameters. These differences were used to set alarm thresholds

Table 5.6 Observations of the configuration of the GSM networks in Oslo from the data published by Aftenposten.

PLMN	Cells	LAs	CRO	TO
Telenor	278	4	0 (0 dBm)	2 (20 dBm) 58 cells 0 (0 dBm)
NetCom	297	5	15 (30 dBm) 19 cells 0 (0 dBm)	7 (infinity) 77 cells 0 (0 dBm)
Network Norway	209	3	0 (0 dBm)	0 (0 dBm)

for alarm 4 and 6 in Table 5.3. Since Delma did not relate the values to the actually observed broadcasted parameters, many possible false positive alarms were triggered, which will be discussed later.

5.5.2 Telenor

Figure 5.4 shows the geographical location of the best measurements in terms of RxL of the 57 cells with a behavior that suggested that they published a TO=2 (20 dBm) in Telenor's network. The recordings done with the Network Guard device did not suggest that any of the Telenor cells used a CRO different than 0.

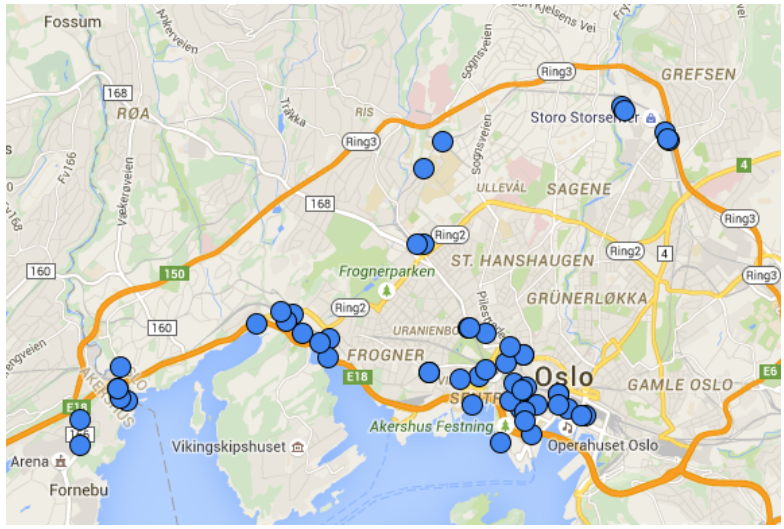


Figure 5.4: Recordings with largest RxL of cells with TO=2 (20 dBm) in Telenor's network. The blue points represent cells with TO=2.

Observed PT on the Telenor cells where this timer expired was approximately 5 minutes. All the cells in Telenor's network that behaved as they published TO=2

operated in the 1800 MHz band. There were observed four different LACs used by Telenor cells, LAC={11801,11901,12001,12901}.

5.5.3 NetCom

Figure 5.5 shows the geographical location of the best measurement in terms of RxL of the 19 different cells in NetCom's network with a behavior that suggested that they published a CRO=15 (30 dBm), and the 77 cells in NetCom's network with a behavior that suggested that they published a TO=7 (infinity). All the cells that behaved as if they broadcasted a CRO=15 also behaved as if they broadcasted a TO of 7 (infinity) and a PT of approximately four minutes. Neither of the 58 other cells measured with a probable TO of 7 (infinity) was ever measured with a C2 > -1. This means that for these cells, the PT did not expire as the Network Guard device observed them. It is thus possible that all the 77 cells that behaved as they broadcasted a TO of 7 (infinity) also broadcasted a CRO of 15 (30 dBm).

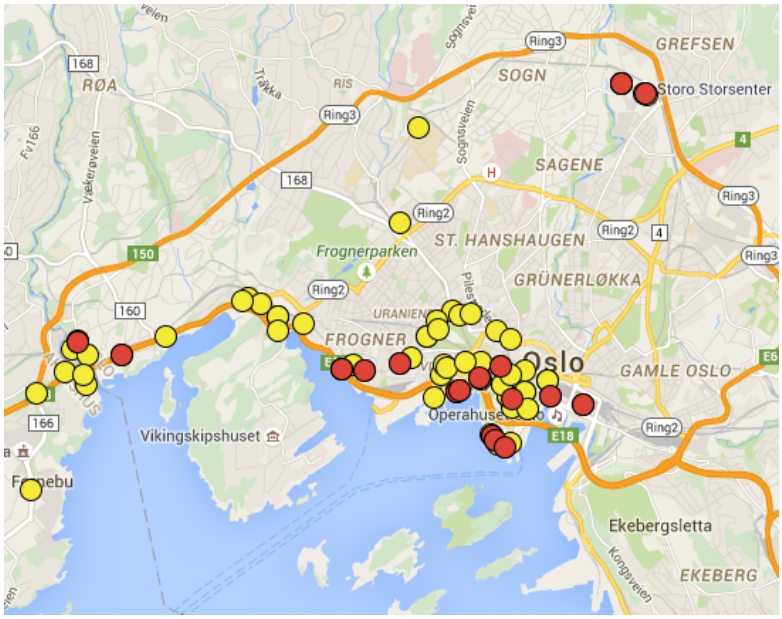


Figure 5.5: Recordings with largest RxL of cells with CRO=15 (30 dBm) or TO=7 (infinity) in NetCom's network. The yellow plots represent recordings of cells with TO=7, the red plots represent cells with CRO=15.

All the NetCom cells that behaved as they published CRO=15 or TO=7 operated on the 1800 MHz band. There were observed five different LACs used by NetCom cells, LAC={3801,3802,3803,3804,3805}.

5.5.4 Network Norway

In all the measurements of Network Norway cells in Oslo C1=C2, which means that for all Network Norway cells, CRO=0, TO=0 and PT=0. There were observed three different LACs used by network Norway cells, LAC={2310,2311,2320}.

5.6 Network Anomalies Detected with Network Guard

Aftenposten and the companies they hired detected several anomalies in the network, which they argued in varying degrees could be IMSI-catchers. In this section, some of the network anomalies discovered with the Network Guard will be discussed. The data is discussed with regards of the GSM standard, common characteristics of IMSI-catchers and compared to observations from Section 5.5, with the goal of deducing whether the anomalies were caused by active attacks or not.

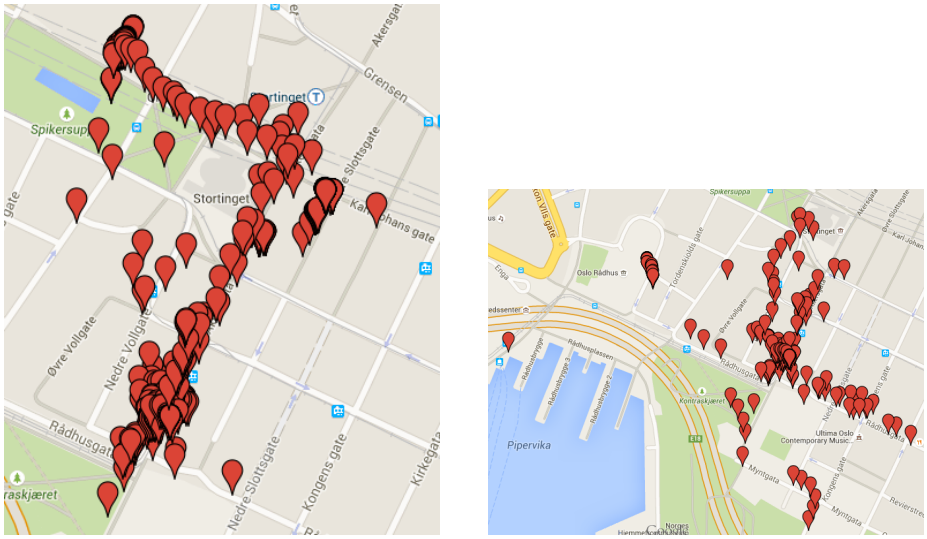
In April 2015, Delma provided Aftenposten with a draft of a network forensic analysis of the data obtained in Oslo[6]. This document contained previously unpublished arguments for all the anomalies discovered. The finished version of the report was provided by email in May 2015[61]. It included notes from the check surveys done in April. Aftenposten wrote a report in Norwegian with analysis of each alarm[5]. These reports were provided by email from Aftenposten before they were published. The arguments and data provided in the reports by Delma and Aftenposten will be discussed in this section. All of the alarms Delma graded to "HIGH" severity are discussed. In addition, some alarms that were emphasized by either Aftenposten or Delma, graded to "MEDIUM" by Delma are discussed.

5.6.1 NetCom Cell 3629

The investigations in Oslo found cells with CI 3629 operating on two different networks, Telenor and NetCom. In the technical description published by Aftenposten in January 2015, they state that the BTS with CI 3629 operating on NetComs network was "most likely" an IMSI-catcher[53]. They claimed that the operation on Telenor's network seemed normal, while the operation on the NetCom network seemed very suspicious.

Figure 5.6 shows all the measurements made of cell 3629 in Oslo during the investigations. From the figure, one can observe that the two cells were observed in the same approximate area, close to the Norwegian parliament.

Aftenposten and their experts also argued that the C2 value of the NetCom cell displayed suspicious fluctuations, and that the cell exhibitted anomalous behavior. This was the main argument that cell 3629 in NetCom's network was an IMSI-catcher. All the alarms raised in regards of cell 3629 with MNC=2 were graded to



(a) Cell 3629 on Telenor network. **(b)** Cell 3629 on NetCom network.

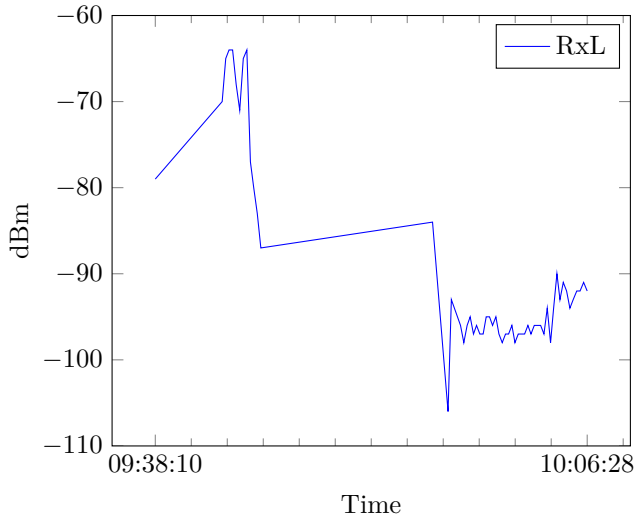
Figure 5.6: Measurements of cells with CI 3629.

"MEDIUM" severity by Delma. Cell 3629 on NetCom's network was observed all the days Aftenposten performed surveys in Oslo. The cell was measured in total 658 times. These measurements includes measurements of the cell as both serving cell and as adjacent cell.

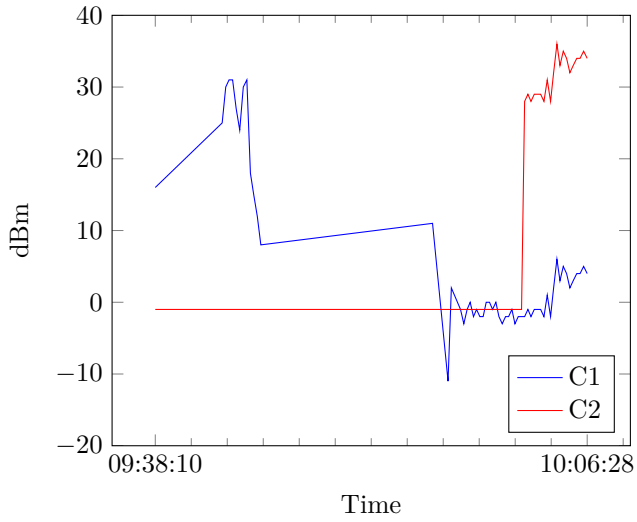
Duplicated Cell

The fact that two different PLMNs each have a cell with the same CI in the same approximate area is somewhat strange. The CI is a 16-bit value and is not chosen according to a standard, but rather decided by the PLMNs themselves[14]. It is thus unlikely that two different PLMNs each have a cell with the same CI in the same approximate area by chance.

PST had access to network and BTS configurations of the PLMNs, and claimed that both PLMNs have a legitimate cell with CI in the area. This was also confirmed by the PLMNs in an email correspondence between Aftenposten and the PLMNs[5]. Aftenposten and their collaborators later acknowledged in their reports that the CI exists on both networks. Thus, the fact that the Network Guard detected the CI on two different networks in this area is not suspicious, it is a part of the configuration of the two networks in Oslo.



(a) RxL from NetCom cell 3629 the 03.12.2014 between 09:38:11 and 10:06:29.



(b) C1 and C2 values from NetCom cell 3629 the 03.12.2014 between 09:38:11 and 10:06:29.

Figure 5.7: Observed RxL, C1 and C2 values from NetCom cell 3629 the 03.12.2015 from 09:38:11 to 10:06:29

C Anomaly

The C1, C2 and RxL of NetCom cell 3629 between 09:38 and 10:06 from the investigation the 03.12.2014 is shown in Figure 5.7. The figure shows an example of

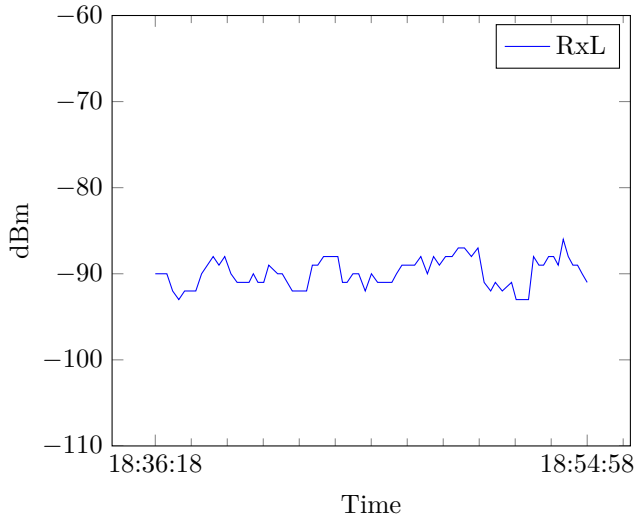
the fluctuations that Aftenposten and Delma claimed were unusual. The example was used in both the report of Aftenposten and the report of Delma. Delma argued that the C2 value variation was "unclear". The "C Anomaly" alarm was raised for this cell because the difference between the C1 and the C2 value sometimes were greater than 30, $|C2 - C1| > 30$.

From Figure 5.7, one can observe that the RxL from the cell and the C1 values correlate. From Figure 5.7a, it is plausible to conclude that the Network Guard device was moving away from the BTS broadcasting the signal, which can be observed by how the RxL value drops from around -60 dBm to around -100 dBm between 09:44 and 09:58.

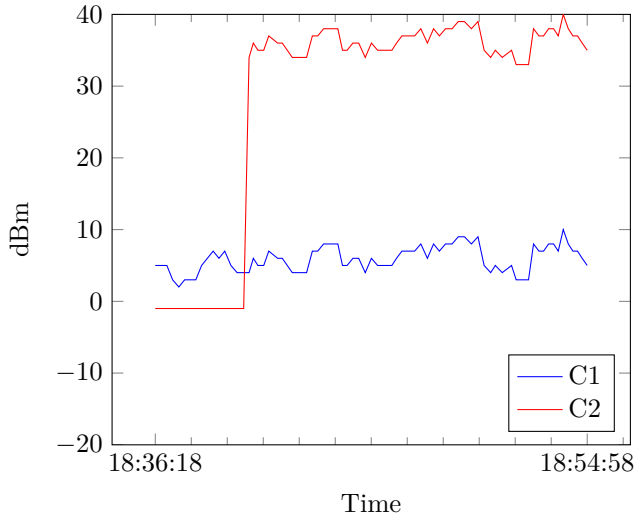
There are no suspicious spikes in the plot that suggests that an IMSI-catcher was turned on with the same CI, LAC and ARFCN during this time, or that the source of the signal originated from multiple BTSs. The reason why the plot is not very smooth, is that the cell was not observed continuously in all the measurements of the slot of the NetCom SIM between 09:30:10 and 10:06:08.

In all the measurements of cell 3629 on NetCom's network, C1-RxL = 95 dBm. The C1 value was thus larger than the RxL by a constant factor in all of the measurements of the cell. Thus, the RXLEV_ACCESS_MIN, MS_TXPWR_MAX_CCH and P were all static values. As RXLEV_ACCESS_MIN and MS_TXPWR_MAX_CCH are broadcasted by the cell and P is the maximum RF output of the Network Guard device, the difference between C1 and RxL should normally be static. Thus, it can be concluded that the measured values of C1 did not perform any unusual fluctuations. The behavior was normal. 72 other cells in NetCom's network were observed with the same difference between C1 and RxL, C1-RxL = 95 dBm.

It was the C2 behavior of the cell that Delma and Aftenposten found most suspicious. In Figure 5.7 the C2 is -1 from the first measurement of the cell at 09:38:11 until 10:02:23, 54 minutes later. The cell was, however, not continuously measured during this time, which is the reason for why the C2 value was -1 for such a long time. The cell was not observed continuously long enough for PT to expire until 10:02:23, when the cell had been measured continuously from 09:57:59. In all the following measurements of the cell when it was in the vicinity of the Network Guard device, the C2 value was consistently 30 dBm larger than the C1 value. This coincides with a CRO value of 15 (30 dBm), a TO value of 7 (infinity) and a PT of approximately 4 minutes. In Section 5.5.1 it was shown that this is a somewhat normal configuration in NetCom's network in Oslo based on the measurements made by Aftenposten. 19 cells were observed with this exact configuration. Several more might have the same configuration, as many cells with a TO of infinity were not observed after the PT. The C2 behavior was identical for all measurements made of cell 3629 with



(a) RxL from NetCom cell 3629 the 03.12.2014 between 18:36:19 and 18:54:58.



(b) RxL from NetCom cell 3629 the 03.12.2014 between 18:36:19 and 18:54:58.

Figure 5.8: Observed RxL, C1 and C2 values on NetCom cell 3629 the 09.12.2015 from 18:36:19 to 18:54:58

MNC=2. Thus, the observed C2 value did not display any suspicious fluctuations, as Aftenposten argued.

In the forensic analysis by Delma[6, 61], they claimed that the behavior of the cell during the investigation six days later, 09.12.2014, was ”more in line with

expectations". They did not define what these expectations were. The measurements of the cell made the 09.12.2014 were from a static survey, i.e. the Network Guard device did not move during this survey. In Figure 5.8, the RxL, C1 and C2 values of cell 3629 in NetCom's network between 18:36:19 and 18:54:58 are plotted. Delma argued that the behavior between 18:39 and 18:55 this day was more in line with the expectations, and backed this with a plot of the RxL, C1 and C2 values of the cell between 18:36:19 and 18:54:58. Delma's plot showed a PT of approximately 2 minutes. The cell was, however, observed by the Network Guard for several measurements before 18:39. It was first measured at 18:36:19, and was continuously measured until 18:54:58. The data from these measurements were not included in Delma's plot. In Figure 5.8 these data are included. The cell was first discovered by the Network Guard device at 18:36:19. The C2 value was -1 for four minutes until 18:40:22. In all the following measurements of the cell, the C2 value was 30 dBm greater than the C1 value. In all the measurements of the cell, the C1 value was 95 dBm greater than the RxL. The observed behavior thus coincides with CRO=15 (30 dBm), TO=7 (infinity) and PT=12 (4 minutes). Thus, the behavior of the cell the 09.12.2014 between 18:36:19 and 18:55:10 was not different from the behavior of the cell the 03.12.2014 between 09:38:11 and 10:06:43. The behavior was consistently the same on the two measurements, six days apart. The behavior Delma claimed was "more in line with expectations" was identical to the behavior Delma claimed was "unclear".

In the report made by Aftenposten in May 2015[5], the journalists argued that the Network Guard device registered unusual RxL fluctuations when the device moved while measuring the cell. The example that was highlighted by Aftenposten was the RxL behavior the 04.12.2014 between 12:43 and 12:45. During this time, the Network Guard moved 22 meters, and the RxL dropped from -68 dBm to -86 dBm, thus a difference of 18 dBm. These fluctuations are to be expected, as the Network Guard was moving, most likely away from the cell. In addition to the moving of the measuring device, there might be several other reasons for this fluctuation, for instance that physical obstacles occurred between the cell and the Network Guard device.

Because the threshold of the "C Anomaly" alarm was set to 30 dBm, as described in Section 5.5.1, the alarm was raised every time the RxL was greater than -65 dBm during the PT. The TO of the cell was set to infinity, which means that C1-C2>30 dBm when RxL>-65 dBm. The observed differences between C1 and C2 were thus not suspicious for this cell, and all the alarms of this nature related to this cell can be considered as false positives. The alarms were raised because Delma and their collaborators did not relate their alarm threshold to the actual parameters broadcasted by the BTSs in Oslo.

Discussion Cell 3629

The use of PT and TO with values observed as the ones for this cell is not a typical behavior for an IMSI-catcher. Since both parameters are optionally broadcasted by the cell, and the purpose of the parameters is to prevent MSs to camp on the cell during the PT, this configuration would not benefit an attacker. In general the cell would need to be in close vicinity of the MSs during a time of at least four minutes for the attacker to catch any IMSIs. An IMSI-catcher with this configuration would not be very effective. Typical behavior for IMSI-catchers is to boost C2 value, not decrease it. The cell is also boosting the C2 value after the PT, by broadcasting a CRO of 15 (30 dBm), but as shown in Table 5.6, this is not an unusual configuration in NetCom's network. The behavior of the cell was consistent in all surveys performed.

It should also be mentioned that all the observed neighbor cells of cell 3629, i.e. all the "A cells" that were measured at the timestamps cell 3629 were measured as "S cell", on NetCom's network had the exact same LAC as cell 3629, LAC=3804. IMSI-catchers will typically choose a different LAC than the neighbor cells in order to force a location update.

The behavior of cell 3629 on NetCom's network was not suspicious compared to other cells operating in NetCom's network, the GSM standard and typical behavior of IMSI-catchers. Since NetCom confirmed that there was a cell with this CI in the area, this cell was most likely a legitimate BTS and not an IMSI-catcher.

5.6.2 NetCom Cell Nydalen

During a mobile survey the 22.12.2014, the Network Guard registered both a "Channel LAC change" alarm and a "system denial" alarm. The incident was graded to "HIGH" severity by Delma. The geographical location of the incident is shown in Figure 5.9.

The measurements made on the NetCom slot around the time of the measurement that lead to the alarms are shown in Figure 5.10. The observation was done very close to the PST headquarter at Nydalen.

The measurement highlighted in Figure 5.10 was the only "No GSM" measurement where the LAC observed was different from 0. The observation was made on the NetCom slot. The observed LAC in the measurement was 11901, a LAC used by Telenor cells nearby.

According to Aftenposten and Delma, the "No GSM" measurements means that the Network Guard "loses signal" to the cell. They were not able to explain this in greater details, but it might mean that the Network Guard was not able to read system information messages on the BCCH. There could be many reasons for why the device was not able to read system information messages, for instance, the use

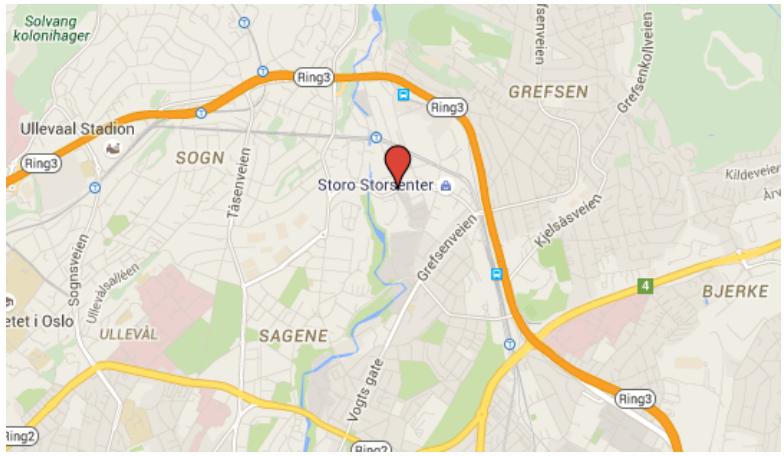


Figure 5.9: Geographical location of the channel LAC change and system denial incident.

time	lac	cellid	rxl	arfcn	celltype	c1	c2
12:08:32	3805	51783	-88	12	S Cell	23	23
12:08:32	3805	51787	-92	721	A Cell	3	-1
12:08:51	11901	0	-200	0	No GSM	0	0
12:09:17	3805	24063	-106	12	S Cell	5	5

Figure 5.10: Measurements made on the slot of the NetCom SIM around the time of the ”System Denial” incident.

of a jamming device in the area, the RxL from the cell became too small or the BP on the ME experienced troubles at the time. There are in total 737 ”No GSM” measurements in the data set. Delma only graded two of them suspicious, including this incident. The other ”No GSM” incident that was marked as suspicious is also discussed in this chapter.

How the Network Guard was able to detect a LAC at the same time a ”No GSM” observation was made is unclear. It is questionable how the Network Guard would be able to read the LAC value, but no other values, for instance CI. The Network Guard was not able to detect what ARFCN the LAC was observed on or able to measure the RxL. The question was raised to Aftenposten, but they could not provide an answer for how this could be possible.

From Figure 5.11 it can be observed that the observed LAC at the time of the alarm was identical to the last LAC measured in the previous slot. The last measured LAC from the previous slot is stored in the previous row in the data set.

time	mnc	lac	cellid	rxl	arfcn	celltype	c1	c2
12:08:46	1	11901	3573	-111	59	S Cell	0	0
12:08:51	2	11901	0	-200	0	No GSM	0	0
12:09:03	5	2310	1383	-93	982	S Cell	11	11

Figure 5.11: Measurements from all slots around the time of the "System Denial" incident. LAC observed on the "No GSM" measurement is the same as the LAC observed on the previous slot.

Neither of the observed cells in the area displayed any typical IMSI-catcher behavior. All the cells behaved according to the observed behavior of NetCom's network. Some of the cells in the area had a CRO of 15 (30 dBm) and some had a CRO of 0. The NetCom cells observed in the area broadcasted a LAC of either 3804 or 3805.

It is possible that this alarm was raised by a measurement error or bug in the Network Guard software. However, it is possible that the Network Guard camped on the cell, the location update was rejected immediately and this is how it is represented by the Network Guard. It cannot be validated how the Network Guard represents an immediate location update reject, as no technical description of the Network Guard is published and the source code of the software is not open source.

5.6.3 Cell LAC Changes

In the surveys performed by Aftenposten, six cells were observed changing LAC. There are two scenarios that could cause this alarm to be raised; one cell changes the value of the LAC broadcasted in the system information messages, or two cells are using the same CI in the area on the same ARFCN with different LACs and the MS reads the system information messages from the BTS with the largest RxL, first from one BTS then the other.

The observed behavior of these cells were so similar, that they are discussed together in this section. Observations of each incident are first described and discussed, to determine whether the LAC changes were caused by multiple BTSs or if it was caused by one BTS changing the LAC in the system information messages. At the end of this section, all the cells that performed LAC changes are compared and discussed.

Telenor Cell 3107

During a static survey the 09.12.2014 two Telenor cells, cell 3107 and 3218, were observed switching LAC. This caused alarm 3 in Table 5.3 to be raised. The severity was defined to "HIGH" by Delma. The anomalies detected with regards of cell 3107 is discussed in this section. Cell 3218 is discussed later. The geographical location of

where the survey was conducted is shown in Figure 5.12. The survey was performed between 18:36:08 and 20:54:55.

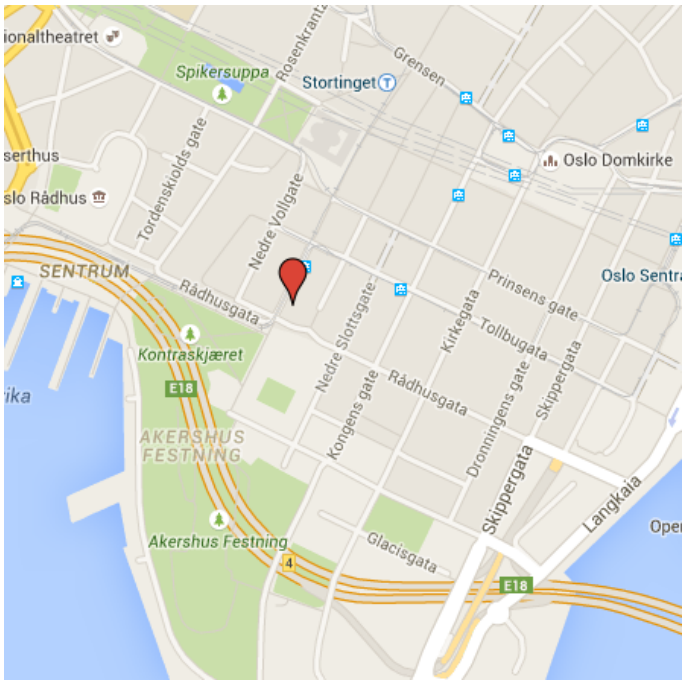


Figure 5.12: The geographical location of the survey 09.12.2014.

Cell 3107 was observed changing LAC two times the 09.12.2014. Both times it changed from 11901 to 2311, which is a LAC used by nearby cells in Network Norway's network. The LAC 11901 was used by all the other Telenor cell's observed in the static survey the 09.12.2014.

CI 3107 was observed all the days Aftenposten performed surveys in Oslo. The CI was measured in total 893 times. In all the measurements of the cell, C1 and C2 were equal. Thus, the CRO and TO broadcasted by the cells were consistently 0 all the days measurements of the cell were made. The cell was always observed operating on ARFCN 67. In all the measurements made of CI 3107, the difference between C1 and RxL was constant. Cell 3107 broadcasted a LAC of 11901 all the days it was observed.

Cell 3107 was the first cell the Network Guard camped on when on the Telenor slot during the static survey the 09.12.2014. The Network Guard device first camped on the cell at 18:36:16 and was camped on the cell until 18:51:40 when a "No GSM" measurement was made. After this measurement, the device camped on cell 3218,

time	lac	cellid	rxl	arfcn	celltype	c1	c2
18:40:31	11901	3107	-85	67	S Cell	26	26
18:40:42	11901	3107	-89	67	S Cell	22	22
18:40:57	11901	3107	-87	67	S Cell	24	24
18:41:10	11901	3107	-86	67	S Cell	25	25
18:41:25	2311	3107	-92	67	S Cell	19	19
18:41:45	11901	3107	-90	67	S Cell	21	21
18:41:58	11901	3107	-89	67	S Cell	22	22

(a) Cell 3107 switches LAC at 18:41:25.

time	lac	cellid	rxl	arfcn	celltype	c1	c2
18:50:28	11901	3107	-93	67	S Cell	18	18
18:50:44	11901	3107	-97	67	S Cell	14	14
18:50:58	11901	3107	-95	67	S Cell	16	16
18:51:11	2311	3107	-97	67	S Cell	14	14
19:32:50	11901	3107	-77	67	S Cell	34	34
19:33:03	11901	3107	-78	67	S Cell	33	33

(b) Cell 3107 switches LAC at 18:51:11.

Figure 5.13: Measurements from the slot of the Telenor SIM in the time around the LAC changes observed on cell 3107.

which will be discussed later.

The LAC changes occurred at 18:41:25 and 18:51:11. The observed LAC of the cell changed from 11901 to 2311. Excerpts from the data showing the measurements made of cell 3107 in the time around the LAC changes are shown in Figure 5.13. The LAC changes are highlighted in the figure.

Figure 5.14 shows the RxL from the cell between 18:36:16 and 18:51:11. From the figure, it does not seem that a rogue BTS was turned on at the time of the LAC changes, because the RxL did not perform any large fluctuations in these timestamps.

The cell was observed again at the same location at 19:32:50. The Network Guard device camped on the cell until the survey was over, at 20:54:45. Figure 5.15 shows the RxL from the cell during this time. The RxL values are similar to the ones observed in Figure 5.14 and there is no reason to believe that the source of the signals between 19:59:37 and 20:54:45 was another BTS than the source of the signals observed between 18:36:16 and 18:51:11. This means that if there was an IMSI-catcher spoofing cell 3107 in the area the 09.12.2014, it was likely the source of all the measurements made of cell 3107 that day.

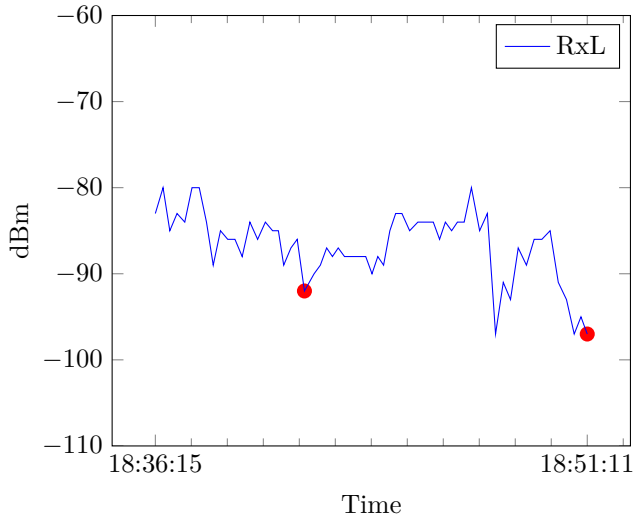


Figure 5.14: RxL from cell 3107 the 09.12.2014 between 18:36:15 and 18:51:11. The red points represents the time LAC changes were observed.

Since there were made measurements of CI 3107 in the same approximate area during other surveys, the RxL observed the 09.12.2014 can be compared to the RxL observed in the same approximate area the other days there were made measurements of the cell. By doing this, it is possible to get an idea of whether there were different signal sources of this CI the different days. All the RxL measurements of cell with CI 3107 made in the area represented by the blue circle in Figure 5.16 from the other surveys, are compared with the RxL measurements from the survey 09.12.2014. The results are shown in Table 5.7.

Table 5.7 Average RxL and the standard deviation from all the measurements of cell 3107 in the same approximate location as where the survey the 09.12.2014 was performed.

Date	**Number of measurements**	**Average RxL**	**Std RxL**
04.12.2014	1	-78 dBm	0
09.12.2014	220	-84.53 dBm	4.19
10.12.2014	38	-78.95 dBm	3.69
11.12.2014	79	-85.83 dBm	5.88
22.12.2014	1	-101 dBm	0

From Table 5.7 one can observe that the RxL from cell 3107 was similar most of the days the cell was observed in the in the same approximate location of where the survey the 09.12.2014 was performed. The observed RxL observed the 22.12.2014

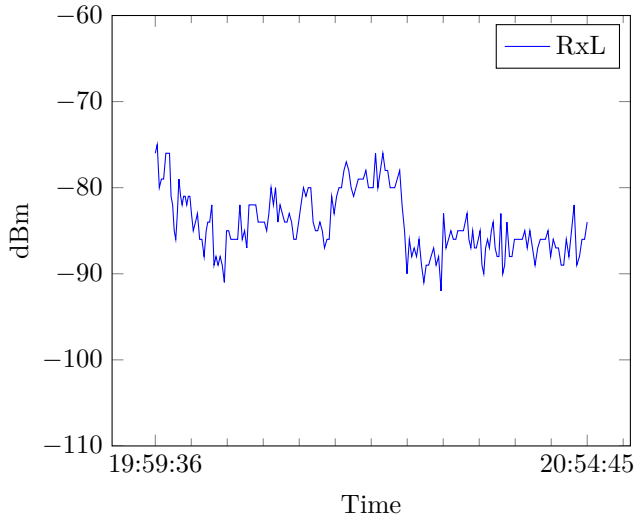


Figure 5.15: RxL from cell 3107 the 09.12.2014 between 19:32:49 and 20:54:45.

stands out from the others, but since only one measurement of the cell was made in the area that day, this individual measurement should not be used to draw any conclusions. There were also individual measurements of the cell the 09.12.2014 with similar RxL as this measurement.

From the results in Table 5.7, it can be observed that the RxL from cell 3107 in the area was very similar the 04.12.2014, 9.12.2014, the 10.12.2014 and the 11.12.2014 in the same approximate location. It is thus likely that the same source broadcasted the signals with CI 3107 all these days. That means that if an IMSI-catcher was in fact spoofing cell 3107 the 09.12.2014, it was likely operating the other days investigations were performed as well.

Cell 3218 Telenor

Cell 3218 on Telenor's network was observed changing LAC during the investigation the 09.12.2014 in Oslo. This caused alarm 3 in Table 5.3 to be raised. The severity was graded to "HIGH" by Delma.

The cell was observed all the days investigations were performed in Oslo. In total 896 measurements of the cell were made with Network Guard. C2 was equal to C1 in all the measurements of the cell. This means that CRO and TO was set to 0 all the days the cell was measured. The difference between C1 and RxL was static for all meaurements of the cell. ARFCN 53 was used by the cell all the days it was observed. The cell broadcasted LAC 11901 all the days it was observed.

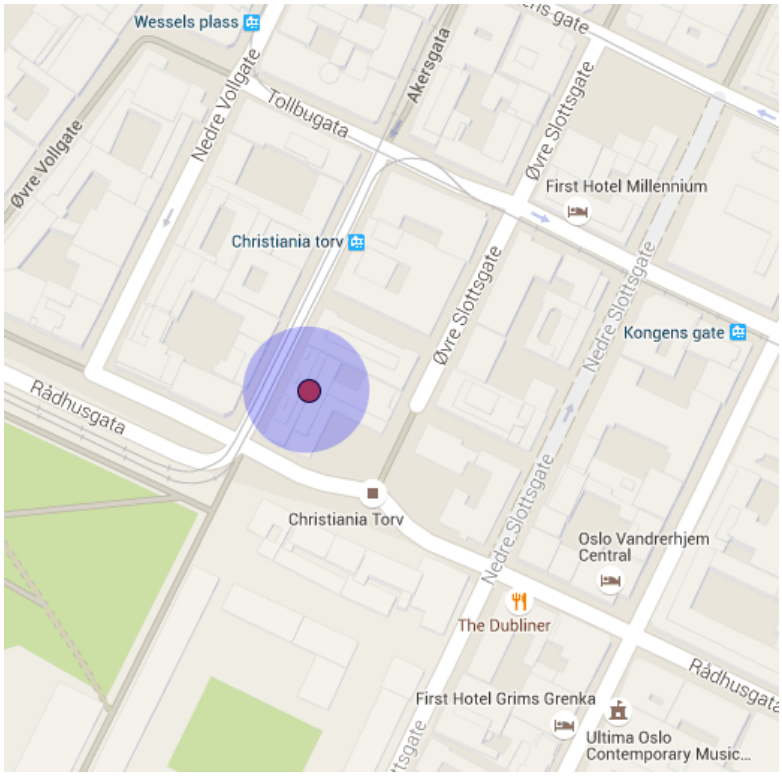


Figure 5.16: The blue circle represents the area RxL from measurements from other surveys are compared to the RxL from the static survey the 09.12.2014. The red dot represents the geographical location of the survey the 09.12.2014.

The cell was observed changing LAC two times during a static survey the 09.12.2014, that caused the Network Guard device to raise alarms. The changes happened respectively at 18:52:08 and 18:59:01. During this survey the device moved less than 5 meters in total. In both the LAC changes, the LAC changed to 2311, a LAC used by Network Norway cells in the area. Geographical location where survey was performed is shown in Figure 5.12.

The static survey the 09.12.2014 was initiated at 18:36. The Network Guard device quickly camped on cell 3107 on the slot of the Telenor SIM. Cell 3107 was the serving cell until the Network Guard reselected to cell 3218 at 18:51:52. During the time cell 3107 was the serving cell, 3218 was not measured as adjacent cell. This could indicate that the ARFCN of CI 3218 was not in the BA list of CI 3107. Figure 5.17 shows that CI 3218 was not measured as ”A cell” when CI 3107 was ”S cell”.

Since the ARFCN of cell 3218 was probably not in the BA list of cell 3107, MSs camped

time	lac	cellid	rxl	arfcn	celltype	c1	c2
18:49:54	11901	3107	-85	67	S Cell	26	26
18:49:54	11901	23013	-97	682	A Cell	13	-7
18:49:54	11901	3106	-91	55	A Cell	19	19
18:49:54	11901	3216	-103	123	A Cell	7	7
18:49:54	11901	3067	-105	124	A Cell	5	5

Figure 5.17: Measurements made by Network Guard at 18:49:54 the 09.12.2014. Cell 3218 was not observed at this time.

on cell 3107 would normally not reselect to cell 3218. The reason why the Network Guard device reselected to cell 3218 from cell 3107 was that the measurement before the reselection was a "No GSM" measurement, as can be observed in Figure 5.18.

time	lac	cellid	rxl	arfcn	celltype	c1	c2
18:51:11	2311	3107	-97	67	S Cell	14	14
18:51:11	11901	23013	-99	682	A Cell	11	-9
18:51:11	11901	3106	-94	55	A Cell	16	16
18:51:11	11901	3830	-102	68	A Cell	8	8
18:51:11	11901	3216	-104	123	A Cell	6	6
18:51:40	0	0	-200	0	No GSM	0	0
18:51:52	11901	3218	-87	53	S Cell	24	24
18:52:08	2311	3218	-88	53	S Cell	23	23
18:52:36	11901	3218	-89	53	S Cell	22	22
18:52:50	11901	3218	-87	53	S Cell	24	24

Figure 5.18: "No GSM" measurement results in camping on 3218.

The "No GSM" measurement at 18:51:40 forced the Network Guard to initiate a cell selection procedure, which in turn resulted in a selection of cell 3218. No neighbor cells of cell 3218 were observed while it was the serving cell, which can be observed from Figure 5.18. This could mean that the cell broadcasted an empty BA list, which is something some IMSI-catchers do in order to force the MSs to camp on the cell for as long as possible, but it could also mean that the Network Guard was not able to decode messages on the ARFCNs in the BA list.

The LAC changes of cell 3218 occurred at 18:52:08 and 18:59:01. Figure 5.19 shows excerpts from the measurements on the slot of the Telenor SIM around the time cell 3218 was observed changing LAC. The LAC changes are highlighted in the figure.

In Figure 5.20, the RxL from all the measurements of cell 3218 the 09.12.2014 is plotted. The figure does not display any large fluctuations in RxL. It is thus likely

time	lac	cellid	rxl	arfcn	celltype	c1	c2
18:51:52	11901	3218	-87	53	S Cell	24	24
18:52:08	2311	3218	-88	53	S Cell	23	23
18:52:36	11901	3218	-89	53	S Cell	22	22
18:52:50	11901	3218	-87	53	S Cell	24	24
18:53:03	11901	3218	-87	53	S Cell	24	24

(a) Cell 3218 switches LAC at 18:52:08.

18:58:22	11901	3218	-88	53	S Cell	23	23
18:58:35	11901	3218	-87	53	S Cell	24	24
18:58:48	11901	3218	-87	53	S Cell	24	24
18:59:01	2311	3218	-86	53	S Cell	25	25
18:59:25	11901	3218	-87	53	S Cell	24	24
18:59:38	11901	3218	-86	53	S Cell	25	25

(b) Cell 3218 switches LAC at 18:59:01.

Figure 5.19: The two LAC changes observed on cell 3218.

that the received signals originated from the same source in all the measurements the 09.12.2014.

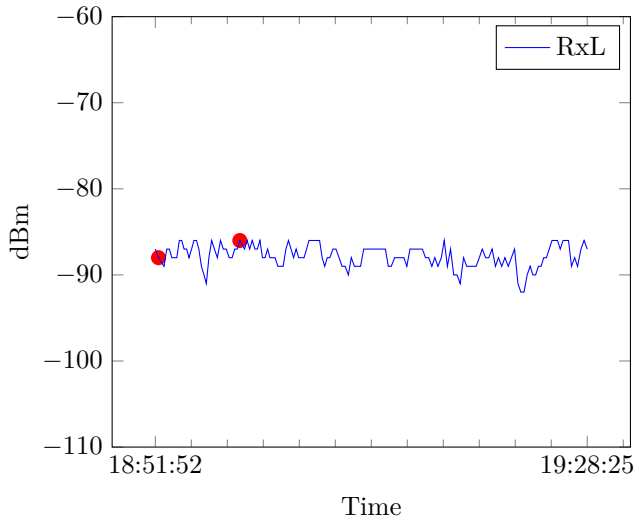


Figure 5.20: RxL from cell 3218 the 09.12.2014 between 18:51:52 and 19:28:25. The red points represents the time LAC changes were observed.

The measured RxL from the 09.12.2014 can be compared to the measured RxL of

the same cell from other surveys performed at the same approximate location. All the RxL measurements of cell 3218 from the other surveys within the area of the blue circle in Figure 5.16 are used to calculate mean, and standard deviation. The result is shown in Table 5.8.

From the table it can be observed that the RxL from the different days the cell was observed does not differ much. It is thus likely that the source of the sender broadcasting a CI of 3218 was the same during all the surveys. This again means that if the source of the signals was in fact an IMSI-catcher the 09.12.2014, the IMSI-catcher was likely operating the other days as well at the same location.

Table 5.8 Average RxL and the standard deviation from all the measurements of cell 3218 in the same approximate location as where the survey the 09.12.2014 was performed.

Date	Number of measurements	Average RxL	Std RxL
04.12.2014	1	-94 dBm	0
09.12.2014	150	-87.79 dBm	1.29
10.12.2014	34	-96.21 dBm	6.38
11.12.2014	81	-94.86 dBm	4.60

time	lac	cellid	rxl	arfcn	celltype	c1	c2
19:28:09	11901	3218	-86	53	S Cell	25	25
19:28:25	11901	3218	-87	53	S Cell	24	24
19:29:44	0	0	-200	0	No GSM	0	0
19:29:59	0	0	-200	0	No GSM	0	0
19:30:13	0	0	-200	0	No GSM	0	0
19:30:28	0	0	-200	0	No GSM	0	0
19:30:42	0	0	-200	0	No GSM	0	0
19:30:57	0	0	-200	0	No GSM	0	0
19:31:12	0	0	-200	0	No GSM	0	0
19:31:27	0	0	-200	0	No GSM	0	0
19:31:45	0	0	-200	0	No GSM	0	0
19:32:50	11901	3107	-77	67	S Cell	34	34

Figure 5.21: ”No GSM” measurements after camping on 3218.

Cell 3218 was not measured again after 19:28:25 the 09.12.2014. The following nine measurements of the Telenor slot were ”No GSM” measurements. This can be observed in Figure 5.21. Neither Aftenposten nor Delma described this observation as suspicious. During the two minutes ”No GSM” readings were measured on the Telenor slot, the Network Guard registered non-corrupt readings on the other slots.

These measurements should be noted, as they may signal suspicious behavior. It could be a jamming device operating for these two minutes, selectively jamming the Telenor ARFCNs. However, two minutes is such a long time that Telenor could be able to notice the noise on the channels. The two minutes of "No GSM" could have other explanations as well, for instance that the BP associated to the slot of the Telenor SIM was experiencing troubles or performing a restart. It should be noted that similar behavior, i.e. several "No GSM" readings in a row on a slot, were observed several times throughout the investigations made with the Network Guard. Neither of these incidents were reported as suspicious by Delma.

Telenor Cell 2174

During a mobile survey the 03.12.2014, cell 2174 on Telenor's network was observed changing LAC. Alarm 3 in Table 5.3 was raised. Delma graded the alarm to "HIGH" severity. The geographical location of where the LAC change occurred is shown in Figure 5.22

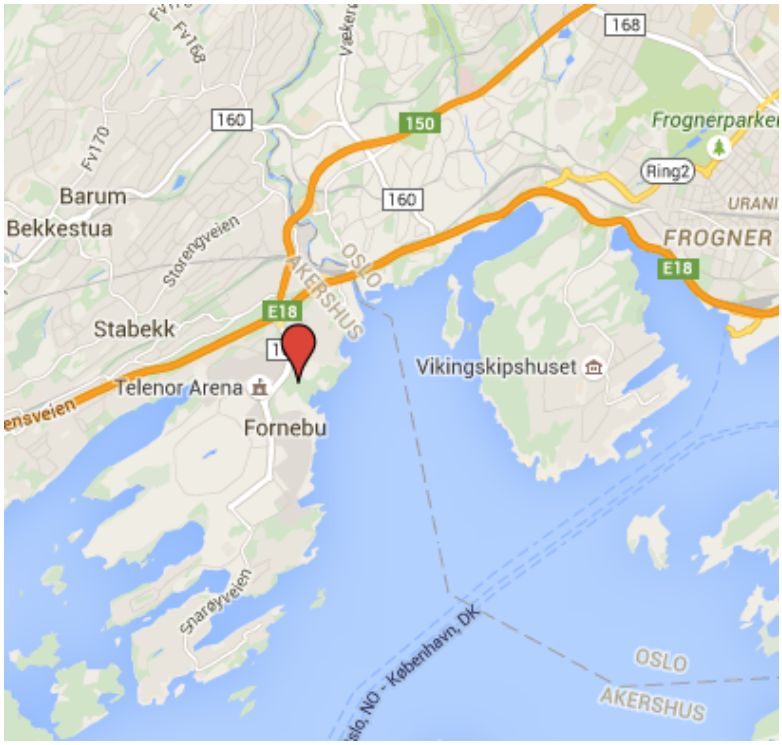


Figure 5.22: Geographical location of LAC change on cell 2174.

The cell was only measured during the survey the 03.12.2014, in total 22 times. Neither of the other surveys were performed in the area of which this cell was

observed. In all the measurements of cell 2174, the C1 and C2 value were equal. This means that CRO and TO both were set to 0 for this cell. The difference between C1 and RxL, C1-RxL, was constant for all measurements.

time	lac	cellid	rxl	arfcn	celltype	c1	c2
14:18:22	11801	2174	-92	56	A Cell	18	18
14:18:41	11801	2174	-77	56	A Cell	33	33
14:19:00	11801	2174	-74	56	S Cell	37	37
14:19:18	11801	2174	-59	56	S Cell	52	52
14:19:42	11801	2174	-52	56	S Cell	59	59
14:20:00	11801	2174	-51	56	S Cell	60	60
14:20:17	2311	2174	-51	56	S Cell	60	60
14:20:45	11801	2174	-51	56	S Cell	60	60

Figure 5.23: The LAC change observed on cell 2174.

Cell 2174 was observed changing LAC at 14:20:17 the 03.12.2014. It changed from 2174, which is a LAC used by several other Telenor cells, to 2311 which is a LAC used by cells in Network Norway's network in the same area. The measurements made of the cell in the time around the LAC change is shown in Figure 5.23.

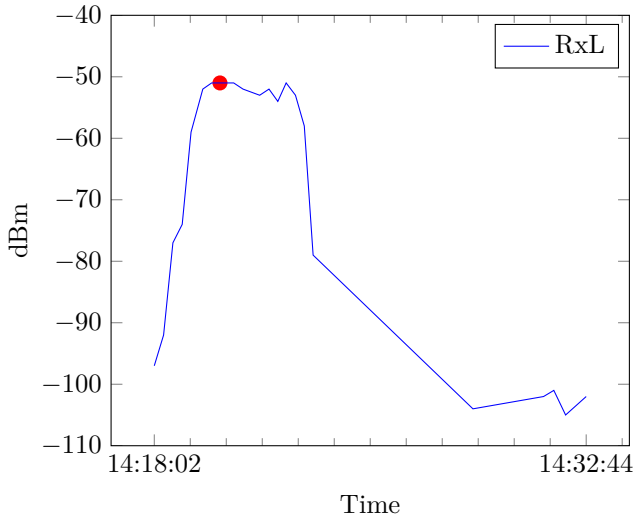


Figure 5.24: RxL from cell 2174 the 03.12.2014 between 14:18:13 and 14:32:44. The red point represents the time LAC change was observed.

Figure 5.25 shows the route traversed with the Network Guard device measurements of cell 2174 were made. During the survey, cell 2174 was only measured once with

a LAC of 2311. The RxL was measured to -51 dBm in this measurement. The RxL from the cell was measured to this value four times and was the strongest measurement of the cell. All the measurements made with this RxL were close to the ”B” in Figure 5.25. Thus, it is likely that this was the closest the Network Guard got to the cell during this survey.

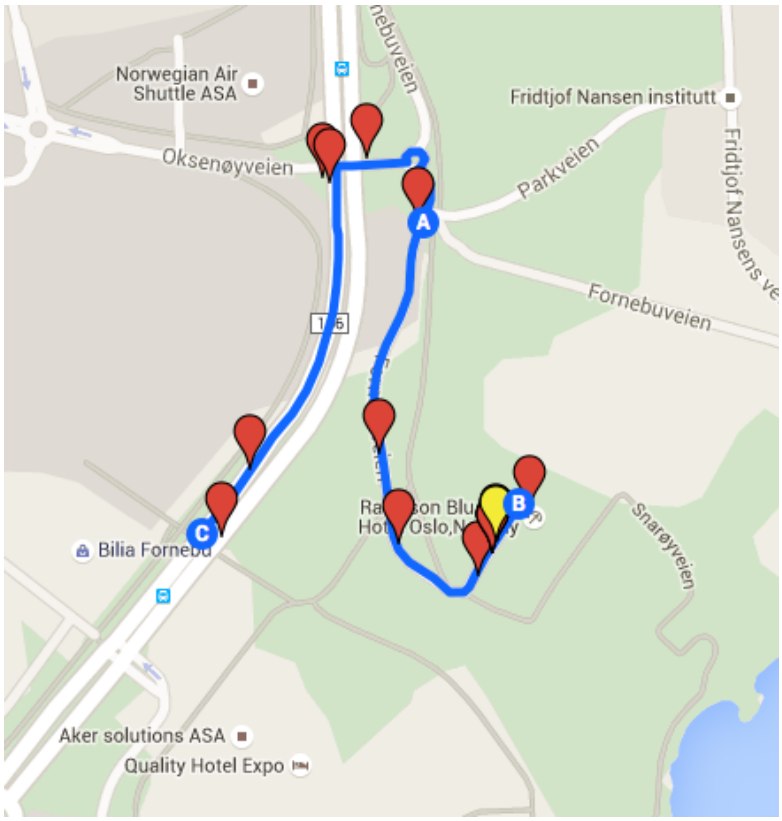


Figure 5.25: All the measurements of cell 2174. The route traversed while observing the cell is highlighted, from ”A” via ”B” to ”C”. The location of the observation of the LAC change is marked with a yellow pin.

The cell was observed during a mobile survey, which means that the Network Guard device was moving. Since the Network Guard was moving, the RxL from the cell would change depending on where the Network Guard device was located compared to the sender of the signals. However based on the RxL shown in Figure 5.24 and the route traversed with the Network Guard shown in Figure 5.25, there are no reason to believe that the received signals originated from multiple senders. There are no fluctuations in the RxL around the time of the LAC switch. Thus, if an IMSI-catcher was spoofing cell 2174 the 03.12.2014, it was likely not turned on at the time of the

LAC switch. All the measurements of cell 2174 the 03.12.2014 likely originated from the same sender.

NetCom Cell 13422

During a mobile survey the 03.12.2014, cell 13422 on NetCom's network was observed changing LAC once. Alarm 3 in Table 5.3 was raised, and Delma graded the alarm to "HIGH" severity.

time	lac	cellid	rxl	arfcn	celltype	c1	c2
13:43:20	3801	13422	-74	43	S Cell	37	37
13:43:37	3801	13422	-71	43	S Cell	40	40
13:44:13	3801	13422	-72	43	S Cell	39	39
13:44:30	3801	13422	-73	43	S Cell	38	38
13:44:50	3801	13422	-73	43	S Cell	38	38
13:45:07	11901	13422	-73	43	S Cell	38	38
13:45:42	3801	13422	-73	43	S Cell	38	38
13:46:01	3801	13422	-71	43	S Cell	40	40

Figure 5.26: The LAC change observed on cell 13422.

The cell was only observed during the survey the 03.12.2014. In total 30 measurements of the cell were made with the Network Guard device. In all the measurements of the cell, C1 and C2 were equal. Thus, CRO and TO were set to 0. ARFCN 43 was used in all measurements of the cell. The difference between C1 and RxL was constant for all the measurements.

The LAC change was observed at 13:45:07. The cell changed LAC from 3801, a LAC used by NetCom cells in the area, to 11901, a LAC used by Telenor cells in the area. The measurements of cell 13422 at the time around the LAC change are shown in Figure 5.27. The cell was observed continuously from 13:34:36 to 13:47:09. An excerpt from the data showing measurements of CI 13422 in the time around the LAC change is shown in Figure 5.26. Figure 5.27 shows the RxL over time when the measurements of the cell were made.

Figure 5.28 shows the route traversed with the Network Guard device around the time of observation of the LAC change. The pins that are not on the highlighted line are measurements made of the cell approximately an hour later in the same survey.

When comparing the RxL graph from Figure 5.27 with the route traversed in Figure 5.28, it seems as if the same sender was the source of all the measurements of cell 13422. No large, unusual fluctuations of RxL values can be observed around the

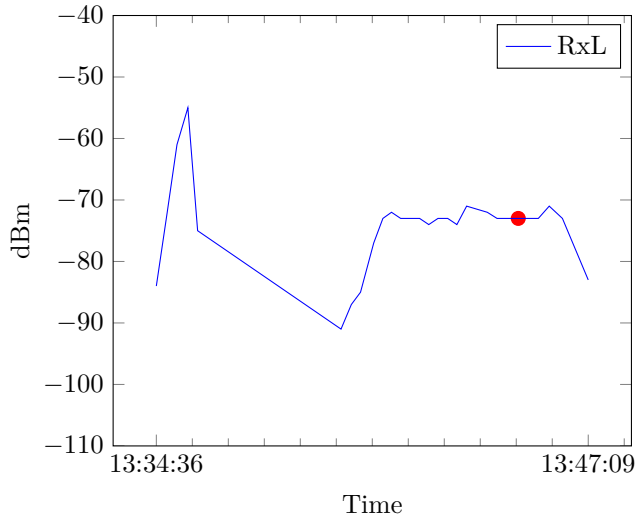


Figure 5.27: RxL from cell 13422 the 03.12.2014 between 13:34:36 and 13:47:09. The red point represents the time LAC change was observed.

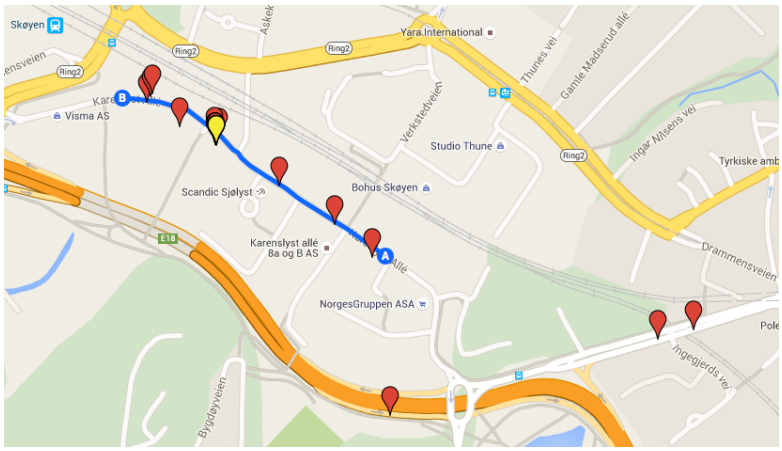


Figure 5.28: All the measurements of cell 13422. The route traversed during the LAC change is highlighted, from "A" to "B". The location of the observation of the LAC change is marked with a yellow pin.

time of the LAC change. Thus, if the source of the LAC change was an IMSI-catcher, it was likely operating during all the measurements made of the CI.

Telenor Cell 3265

Telenor cell 3265 was observed changing LAC once during the investigations in Oslo. The LAC change occurred during a mobile survey the 03.12.2014. Alarm 3 in Table 5.3 was raised. Delma graded the incident to "HIGH" severity.

time	lac	cellid	rxl	arfcn	celltype	c1	c2
13:43:16	11901	3265	-62	64	S Cell	49	49
13:43:33	11901	3265	-60	64	S Cell	51	51
13:43:52	2311	3265	-61	64	S Cell	50	50
13:44:26	11901	3265	-59	64	S Cell	52	52
13:44:45	11901	3265	-59	64	S Cell	52	52

Figure 5.29: The LAC change observed on cell 3265.

The cell was not observed during any other surveys in Oslo. In total 33 measurements of the cell were made the 03.12.2014. In all the measurements of the cell, C2 was equal to C1, thus CRO and TO were not set. The difference between C1 and RxL was constant for all the measurements.

At 13:43:52, cell 3265 was observed changing LAC from 11901 to 2311. LAC 11901 was observed used on all other Telenor cells in the area. LAC 2311 was observed used by Network Norway cells in the area. An excerpt from the data showing the measurements of cell 3265 around the time of the LAC change is shown in Figure 5.29.

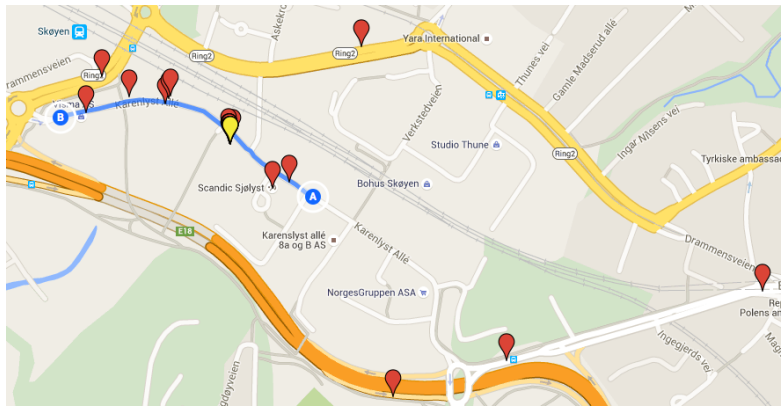


Figure 5.30: All the measurements of cell 3265. The route traversed during the LAC change is highlighted, from "A" to "B". The location of the observation of the LAC change is marked with a yellow pin.

Figure 5.30 shows the route traversed with the Network Guard device during the LAC change. When compared to Figure 5.28, it can be observed that the LAC

change of cell 3265 occurred in the same survey as the LAC change of cell 13422. In addition, the LAC changes of the two different cells occurred at almost the exactly same location and time.

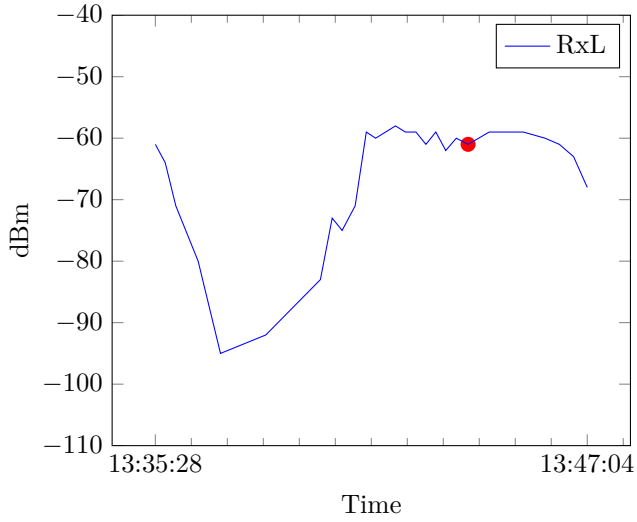


Figure 5.31: RxL from cell 3265 the 03.12.2014 between 13:35:28 and 13:47:04. The red point represents the time LAC change was observed.

Figure 5.31 shows the RxL from the cell during the survey the 03.12.2014. Some RxL fluctuations can be observed, but since the Network Guard was moving during the survey, that is expected. Around the time of the LAC change, the Network Guard was not moving for some minutes. From Figure 5.31 it can be observed that the RxL did not fluctuate during that time, which indicates that all the measurements in the time around the LAC change originated from the same sender.

NetCom Cell 51171

NetCom cell 51171 was observed changing LAC twice during a mobile survey the 03.12.2014. Alarm 3 in Table 5.3 was raised. Delma graded the alarm to ”MEDIUM” severity. The geographical location of the LAC changes observed on cell 51171 is shown in Figure 5.32.

Measurements of cell 51171 was performed during all the surveys in Oslo. In total 736 measurements of the cell were made. In all the measurements of the cell, C2 was equal to C1. Thus, CRO and PT were not set for the cell. The difference between C1 and RxL was constant for all the measurements of the cell.

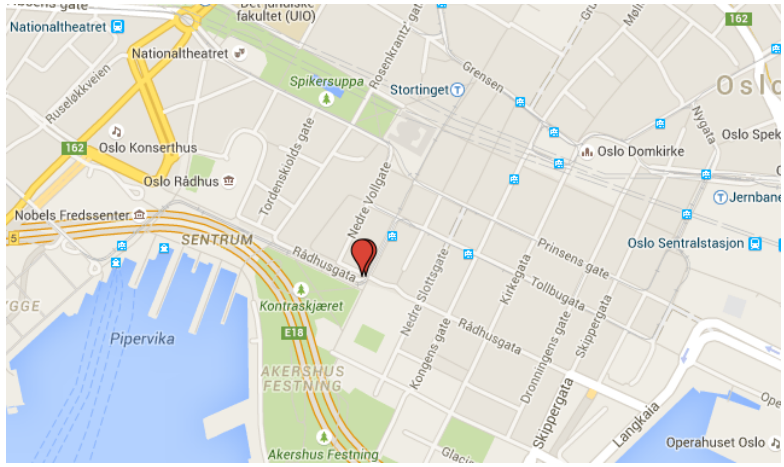


Figure 5.32: The location of the LAC changes observed on cell 51171.

time	lac	cellid	rxl	arfcn	celltype	c1	c2
09:50:30	3804	51171	-81	5	S Cell	30	30
09:50:44	3804	51171	-78	5	A Cell	32	32
09:50:56	0	51171	-80	5	S Cell	31	31
09:51:33	3804	51171	-77	5	S Cell	34	34
09:51:46	3804	51171	-78	5	S Cell	33	33
09:51:59	3804	51171	-78	5	A Cell	32	32
09:52:11	3804	51171	-78	5	A Cell	32	32
09:52:24	3804	51171	-77	5	A Cell	33	33
09:52:37	3804	51171	-78	5	A Cell	32	32
09:52:50	0	51171	-77	5	S Cell	34	34
09:53:12	3804	51171	-78	5	S Cell	33	33
09:53:25	3804	51171	-79	5	S Cell	32	32

Figure 5.33: The LAC change observed on cell 51171.

The cell was observed changing LAC at 09:50:56 and 09:52:50 the 03.12.2014. An excerpt from the data showing the measurements of cell 51171 in the time around the LAC change is shown in Figure 5.33. Both times the cell was observed changing LAC, it was changed from 3801, the LAC used by all the NetCom cells in the area, to LAC 0, a LAC that was not observed used by any PLMNs in Oslo.

Figure 5.34 shows the measured RxL the time around the LAC change. Since the Network Guard was moving during the survey, some RxL fluctuations can be observed. There are no reason to believe that the received signal originated from multiple BTSs

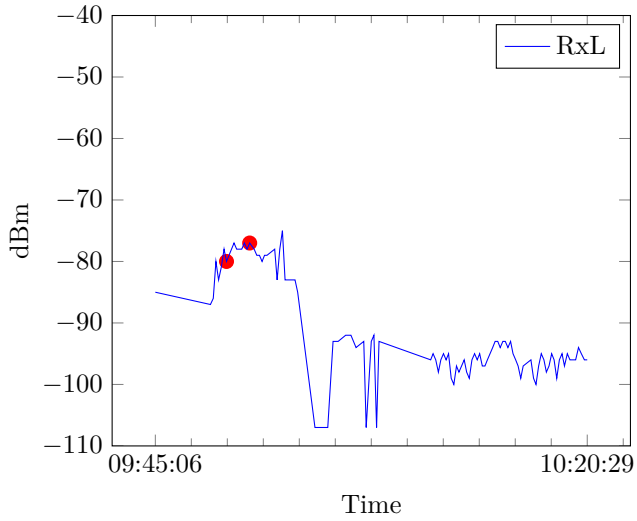


Figure 5.34: RxL from cell 51171 the 03.12.2014 between 09:45:06 and 10:20:30. The red point represents the time LAC changes were observed.

around the time of the LAC change.

Neither Aftenposten nor Delma explained why this incident was graded to "MEDIUM" instead of "HIGH" as all the other LAC changes on a cell were graded to. The behavior of this cell during the LAC change was so similar the five others described in this section, that it should be compared. The most significant difference between this incident and the five others, is that the LAC changed to 0, a value not used by any PLMNs in Oslo. The five other changed LAC to a LAC used by other PLMNs.

From the data it can be observed that the Network Guard device seemed to have some issues during the survey where the LAC changes on cell 51171 were observed. During this survey, the device was not able to register any Telenor or Network Norway cells. Only NetCom cells were measured in the survey. The NetCom SIM was on slot 1, the Network Norway SIM was on slot 2 and the Telenor SIM was in slot 3 in this survey. When on slot 2, the device only registered "No GSM" measurements. No measurements were made while on slot 3.

Discussion Cell LAC Changes

A LAC change is a typical behavior of IMSI-catchers. It will result in a location update for all the MSs that camps on the cell. This in turn will result in the IMSI-catcher being able to request and receive IMSIs of all these MSs.

The behavior of the cells that performed LAC changes were similar to each other.

In all the cases mentioned in this section, the LAC changed only for individual measurements. In addition, for all cells where a LAC change occurred, it seems as if the sender that broadcasted the LAC change also broadcasted all the system information messages observed from the cells before and after. There were not any unusual RxL fluctuations during the measurements of the cells that performed LAC changes, and all the cells showed a consistent behavior of selection and reselection parameters. Thus, there is nothing that indicates that IMSI-catchers were switched on during the measurements of the cells. If the changes were issued by IMSI-catchers, the attackers changed the LAC only for seconds, before changing it back, in order to force location update for all the devices that were camped on the cell during that time.

The reason why an attacker would change the LAC only for seconds could be to make it harder to detect the IMSI-catcher. This might also be the reason why an IMSI-catcher would choose a LAC used by other PLMNs than the one the attacker was spoofing in the area, as was observed in five out of six incidents in this section.

Only three out the six cells that performed LAC changes were observed in more than one survey. Cell 3107 and 3218 in Telenor's network were both observed in multiple surveys. These two cells showed a consistent behavior for all these days, which indicates that the measurements with these CIs originated from the same source all the days. Thus, if cell 3107 and cell 3218 were spoofed by IMSI-catchers the 09.12.2014, they were likely spoofed by IMSI-catchers the other days as well. Cell 51171 also showed consistent behavior in all the surveys there were made measurements of the CI.

Neighbors were not observed for four out of six of the cells mentioned in this section during the LAC changes. Thus, the two other cells, CI 3107 and CI 2174, broadcasted a valid BA list. It does not necessarily mean that the four cells did not broadcast a valid BA list, only that the Network Guard device did not register them at the time. Valid neighbors were observed for the three cells that were observed in multiple surveys when they were observed at other times. Since the behavior of these cells were consistent for all the days they were observed, they likely broadcasted valid BA lists all days. There are several measurements in Oslo where neighbors were not observed. Neither of these was marked as suspicious by Delma.

Neither of the cells described in this section had unusual high C2 values. In all the observed cases of LAC change on cells, the C2 value was equal to the C1. The C1 value was not suspiciously large either.

An interesting observation from the data, is that for all the nine measurements of LAC changes on a cell, the cell changed LAC to the last measured LAC from the previous slot, which is the previous row in the data set. In addition, all the LAC

changes on a cell were observed on cells that the Network Guard device camped on. This can be observed in Figure 5.35. The fact that all the LAC changes resulted in the previously measured LAC is suspicious and can be due to measurement errors or a bug in the software of the Network Guard device. It should also be noted that the same behavior was registered in the incident described in Section 5.6.2. This concern was raised in an email correspondence with Aftenposten[62], which in turn explained it to Delma. Delma refused that the LAC changes could be due to a bug. They stated that they never had experienced that individual parameter had been registered incorrectly.

time	mnc	lac	cellid	rxl	arfcn	celltype	c1	c2
18:41:16	5	2311	61052	-78	975	S Cell	26	26
18:41:16	5	2311	61051	-81	982	A Cell	22	22
18:41:16	5	2311	1022	-95	985	A Cell	2	2
18:41:16	5	2311	61053	-93	987	A Cell	10	10
18:41:16	5	2311	41222	-95	986	A Cell	8	8
18:41:25	1	2311	3107	-92	67	S Cell	19	19
18:41:25	1	11901	23013	-92	682	A Cell	18	-2
18:41:25	1	11901	3106	-93	55	A Cell	17	17
18:41:25	1	11901	23030	-104	677	A Cell	6	-1
18:41:25	1	11901	3525	-99	54	A Cell	11	11

time	mnc	lac	cellid	rxl	arfcn	celltype	c1	c2
18:51:03	5	2311	61052	-77	975	S Cell	27	27
18:51:03	5	2311	61051	-82	982	A Cell	21	21
18:51:03	5	2311	1022	-92	985	A Cell	5	5
18:51:03	5	2311	61053	-90	987	A Cell	13	13
18:51:03	5	2311	1023	-110	988	A Cell	0	0
18:51:11	1	2311	3107	-97	67	S Cell	14	14
18:51:11	1	11901	23013	-99	682	A Cell	11	-9
18:51:11	1	11901	3106	-94	55	A Cell	16	16
18:51:11	1	11901	3830	-102	68	A Cell	8	8
18:51:11	1	11901	3216	-104	123	A Cell	6	6

time	mnc	lac	cellid	rxl	arfcn	celltype	c1	c2
18:51:58	5	2311	61052	-78	975	S Cell	26	26
18:51:58	5	2311	61051	-82	982	A Cell	21	21
18:51:58	5	2311	1022	-93	985	A Cell	4	4
18:51:58	5	2311	61053	-90	987	A Cell	13	13
18:51:58	5	2311	1023	-93	988	A Cell	4	4
18:51:58	5	2311	41222	-94	986	A Cell	9	9
18:51:58	5	2311	40042	-97	979	A Cell	7	7
18:52:08	1	2311	3218	-88	53	S Cell	23	23
18:52:26	2	3804	3629	-93	707	S Cell	3	33

time	mnc	lac	cellid	rxl	arfcn	celltype	c1	c2
18:58:53	5	2311	61052	-77	975	S Cell	27	27
18:58:53	5	2311	61051	-82	982	A Cell	21	21
18:58:53	5	2311	1022	-92	985	A Cell	5	5
18:58:53	5	2311	61053	-94	987	A Cell	9	9
18:58:53	5	2311	41222	-96	986	A Cell	7	7
18:58:53	5	2311	1023	-98	988	A Cell	-1	-1
18:59:01	1	2311	3218	-86	53	S Cell	25	25
18:59:14	2	3804	3629	-89	707	S Cell	7	37

time	mnc	lac	cellid	rxl	arfcn	celltype	c1	c2
14:20:08	5	2320	20431	-71	982	S Cell	34	34
14:20:08	5	2320	20433	-100	985	A Cell	4	4
14:20:08	5	2311	6032	-103	987	A Cell	-6	-6
14:20:17	1	2311	2174	-51	56	S Cell	60	60
14:20:17	1	11801	2537	-76	122	A Cell	34	34
14:20:17	1	11801	2610	-72	65	A Cell	38	38
14:20:17	1	11801	22035	-99	671	A Cell	11	-9

time	mnc	lac	cellid	rxl	arfcn	celltype	c1	c2
13:45:02	1	11901	3265	-59	64	S Cell	52	52
13:45:02	1	11901	3168	-86	60	A Cell	24	24
13:45:02	1	11901	3044	-82	52	A Cell	28	28
13:45:02	1	11901	3227	-87	67	A Cell	23	23
13:45:02	1	11901	23115	-79	684	A Cell	31	11
13:45:02	1	11901	3169	-88	56	A Cell	22	22
13:45:07	2	11901	13422	-73	43	S Cell	38	38

time	mnc	lac	cellid	rxl	arfcn	celltype	c1	c2
09:50:44	2	3804	51171	-78	5	A Cell	32	32
09:50:47	5	0	0	-200	0	No GSM	0	0
09:50:56	2	0	51171	-80	5	S Cell	31	31

time	mnc	lac	cellid	rxl	arfcn	celltype	c1	c2
09:52:37	2	3804	13752	-90	38	A Cell	20	20
09:52:41	5	0	0	-200	0	No GSM	0	0
09:52:50	2	0	51171	-77	5	S Cell	34	34

time	mnc	lac	cellid	rxl	arfcn	celltype	c1	c2
13:43:43	5	2311	1433	-57	987	S Cell	47	47
13:43:43	5	2311	1431	-80	975	A Cell	17	17
13:43:43	5	2311	1432	-81	984	A Cell	22	22
13:43:43	5	2311	41893	-85	981	A Cell	18	18
13:43:52	1	2311	3265	-61	64	S Cell	50	50

Figure 5.35: Excerpt from data of all measurements in the time around all the LAC changes. LAC changed to last measured LAC of previous slot.

Aftenposten and Delma argued that commercial IMSI-catchers often use LACs that are in use nearby. In five out of six incidents in this section, this was the case. The cells changed LAC to a LAC used by other PLMNs in the area. If these cells were IMSI-catchers, the attackers configuring the devices had a choice between the LACs

used by the PLMNs that the attacker was not spoofing in the area. In four out of the five cases where the cell changed LAC to another PLMN's LAC, the attacker had two LACs to choose from, as the other PLMNs were only observed with one LAC each in the area. For the fifth cell, 2174, the attacker had three LACs to choose from, as two LACs were used by the Network Norway cells nearby. Since an attacker would not know the slot order of the Network Guard device, the fact that the attackers always chose the previously measured LAC must have happened by chance. The probability, p, for this to happen can thus be calculated:

$$p = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{3} = 0.0208 \tag{5.1}$$

The probability that attackers by chance would choose the previous measured LAC for the five cells where the LAC change to a LAC used by other PLMNs in the area is thus approximately 2%.

The incident where the LAC changed to 0 after a "No GSM" measurement was made, is not included in the calculation in Equation 5.1. Setting the LAC to 0 is most likely a conscious decision made by an attacker, and in general a bad value to use if the attacker wants to operate unnoticed, as it stands out from all other values.

The incident described in Section 5.6.2 makes this observation even more interesting. The LAC in that incident was also identical as the row before, even though the measurement was a "No GSM" measurement. If this was an attacker, she decided to use a LAC of one of the other PLMNs nearby. The attacker could choose between two LACs in the area, one for Network Norway and one for Telenor. The attacker chose the Telenor LAC. The probability was thus 50%. If we include this in the calculation above, the total probability, p_2, that all these LACs were chosen by chance by attackers is:

$$p_2 = \frac{1}{2} \cdot 0.0208 = 0.0104 \tag{5.2}$$

In the email correspondence, Aftenposten was recommended to ask Delma if they could review the source code and compare the observation with previous surveys Delma had done at different locations. If the measurements were due to a bug, it would most likely be possible to observe the same type of observations in other surveys. Nothing suggested that Delma had looked into the potential issue in the answer they provided by email to Aftenposten.

There were also two other incidents in the data set where the LAC changed on a channel. However, in these two incidents, the CI changed as well and the RxL from

these cells suggested that the received signal was from another BTS after the LAC and CI change. Thus, the observed behavior of these two cells differed greatly from the observed behavior of the six other cells where only a LAC change occurred on the channel.

If the incidents regarding LAC changes were not due to measurement errors or a bug in the Network Guard software, it is likely that Aftenposten observed IMSI-catchers in these cases. There is no reason for individual, legitimate cells to change their LAC as the LACs typically is a static value defined by the BSC. A PLMN would most likely not change the LAC for single cells to a LAC used by other PLMNs in the area.

Since the observed behavior of these cells were so similar, it is likely that, if the incidents were caused by IMSI-catchers, the same equipment were used in all the incidents mentioned in this section. According to Delma, some commercial IMSI-catchers can be configured to operate on a random, legitimate LAC in the area, as observed in five out of six cases mentioned in this section.

5.6.4 Network Norway Cell 1091

During the mobile survey the 11.12.2014, alarm 9, "Provider anomaly", in Table 5.3 was raised on cell 1091 in Network Norway's network. Two Telenor ARFCNs were broadcasted in the BA list of the cell. The alarm was graded to "HIGH" severity by Delma. Five measurements of this anomaly were made. The locations of the measurements is shown in Figure 5.36.

Figure 5.37 shows measurements from the data where two Telenor cells were observed as adjacent cells of Network Norway cell 1091. Measurements of the two Telenor cells are highlighted. From the figure, it can be observed that the Network Guard device was on slot 3 at the moment of the measurement, which was the slot of the Network Norway SIM during the survey. The two Telenor cells with CI 58135 and 59403 appeared in the measurements made in the slot. This is likely because cell 1091 broadcasted ARFCN 68 and ARFCN 66 in the BA list. Aftenposten claimed that this is a common method used by attackers to lure MSs to release information.

There were made 26 measurements of cell 1091 the 11.12.2014. The Network Guard camped on the cell only for five measurements. The cell was also observed once the 04.12.2014, but not as serving cell. Since the Network Guard did not camp on the cell the 04.12.2014, it is unknown whether the cell broadcasted the same BA list the 04.12.2014 or not. For all the measurements of the cell, the C1 and C2 values were equal and the difference between C1 and RxL was constant for all the measurements. Thus, nothing suggests that different BTSs were the sources of the signals the 04.12.2014 and the 11.12.2014.

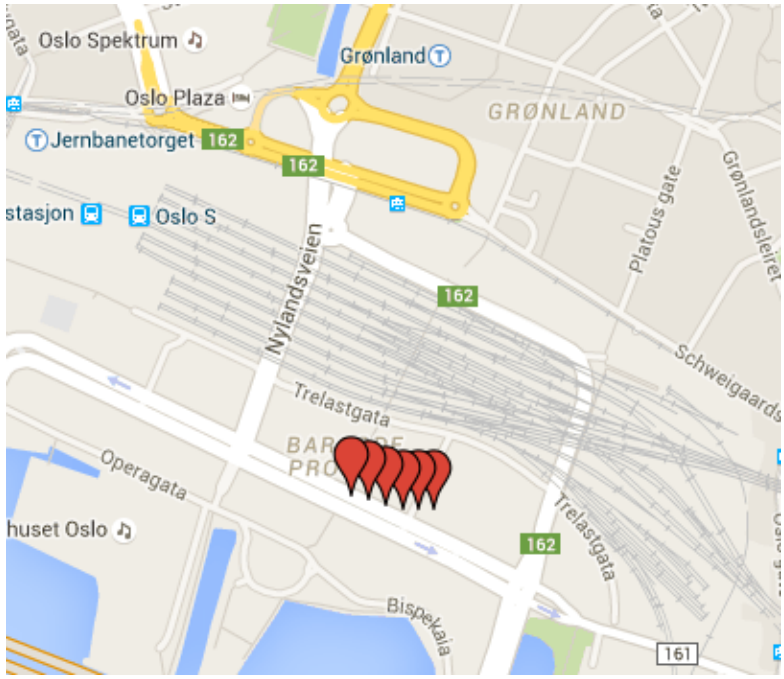


Figure 5.36: Geographical location of measurements of provider anomaly.

time	lac	cellid	mnc	rxl	arfcn	celltype	c1	c2	slot
10:52:30	2311	1091	5	-78	986	S Cell	27	27	3
10:52:30	2311	41922	5	-80	987	A Cell	23	23	3
10:52:30	11901	59403	1	-72	68	A Cell	38	38	3
10:52:30	11901	58135	1	-81	66	A Cell	29	29	3
10:52:30	2311	1032	5	-83	984	A Cell	14	14	3

Figure 5.37: Two Telenor cells in the BA list of Network Norway cell 1091.

Setting up a rogue BTS spoofing one PLMN and broadcasting neighbor ARFCNs associated to another PLMN could be used by an attacker in order to lure MSs from one PLMN to another. An example of a situation where this could be used, is close to land borders, where a PLMN of one country could set up a rogue BTS on the other side of the border, spoofing the other nation's network. By broadcasting its own ARFCNs in the BA list of the rogue BTS, the attacker would move MSs from the network of one country to the attacker's network in the other country. This would result in roaming costs for the subscribers and revenues for the attacker's network.

It is questionable why such an attack would be performed in Oslo. The only result of the attack would be to move subscribers from Network Norway's network to Telenor's network. Network Norway had a roaming agreement with Telenor, to give

their subscribers good coverage all over Norway[63]. Thus, it might be a legitimate configuration made by Network Norway for the cell to provide good coverage for their subscribers in the area. Thus, the motivation for an attacker to perform such an attack is unclear. Only two out of four observed neighbors were Telenor ARFCNs. If an attacker wanted to move Network Norway subscribers to Telenor's network, it would make more sense if all the ARFCNs published in the BA list were Telenor ARFCNs, which was not the case for this cell.

5.6.5 Telenor Cell 32478

Measurements made of Telenor cell 32478 during a mobile survey the 22.12.2014 was by Delma and Aftenposten considered the clearest proof that active attacks were performed in Oslo during the time of the investigations. Both "C anomaly" alarm and "service denial" alarm were raised, and Delma graded the incident to "HIGH" severity. The geographical location of the measurements of the cell is shown in Figure 5.38.

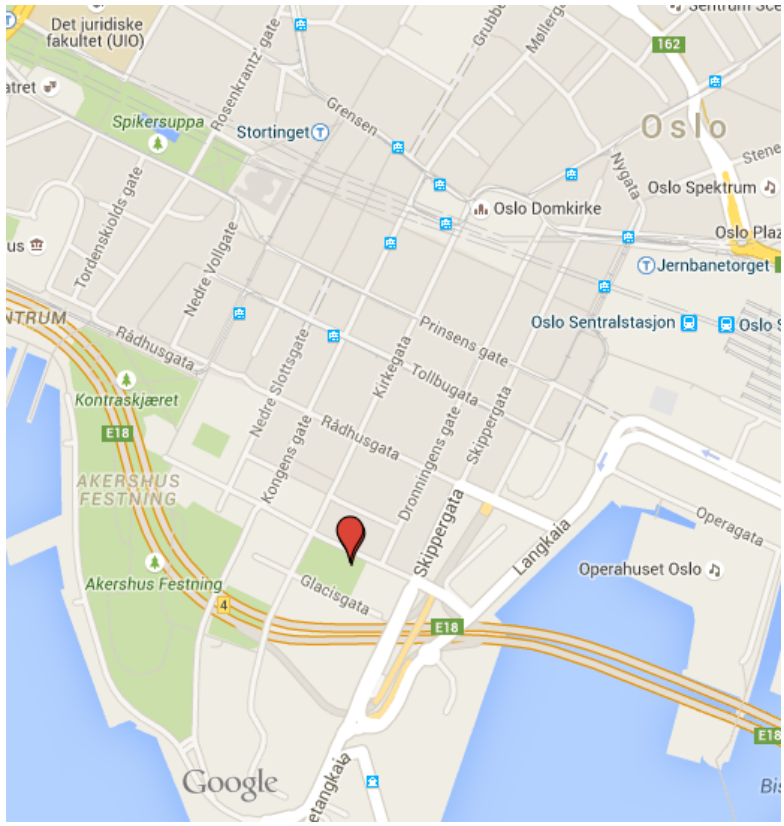


Figure 5.38: Geographical location of measurements of cell 32478.

Delma argued that this finding was so clear that they assumed that they observed operations made by Norwegian or foreign governments. They recommended that Aftenposten should let the Norwegian government look at the material before mentioning it in public. The data and analysis of the findings were sent to PST. PST did not mention this incident in their status update in April 2015.

There were in total two measurements of cell 32478 during the survey the 22.12.2014. The cell was not observed in any other surveys. The two measurements of the cell are shown in Figure 5.39.

time	mnc	lac	cellid	rxl	arfcn	celltype	c1	c2
14:15:44	1	11901	23488	-91	672	S Cell	15	15
14:15:44	1	11901	3783	-103	61	A Cell	7	7
14:15:44	1	12901	32478	-94	679	A Cell	8	43
14:16:03	1	12901	32478	-83	679	S Cell	32	83
14:16:21	1	0	0	-200	0	No GSM	0	0
14:31:56	1	11901	23013	-102	682	S Cell	9	-11

Figure 5.39: Measurements of cell 32478.

At 14:15:44, the Network Guard device registered cell 32478 in the BA list of cell 23488 in Telenor's network. The cell broadcasted on ARFCN 679, a valid Telenor ARFCN. The Network Guard camped on cell 32478 at the next measurements made on the Telenor slot at 14:16:03, which can be observed from Figure 5.39 by the fact that the "celltype" of the second measurement is "S Cell", serving cell.

Cell 32478 broadcasted a LAC of 12901. This LAC was not observed any other time during the investigations in Oslo. The Network Guard device was camped on the cell only for one measurement. The next measurement was a "No GSM" measurement, which indicates that the device was not able to read messages from the cell. There may be many reasons for that, amongst them that the cell stopped broadcasting, or the cell was barred. It could also be due to some measurement errors, as these type of measurements were measured all over Oslo throughout all the surveys, without being flagged as suspicious by Delma. Another reason for this measurement could be that the location update procedure initiated by the Network Guard device was rejected. An IMSI-catcher that only catches IMSIs could use this method. It could also be used by an IMSI-catcher that selectively targeted one or more IMSIs and the Network Guard IMSI was not amongst them.

After the "No GSM" measurement, the Network Guard was moved, and Telenor cells were not observed for approximately 15 minutes. From the figure, it can be observed that no neighbor cells were observed while the Network Guard camped on cell 32478. This could indicate that the BA list broadcasted by the BTS was empty.

From Figure 5.39 it can be observed that the C2 values of the cell have unusual values compared to what was observed for other cells in Telenor's network, shown in Section 5.5.1. The measurements of this cell were the only measurements where the C2 value of a cell was greater than the C1 value on Telenor's network. Thus, cell 32478 was the only cell in Telenor's network that used a CRO different than 0. At the first measurement of the cell, the difference between C2 and C1 was 35 dBm, $C_A = C2 - C1 = 35$ dBm. At the next measurement, the difference between the C2 and the C1 value was even greater, $C_B = C2 - C1 = 51$ dBm. There are two possible reasons for a change in the difference between the C values in two consecutive measurements, such as observed in this case where $C_A - C_B = 16$ dBm. Either a TO was used with a PT or the CRO was changed between the two measurements.

As described in Chapter 2 the TO can only be set to a value divisible by ten in the range [0,6], or infinity. Thus, TO cannot be 16 dBm that was the observed difference in this case. If the TO had been infinity, the C2 values would have been -1. It can thus be concluded that the cell did not use a TO, TO=0.

The CRO must have been changed during the time between the two measurements. However, the difference between the C values, C2 and C1, was an odd number for both of the measurements. In Chapter 2, it was explained that the CRO represents an even number between 0 and 126 dBm. Regardless of what valid CRO value the MS receives from the BTS, the CRO will be interpreted as an even number by the MS. It is thus not possible to set the CRO to values that lead to a difference of C values of respectively 35 dBm and 51 dBm, as was measured for this cell. An odd difference of C values when TO$\neq$ 7 should not be possible in GSM, since both CRO and TO are even.

Since the C values are calculated at the ME, the reason why there are observed odd differences of C values, may have been caused by how the BP of the Network Guard calculated the values. There might be some implementation decisions or implementation errors in the Network Guard software and firmware that enables an odd difference to occur, or it was a measurement error. Since the source code is not public, the implementation of the reselection procedure on the Network Guard BP cannot be checked.

It is also worth noting that the difference between the C1 value and the RxL changed between the two measurements. In the first measurement, C1-RxL = 102 dBm. In the second measurement, C1-RxL = 115 dBm. Thus, the BTS broadcasting the signals must have changed the selection parameters in the time between the two measurements. Either the RXLEV_ACCESS_MIN or the MS_TXPWR_MAX _CCH was changed. This observation is the only observation in the dataset of a change of selection parameters between two consecutive measurements of a cell.

The measurements made of cell 32478 stands out from all the other measurements made of the networks in Oslo. The incident described in this section is the only incident in the data set where the CRO and either of the selection parameters was observed changing for a cell, and also the only measurement of a cell in Telenor's network with a C2 value greater than the C1 value.

The very high C2 values, the unusual fluctuations of the C values, the service denial and the fact that the cell used a LAC not used by any other observed cells in Oslo is very suspicious. The cell displayed some characteristic IMSI-catcher behaviors. Since it was observed while the Network Guard camped on another cell, it broadcasted on an ARFCN broadcasted in the BA list of the cells nearby. It used a LAC that was not used by the cells nearby, which would force a location update procedure to be initiated by all the MSs reselecting to the cell. Thus the BTS could request IMSIs. The cell was also boosting the C2 value significantly, possibly by manipulating the broadcasted CRO, which would force most MSs nearby to reselect to the cell. Aftenposten searched in the same area during the check surveys in April 2015. The CI was not observed in this survey[61].

The measurements made of cell 32478 clearly indicates anomalies compared to measurements of all the other cells in Oslo. It is possible that Aftenposten observed a cell that was not part of Telenor's legitimate network. The fact that an odd difference between C2 and C1 was observed is very strange, but could be caused by how the reselection procedure is implemented on the BP of the Network Guard. It could, however, also be due to some measurement errors. It is assumed that the odd difference between C1 and C2 are not due to data manipulation by Aftenposten or Delma.

5.6.6 Channel Cell Changes

In the data acquired by Aftenposten, there were observed multiple incidents in which only the CI changed on an observed ARFCN. Aftenposten claimed that such a change of CI is a normal method used for manipulation by several different IMSI-catchers.

Aftenposten graded two of these incidents to "HIGH" severity in their report[5]. By Delma, all the incidents where the CI changed on an ARFCN were graded to "MEDIUM" severity. There are two scenarios in which a channel cell change can be observed; one BTS changes the value of the CI in the system information messages, or two different BTSs operate on the same ARFCN in the same approximate area with the same LAC.

The incidents that were graded to "HIGH" severity by Aftenposten are discussed in this section. The observations of the different incidents are first described and discussed. At the end of this section, the incidents are discussed together.

Telenor ARFCN 55 Aker Brygge

During a mobile survey the 04.12.2014, the CI broadcasted on ARFCN 55 was observed changed. ARFCN 55 is allocated Telenor. Neither of the other parameters observed by the Network Guard device changed. The CI was observed changed from 3106 to 3329 and back.

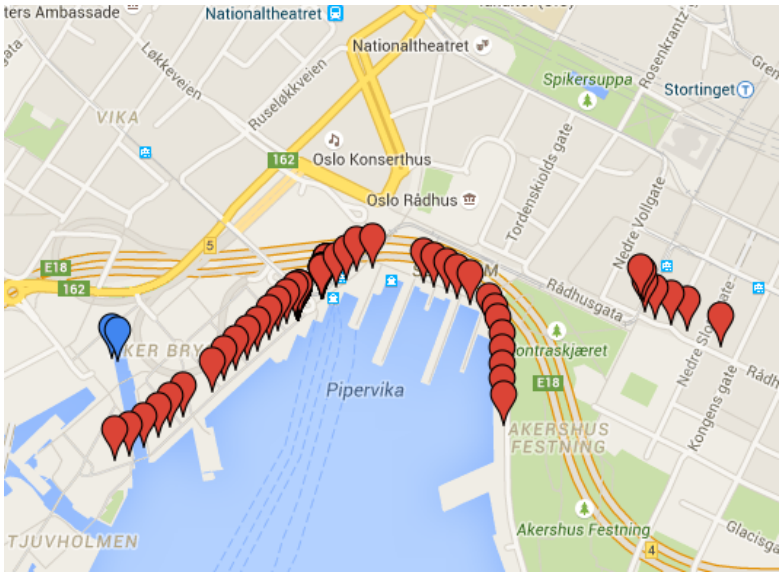


Figure 5.40: CI change on ARFCN 55 at Aker Brygge. Measurements of CI = 3106 are marked with red pins. Measurements of CI = 3329 are marked with blue pins.

Figure 5.40 shows the location of the measurements of ARFCN 55 during the survey the 04.12.2014. Figure 5.41 is an excerpt from the data showing all the measurements of ARFCN 55 at the time around the CI change. It can be observed that CI 3329 was observed in two measurements in a row.

time	lac	cellid	rxl	arfcn	celltype	c1	c2
11:57:52	11901	3106	-80	55	A Cell	30	30
11:58:08	11901	3106	-77	55	A Cell	33	33
12:00:50	11901	3329	-79	55	A Cell	31	31
12:01:05	11901	3329	-77	55	A Cell	33	33
12:09:39	11901	3106	-70	55	A Cell	40	40

Figure 5.41: ARFCN 55 at Aker Brygge changes CI

The Network Guard device had moved approximately 160 meters from the last

measurement of CI 3106 to the first measurement of CI 3329. The RxL changed by 2 dBm during this movement, as can be observed in Figure 5.41. The time between these two measurements was almost nine minutes. During this time, there were made several measurements on the slot of the Telenor SIM, but ARFCN 55 was not observed. The distance between the second measurement of CI 3329 and the next measurement of CI 3106 could not be calculated, as the measurement made at 12:09:39 did not include GPS location, possibly because the Network Guard device lost GPS signal. There are several measurements in the surveys in Oslo where this occurred.

The next measurement GPS data was included was measured at 12:10:35. The distance from the cell change to this measurement was approximately 350 meters. The RxL from ARFCN 55 changed by 7 dBm during the movement between the last measurement of cell 3329 and the next measurement of cell 3106. The time between these two measurements was approximately eight minutes and 30 seconds.

CI 3329 was not observed any other days. It was only observed for the two measurements the 04.12.2014. CI 3106 was observed during all the surveys. In all the measurements of the CI 3106, the LAC was 11901. The C2 value was equal to the C1 value for all the measurements of CI 3106, thus the CRO and TO were set to 0 for all the measurements of the cell, all the days it was observed.

Since ARFCN 55 was observed for only two measurements and the Network Guard moved 160 meters between the last measurement of CI 3106 and the first measurement of CI 3329, it is possible that the Network Guard device observed two different cells. Since CI 3329 was only observed for these two measurements, it might be a small cell in the Telenor network. CI 3106 seems to be a large cell from the measurements shown in Figure 5.40. If the measurements originated from two different cells, there might have been some interference as both were observed in close proximity with similar RxL.

Network Norway ARFCN 987 Barcode

During a mobile survey the 11.12.2014, two CIs were observed on the same ARFCN around Barcode in Oslo. Figure 5.42 shows the measurements of ARFCN 987 in the area close to the cell changes as well as the movement during the survey.

Excerpts from the data showing the measurements of ARFCN 987 around the time of the first CI change from 1153 to 41922 is shown in Figure 5.43. The LAC did not change.

The Network Guard device moved approximately 2 meters from the measurement of CI 1153 at 10:43:56 to the measurement of CI 41922 at 10:44:32. The RxL from

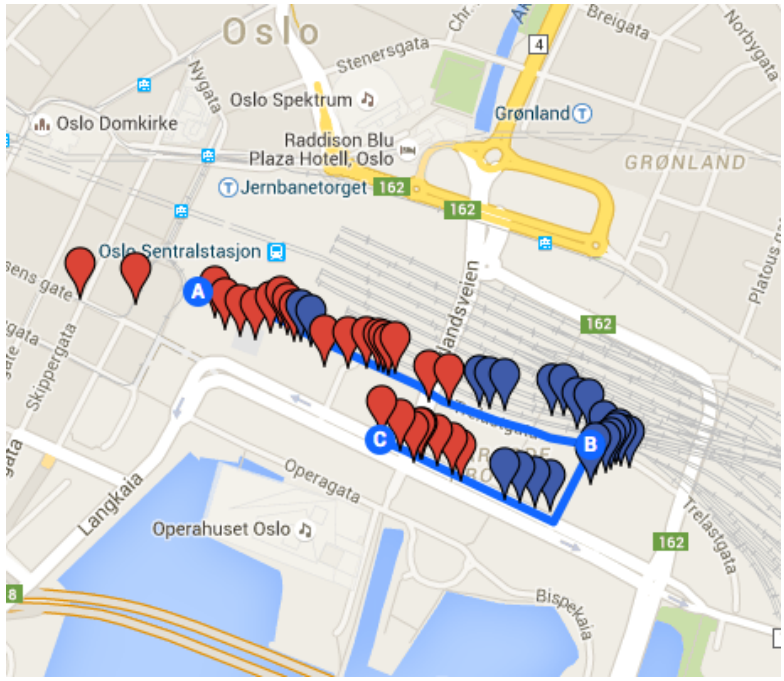


Figure 5.42: ARFCN 987 at Barcode changes CI. The blue pins represent CI 41922, and the red pins represent CI 1153. The Network Guard moved from "A" via "B" to "C".

ARFCN 987 changed only with 1 dBm during this movement, which could suggest that both the measurements originated from the same BTS. The same can be observed when the CI changed from 41922 to 1153. The RxL did not fluctuate. However from Figure 5.43 it can be observed that the behavior of the two CIs differs, and suggests that there might be two different BTSs that are the source of the signals.

In the measurements of CI 1153 the difference between C1 and RxL was consistently 93 dBm the 04.12.2014. The difference between C1 and RxL when CI 41922 was observed was consistently 103 dBm. The difference is significant, and since it was consistent for the two different CIs, it is likely that there were two different BTSs configured differently that were the sources of the signals received. The only alternative explanation is that one BTS would change both the CI and the RXLEV_ACCESS_MIN or the MS_TXPWR_MAX_CCH simultaneously.

The difference between C1 and RxL was much larger for CI 41922 than CI 1153, but it was not unusually large. Network Norway used many different values for RXLEV_ACCESS_MIN or MS_TXPWR_MAX_CCH in their network. A difference between C1 and RxL of 93 dBm was used by five cells in Network Norway's

time	lac	cellid	rxl	arfcn	celltype	c1	c2
10:43:43	2311	1153	-84	987	A Cell	9	9
10:43:56	2311	1153	-84	987	A Cell	9	9
10:44:14	2311	41922	-85	987	A Cell	18	18
10:44:32	2311	41922	-78	987	A Cell	25	25
10:44:49	2311	1153	-76	987	A Cell	17	17

(a) ARFCN 987 at Barcode changes CI from 1153 to 41922 and back.

time	lac	cellid	rxl	arfcn	celltype	c1	c2
10:53:51	2311	41922	-76	987	A Cell	27	27
10:54:10	2311	41922	-76	987	A Cell	27	27
10:54:58	2311	1153	-73	987	A Cell	20	20
10:55:18	2311	1153	-69	987	A Cell	24	24

(b) ARFCN 987 at Barcode changes CI changes CI from 41922 to 1153.

Figure 5.43: ARFCN 987 at Barcode changes CI.

network. A difference between C1 and RxL of 103 dBm was used by 113 different cells in Network Norway's network. Both the CIs used the same LAC as all the other Network Norway cells in the area. Large C2 values were not observed either, as the C2 value was consistently equal to the C1 value for both the CIs.

There is a possibility that there were two legitimate Network Norway cells in the area, but since the RxL from the two possible BTSs were so similar at the location of the measurements, this would likely cause severe interference. It might be a misconfiguration in the Network Norway network, where two cells in close proximity were configured to operate on the same ARFCN. As shown in Chapter 2, Network Norway was allocated only a third of the frequency band that NetCom and Telenor were allocated. This means that Network Norway cells would have to reuse ARFCNs more often than NetCom and Telenor, which in turn would cause situations like the one explained in this section to occur more often than for Telenor and NetCom, especially in urban areas where there are many cells.

Discussion Channel Cell Changes

The findings of channel cell changes indicate anomalies in the networks in Oslo. Multiple different cells should not operate on the same frequency in close proximity in a cellular network. BTSs would not normally change the CI broadcasted in the system information messages either. CI is a very static value[37].

In both the cases described in this section, the incidents occurred while moving. It is possible that different cells operating on the same ARFCN were observed in both the described cases. IMSI-catchers will often use an ARFCN that is unused in the

area to avoid interference and detection[37]. However, it should not be dismissed that some IMSI-catchers might use the same ARFCN as legitimate cells in the area.

The RxL did not fluctuate much during any of the cell changes on a channel. Thus, it is also possible that the alarms were raised because individual cells changed their CI, broadcasted on the BCCH. A legitimate cell would likely not do this. It is not a typical behavior for IMSI-catchers either, as it does not result in uplink communication[3], and will thus not benefit an attacker. However, it is possible that some IMSI-catchers change the CI to an invalid value, for instance larger than 16-bit. Using an invalid CI value could, based on the BP on the ME, result in exploits of memory corruptions. Such an attack would be similar to the attacks described by Weinmann[30]. There is, however, nothing that indicates such attacks in the data acquired by Aftenposten. The CIs that were changed in the incidents described in this section were changed to valid CIs. In addition, neither of the other parameters received, such as LAC, MNC or MCC seem to be corrupt. MCC, MNC and LAC are the following values in the system information messages after the CI value. Since these were not corrupt, and the CI values were valid, nothing indicates that such BP attacks have been performed in the incidents described in this section.

The LAC did not change during the CI changes in this section. If the observed cells were IMSI-catchers, the attackers have listened to cells in the area to set the LAC to the same value as the LAC of the other cells in the area. The attackers would then have to wait for T3212 to expire or for the camped MSs to request a service to catch their IMSIs. Some IMSI-catchers might do this, but if the attacker copies the LAC and the ARFCN of a nearby cell, it would make more sense if the attacker copied the CI as well. The reason why an attacker would copy the LAC of the cells of the PLMN the attacker is spoofing nearby, would likely be done to make it harder to detect the IMSI-catcher. Using a different CI, while using the same LAC and ARFCN as a nearby cell, would by no means benefit the attacker, as it would only distinguish the cell from the legitimate cell operating on the same ARFCN, such that it would be easier to catch the IMSI-catcher. Other typical IMSI-catcher behavior were not observed in the incidents described in this section either.

Since no typical IMSI-catcher behavior was observed, it is likely that all the cells described in this section were legitimate cells. If this is the case, this indicates that the GSM networks in Oslo are somewhat misconfigured. Even though some of the cells might be small, multiple cells should not operate on the same frequency in that close proximity in a cellular network.

[3]It was validated in an experiment in Appendix D that a CI change does not cause uplink communication.

5.6.7 Cells Described as Probable IMSI-Catchers by Aftenposten in January 2015

In the technical description released by Aftenposten in January 2015, the newspaper claimed that they had revealed nine BTSs that "most likely" were IMSI-catchers in Oslo[53]. The CIs of six of these were mentioned in the report. These CIs are shown in Table 5.9.

Table 5.9 Cells described as probable IMSI-catchers by Aftenposten in January 2015.

CI	MNC
3629	02
3257	02
3013	02
24079	02
13869	02
61102	05

In the report by Delma released in April 2015, neither of these cells raised alarms classified to "HIGH" severity. Only CI 3629 has been analyzed in details in this thesis. The others were not significantly highlighted by Delma or Aftenposten in the latest reports.

Cell 61102 was not mentioned at all by neither Delma nor Aftenposten in the latest reports. There is no explanation for why this cell was considered an IMSI-catcher. The cell was observed in four different surveys, and the observed behavior of the cell during these surveys were consistent, did not stand out from measurements of the other Network Norway cells observed and did not display any typical IMSI-catcher behavior or other unusual behavior.

The main argument Aftenposten used when they claimed that these cells were IMSI-catchers was that they had unusual cell reselection values. The "C Anomaly" alarm was raised for all of these cells except cell 61102. As explained in Section 5.5.1, Aftenposten and Delma did not relate the alarm threshold to the actual parameters observed broadcasted by the cells in Oslo. Delma set the alarm threshold for NetCom's network to 30 dBm and the alarm threshold for Telenor's network to 20 dBm. The alarm would be raised each time the difference between the observed C1 and C2 value of a cell exceeded these values.

From Table 5.9 one can observe that five out of six cells Aftenposten pointed out as probable IMSI-catchers in January 2015 broadcasted an MNC of 2. The behavior

of all these cells suggested that they broadcasted a TO of 7 (infinity), which means that the C2 value was -1 during PT.

Since the C2 value always was -1, the ”C anomaly” alarm would be raised every time the C1 value was greater than 29 dBm during PT. For all the incidents related to the cells in Table 5.9 with MNC=2, the Network Guard device happened to move close enough to the BTSs of the cells that the RxL was high enough for the C1 value to exceed 29 dBm during PT.

When compared to the observed configuration of the NetCom network, the behavior of these cells was not suspicious. Aftenposten and their collaborators likely interpreted the reselection values incorrectly. The cells did not display any other characteristic IMSI-catcher behavior. It is thus likely that neither of these cells was spoofed by IMSI-catchers during the time of investigation.

In the technical description, Aftenposten claimed that there most likely was three more IMSI-catchers in Oslo, but did not give more details about these. According to Aftenposten, two of them were located in Parkveien and one at Aker Brygge. There were no anomalies graded to ”HIGH” severity in these areas in the forensic analysis by Delma.

PST focused on these nine cells in their status update, when they concluded that there were no indications of IMSI-catchers in Oslo[7].

5.7 Summary and Discussion of the Aftenposten Investigations

Aftenposten performed thorough network investigations in Oslo by the end of 2014. The investigations showed some anomalies in the networks in Oslo. The most severe of these were analyzed in this chapter.

The results of the survey performed with the CryptoPhone by Aftenposten cannot be used to conclude whether active attacks were performed at the time or not. It was known by the company producing the device that false positives often occur. No documentation of the effectiveness of the device exists either. Since no network anomalies were detected with the device, there are no clear indications that the device registered active IMSI-catcher attacks in Oslo at the time of the investigation.

The investigations performed with Network Guard were more thorough and professional, as the newspaper had acquired assistance from a company experienced in search after IMSI-catchers. The investigations resulted in a significant amount of data from the networks in Oslo and showed details of how the PLMNs in Oslo have configured their networks.

Three different security companies were used in the investigations, Aeger, CEPIA and Delma. Delma had the expertise and the device used in the search, but the company did not want any public attention. Delma found some anomalies, and detailed these to the other companies, which in turn described these to Aftenposten.

PST investigated the data Aftenposten based their conclusions on. The conclusion of PST presented at a "status update" in March 2015, was that there were no indications of false BTSs or IMSI-catchers in Oslo, based on the data acquired by Aftenposten. PST backed this conclusion with arguments for all the cells Aftenposten claimed were IMSI-catchers in their technical description[53]. PST did not mention any of the incidents that were graded to "HIGH" severity by Delma in the forensic analysis.

After PST dismissed the arguments from Aftenposten, the newspaper ordered a forensic analysis from Delma. The report by Delma contained much clearer arguments than was previously made by Aftenposten, CEPIA and Aeger, and pointed out many anomalies in the networks, some that were very suspicious[6, 61]. Neither Delma nor the newspaper analyzed the anomalies pointed out in greater details. A detailed technical analysis of the anomalies was performed in this chapter. The anomalies were compared to the observed configuration of the different networks, the GSM standard and common characteristics of IMSI-catchers.

A summary of all the incidents described in this chapter is shown in Table 5.10. It was found that the first articles published by Aftenposten in late 2014 seem to be based on misinterpretations of the data acquired with the Network Guard and the data acquired with the CryptoPhone. The cells first described as possible IMSI-catchers did not display any characteristic IMSI-catcher behavior, and acted similar to multiple other cells in the same networks. These cells are described in Section 5.6.7. Multiple other anomalies were detected in surveys performed before the first articles were published by Aftenposten, but they were not mentioned by the newspaper at the time. These anomalies were first mentioned in the forensic analysis report performed by Delma in 2015.

It was also found that it is a possible bug in the Network Guard software leading to some of the alarms. The potential presence of such a bug could not be verified in this thesis, as the source code of the Network Guard is not public, and Delma did not provide a detailed technical description of the device. However, if it was no software bug or measurement error, it is likely that these alarms were raised by IMSI-catchers.

One of the anomalies described by Delma, displayed some typical IMSI-catcher behavior, and was possibly caused by a rogue BTS. The cell did, however, display a very unusual difference between C1 and C2 that should not be possible in GSM. Since it is assumed that the data has not been tampered with, the unusual difference must have been caused by implementation errors, implementation choices in the Network

Guard choices or measurement errors. This anomaly was detected the 22.12.2014. It is described in Section 5.6.5. The anomaly was not commented by PST even though they had received a notice describing the anomaly.

Some of the anomalies found by Aftenposten might have occurred due to misconfigurations or non-optimal configurations of the GSM networks in Oslo. The investigations made by Aftenposten may lead to the PLMNs to fix these issues, and thus may lead to better configured cellular networks in Norway.

Several locations where anomalies were detected were only investigated once during the investigations in December 2014. Aftenposten did not perform a second survey at these locations until the survey in April 2015, long after the first publications of the articles. The data from the survey from April 2015 were not provided by Aftenposten and are thus not included in this analysis. Static surveys should have been performed at the locations were alarms graded to "HIGH" were detected, preferably a short time after the first alarms, to weed out false positives or to confirm results. Second surveys should especially have been done in the cases where anomalies were detected while the Network Guard was moving. Aftenposten and their collaborators did not do this.

Many of the anomalies discussed in this chapter could be confirmed or denied as IMSI-catchers by the PLMNs. The PLMNs could check if the observed data corresponds to the configuration of the networks. Nothing indicates that the PLMNs have done this.

Several false negatives could occur with both the devices used in the investigations by Aftenposten. The CryptoPhone can, for instance, not detect large C2 values and unusual LAC values. The Network Guard cannot detect if encryption is turned off. There are also several parameters that the Network Guard does not check, that could help in IMSI-catcher detection, such as the T3212, the actual values of the CRO, PT, TO and the CRH.

The Network Guard does not give reasons for "No GSM" measurements, thus it is impossible to determine whether the "No GSM" measurements are caused by suspicious activity or not. If the device could give indications of suspicious protocol incidents, such as location update rejects, the device would be more effective in IMSI-catcher detection, and the alarms raised by the device would be clearer. The "C anomaly" alarm on the Network Guard could possibly be implemented more effective, such that false positives would occur less often. A difference between C2 and C1 is most often not suspicious when the C2 value is less than the C1 value.

Table 5.10: Summary of all the incidents described.

Incident	Section	Alarm	Severity	Comment
CI 3629	5.6.1	”C Anomaly” ”Duplicated cell”	MEDIUM	It is confirmed that both Telenor and NetCom have CI 3629 in the area. Reselection (C) values did not display suspicious behavior compared to other observed NetCom cells. Likely not an IMSI-catcher.
NetCom Nydalen	5.6.2	”Service Denial” ”Channel LAC Change”	HIGH	”No GSM” measurement. LAC identical as the previous measurement. No other parameters were measured. Possible measurement error or bug.
LAC changes	5.6.3	”Cell LAC Change”	HIGH	LAC was observed to change to the LAC of the previous measurement. Possible measurement error or bug. Possible IMSI-catchers if the alarms were not caused by measurement errors or bug.
Cell 1091	5.6.4	”Provider anomaly”	HIGH	Network Norway and Telenor had a roaming agreement. Likely legitimate cell configuration and not an IMSI-catcher.
Cell 32478	5.6.5	”C anomaly” ”Service Denial”	HIGH	The only cell in Telenor’s network with C2 value greater than C1. Observations suggest invalid CRO values which could be due to how the reselection procedure is implemented on the Network Guard. The cell used a LAC no other cells used in Oslo. Possibly an IMSI-catcher.

CI changes	5.6.6	”Channel cell Change”	HIGH	Likely multiple cells in the same area on the same ARFCN. Could be due to misconfigurations of the networks in Oslo. Likely not IMSI-catchers.
Probable IMSI-catchers from January	5.6.7	”C Anomaly”	MEDIUM	Reselection values likely misinterpreted by Aftenposten. The cells did not display suspicious behavior compared to other cells in the same networks. Likely not IMSI-catchers.

Chapter 6
Conclusion

IMSI-catchers have been studied in this thesis. A thorough technical background of the subject has been presented, as well as practical experiments and observations from a large dataset acquired from GSM BTSs in Oslo.

A method of searching for BTSs and reading BTS configuration parameters was shown in Chapter 3. BTS configuration parameters related to IMSI-catchers were read and interpreted.

In Chapter 4, an open source IMSI-catcher was built and experimented with. A thorough explanation of the steps to configure the IMSI-catcher was presented. Two types of DoS attacks were successfully demonstrated in an experiment. In both the attacks IMSIs and IMEIs were caught. From the experiments, it was found that the IMSI-catcher should be in the vicinity of targeted MSs continuously for several minutes to be effective. The effectiveness of the IMSI-catcher depends on the C2 value calculated at the MSs compared to the C2 value of the legitimate cells in the area. It was found that the biggest drawback of the proposed IMSI-catcher is the Tx power. There are several ways the device can be improved, some of which are discussed in Section 6.1.

In this thesis, the IMSI-catcher investigations made by the Norwegian newspaper, Aftenposten, in Oslo in December 2014 have been analysed. A technical analysis was performed in Chapter 5. It was found that Aftenposten possibly observed at least one IMSI-catcher during the investigations. However, the measurements made of the most suspicious incident showed some values that should not be possible to observe according to the GSM standard.

It was found that some of the anomalies detected by Aftenposten may have occured due to a bug in the device performing parts of the investigation. However, if these anomalies were not due to a bug, they were likely caused by IMSI-catchers. Some of the data Aftenposten interpreted as suspicious were found to be according to

the configuration of the networks in Oslo. The data was in these cases most likely misinterpreted by Aftenposten and their collaborators. It is likely that the first articles published by Aftenposten in December 2014 were based on these misinterpretations. Some of the anomalies detected by Aftenposten were likely due to misconfigurations of the BTSs in Oslo.

6.1 Further work

6.1.1 Open Source IMSI-Catcher

The IMSI-catcher proposed in this thesis could be improved by several means. One improvement of the IMSI-catcher is to enlarge the C2 value. One way this can be done, is to install larger antennas than the VERT900 on the USRP. Another very effective way to enlarge the C2 value would be to broadcast a large CRO. Since the CRO value can be as large as 126 dBm, this could boost the C2 value significantly. It is however not possible to change the CRO value in OpenBTS v. 5.0.0. Changes would have to be made to the source code of OpenBTS to broadcast this value. In possible future work both these improvements could be done.

In further work, the configuration of the IMSI-catcher could be made automatic with software. It could also be further improved to perform interception attacks as described in Chapter 2 Section 2.9.3 and to avoid being detected by IMSI-catcher-catchers.

The IMSI-catcher proposed in this thesis can be used to experiment with BP memory corruption exploits, and find the attacks Weinmann found but did not publish[30].

6.1.2 Aftenposten Analysis

The analysis performed in this thesis only focused on the CryptoPhone investigation and the major incidents from the Network Guard investigation. All the alarms graded to ”HIGH” by Delma and some alarms graded to ”MEDIUM” by Delma were discussed. All the alarms graded to ”MEDIUM” and ”LOW” could be analyzed in possible further work.

References

[1] C. Paget, "Practical cellphone spying." https://www.youtube.com/watch?v=DU8hg4FTm0g, July 2010. Talk by Chris Paget at the Defcon 18. [Online; Accessed 09.06.2015].

[2] Y. Song, K. Zhou, and X. Chen, "Fake BTS attacks of GSM system on software radio platform," *Journal of Networks*, vol. 7, no. 2, pp. 275–281, 2012.

[3] M. Hadzialic, M. Skrbic, K. Huseinovic, I. Kocan, J. Musovic, A. Hebibovic, and L. Kasumagic, "An approach to analyze security of GSM network," in *Telecommunications Forum Telfor (TELFOR), 2014 22nd*, pp. 99–102, IEEE, 2014.

[4] M. Glendrange, K. Hove, and E. Hvideberg, "Decoding GSM," Master's thesis, NTNU, Norway, 2010.

[5] P. A. Johansen, A. Bakke Foss, and F. Hager-Thoresen, "Rapport om arbeidet med mobilovervåkning i Oslo," May 2015.

[6] G. McKay, "Mobile Network Forensic Analysis (Draft)," April 2015.

[7] PST, "Statusoppdatering i etterforskningssaken om mulige falske basestasjoner." http://www.pst.no/media/utgivelser/statusoppdatering-i-etterforskningssaken-om-mulige-falske-basestasjoner/. [Online; Accessed 09.04.2015].

[8] GSMA, "GSM." http://www.gsma.com/aboutus/gsm-technology/gsm. [Online; accessed 18.03.2015].

[9] S. M. Redl, M. K. Weber, M. W. Oliphant, and M. Weber, *An introduction to GSM*. Artech House Norwood, MA, USA, 1995.

[10] J. A. Audestad, *Technologies and systems for access and transport networks*. Artech House, 2007.

[11] GSMA, "IMEI Allocation and Approval Guidelines," *PRD TS*, vol. 6, 2010. [Online; Accessed 01.05.2015].

[12] D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi, *LTE Security*. John Wiley & Sons, 2012.

[13] ETSI, "Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification (3GPP TS 03.03 version 5.5.0 Release 1996)," 2003.

[14] U. R. Patel and B. N. Gohil, "Cell identity assignment techniques in cellular network: A review," in *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, vol. 2, pp. 594–596, IEEE, 2010.

[15] ETSI, "Digital cellular telecommunications system (Phase 2+); Functions related to Mobile Station (MS) in idle mode and group receive mode (3GPP TS 03.22 version 8.7.0 Release 1999)," 2002.

[16] ETSI, "Digital cellular telecommunication system (Phase 2+); Radio subsystem link control (3GPP TS 05.08 version 8.23.0 Release 1999)," 2005.

[17] ETSI, "Digital cellular telecommunications system (Phase 2+); Support of Localized Service Area (SoLSA); Service description; Stage 1 (3GPP TS 02.43 version 8.0.0 Release 1999)," 2001.

[18] ETSI, "Digital cellular telecommunications system (Phase 2+); Security aspects (3GPP TS 02.09 version 8.1.0 Release 1999)," 2006.

[19] ETSI, "Digital cellular telecommunications system (Phase 2+); Security-related network functions (3GPP TS 03.20 version 8.6.0 Release 1999)," 2008.

[20] ETSI, "Digital cellular telecommunications system (Phase 2+); Location registration procedures (GSM 03.12 version 7.0.0 Release 1998)," 1999.

[21] M. Briceno, I. Goldberg, and D. Wagner, "A pedagogical implementation of the GSM A5/1 and A5/2 "voice privacy" encryption algorithms," *Originally published at http://www.scard.org, mirror at http://cryptome.org/gsm-a512.htm*, 1999.

[22] E. Barkan, E. Biham, and N. Keller, "Instant ciphertext-only cryptanalysis of GSM encrypted communication," in *Advances in Cryptology-CRYPTO 2003*, pp. 600–616, Springer, 2003.

[23] F. A. Stevenson, "[A51] The call for Kraken." https://lists.srlabs.de/pipermail/a51/2010-July/000683.html, July 2010. [Online; Accessed 11.06.2015].

[24] K. Nohl, "Mobile self defence." https://www.youtube.com/watch?v=GeCkO0fWWqc, December 2014. Talk by Karsten Nohl at the annual Chaos Communication Congress, 27.12.2014. [Online; Accessed 01.05.2015].

[25] A. Kerckhoffs, *La cryptographie militaire*. University Microfilms, 1978.

[26] K. Scarfone, W. Jansen, and M. Tracy, "Guide to general server security," *NIST Special Publication*, vol. 800, p. 123, 2008.

[27] U. Meyer and S. Wetzel, "A man-in-the-middle attack on UMTS," in *Proceedings of the 3rd ACM workshop on Wireless security*, pp. 90–97, ACM, 2004.

[28] R. Bott and J. Frick, "Method for identifying a mobile phone user or for eavesdropping on outgoing calls," July 2001. EP Patent App. EP20,000,107,879.

[29] S. Yubo, Z. Kan, Y. Bingxin, and C. Xi, "A GSM/UMTS selective jamming system," in *Multimedia Information Networking and Security (MINES), 2010 International Conference on*, pp. 813–815, IEEE, 2010.

[30] R.-P. Weinmann, "Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks," in *6th USENIX Workshop on Offensive Technologies, WOOT'12, August 6-7, 2012, Bellevue, WA, USA, Proceedings*, pp. 12–21, 2012.

[31] S. Orr, "Stingray cell-phone trackers have been used here." http://www.democratandchronicle.com/story/watchdog/2015/04/10/stingray-cell-phone-trackers-used-in-rochester/25567137/, April 2015. [Online; Accessed 06.06.2015].

[32] MyFoxNY, "Police use cellphone spying device." http://www.myfoxny.com/story/25597191/police-use-cellphone-spying-device, May 2014. [Online; Accessed 06.06.2015.

[33] HARRIS, "Wireless products group price list," September 2008.

[34] H. Federrath, "Protection in mobile communications," 1999.

[35] F. Pönsgen, "GSM and GPRS security using OsmocomBB," Master's thesis, NTNU, Norway, June 2015.

[36] D. Strobel, "Imsi catcher," *Chair for Communication Security, Ruhr-Universität Bochum*, p. 14, 2007.

[37] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "IMSI-catch me if you can: IMSI-catcher-catchers," in *Proceedings of the 30th Annual Computer Security Applications Conference*, pp. 246–255, ACM, 2014.

[38] The Norwegian Competition Authority, "Vedtak V2015-1 - TeliaSonera AB (publ) - Tele2 Norge AS/Network Norway AS - Konkurranseloven § 16 jf. § 20 - inngrep mot foretakssammenslutning." http://www.konkurransetilsynet.no/ImageVaultFiles/id_7909/cf_5/2014-0289-355_Vedtak_V2015-1_-_OFFENTLIG_VERSJON.PDF, February 2015.

[39] Nkom, "Tildelte spektrumsillatelser." http://www.nkom.no/teknisk/frekvens/tillatelser/tildelte-frekvenstillatelser/_attachment/2319?_ts=14c2bcab361, March 2015. [Online; Accessed 27.04.2015].

[40] M. Dillinger, K. Madani, and N. Alonistioti, *Software defined radio: Architectures, systems and functions*. John Wiley & Sons, 2005.

[41] Ettus, "About." http://www.ettus.com/about. [Online; Accessed 25.04.2015].

[42] GNU Radio, "What is GNU Radio and why do I want it?." http://gnuradio.org/redmine/projects/gnuradio/wiki/WhatIsGR. [Online; Accessed 25.04.2015].

[43] "Airprobe." https://svn.berlin.ccc.de/projects/airprobe/. [Online; Accessed 26.04.2015].

[44] Nkom, "finnsenderen.no." http://finnsenderen.no/finnsender. [Online; Accessed 26.04.2015].

[45] DRLABS, "Airprobe how to." https://srlabs.de/airprobe-how-to/. [Online; Accessed 27.04.2015].

[46] Telenor. Personal communication, April 2015.

[47] NetCom. Personal communication, April 2015.

[48] Network Norway. Personal communication, March 2015.

[49] Nkom. Personal communication, March 2015.

[50] Range, "Main page." http://openbts.org/w/index.php/Main_Page. [Online; Accessed 23.04.2015].

[51] Range, "OpenBTSConfig." http://openbts.org/w/index.php/OpenBTSConfig, July 2014. [Online; Accessed 02.05.2015].

[52] GSMK, "GSMK CryptoPhone Baseband Firewall Technical Briefing,"

[53] P. A. Johansen, A. B. Foss, and F. Hager-Thoresen, "Teknisk beskrivelse av Aftenpostens kartlegging av mobilovervåking i Oslo," January 2015.

[54] Aftenposten, "Alt om mobilspionasje-saken." http://mm.aftenposten.no/mobilspionasje/. [Online; accessed 28.03.2015].

[55] P. A. Johansen and A. B. Foss, "Stortinget og statsministeren OVERVÅKES," December 2014.

[56] P. A. Johansen and A. B. Foss, "Revidert nasjonalbudsjett: Skal jakte mer på falske basestasjoner," May 2015.

[57] F. Rieger and V. UVIN, "Mobile device and method to monitor a baseband processor in relation to the actions on an applicaton processor," January 2014. US Patent App. 13/918,695.

[58] GSMK, "Source code." http://www.cryptophone.de/en/background/source-code/. [Online; Accessed 26.03.2015].

[59] K. Osterberg. Personal communication, 2015.

[60] CEPIA, "Falcon II - Hostile Network Detector," May 2014.

[61] G. McKay, “Mobile Network Forensic Analysis,” April 2015.

[62] P. A. Johansen, A. B. Foss, and F. Hager-Thoresen. Personal communication, March to June 2015.

[63] “God dekning. Uansett.” http://www.networknorway.no/artikler/god-dekning-uansett/. [Online; accessed 27.05.2015.

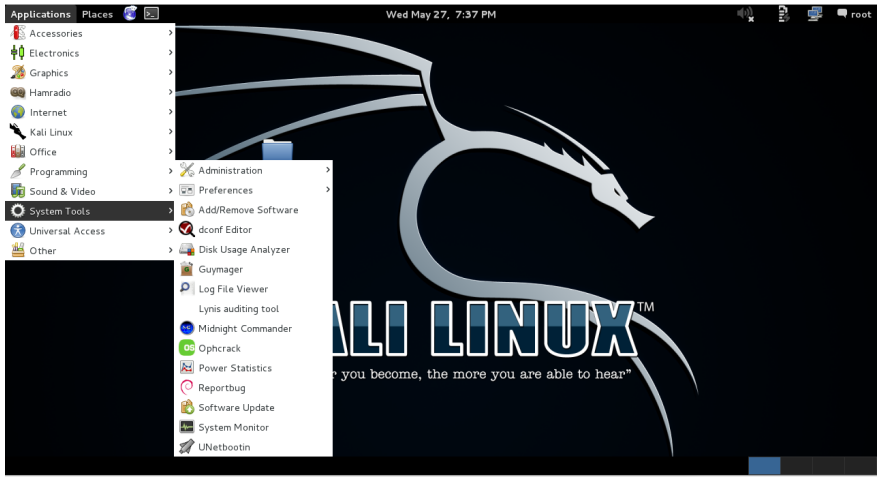
[64] M. Iedema, *Getting Started with OpenBTS*. " O’Reilly Media, Inc.", 2014.

Appendix

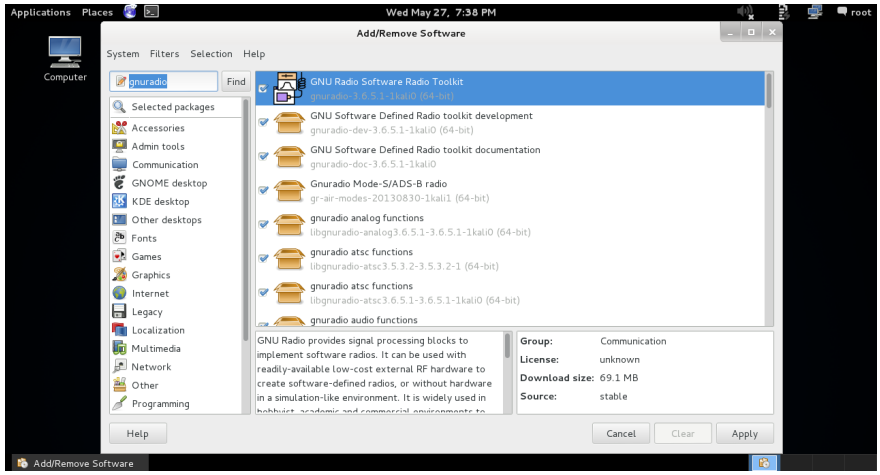
GNU Radio Installation Tutorial

This appendix provides a tutorial on how to install GNU Radio 3.6 on Kali Linux. By the time of writing, the newest version of GNU Radio is version 3.7. Because Airprobe does not support GNU Radio 3.7, it was decided to use 3.6. It was chosen to install the software on Kali Linux as there were issues when attempting to install both GNU Radio and Airprobe on Ubuntu 14.04. Kali Linux 10.1 provides a GUI for installing GNU Radio 3.6. The installation process is fairly straight forward.

Press ”Applications” –> ”System Tools” –> ”Add/Remove Software”



In the next view, search for ”gnuradio”, press ”Find”. Mark all checkboxes, and then press ”Apply”.



This will install GNU Radio and all dependencies, including the driver for the USRP, the USRP Hardware Driver Repository (UHD).

Appendix B

Airprobe Installation Tutorial

This appendix provides a tutorial on how to install Airprobe. Airprobe uses several libraries provided with GNU Radio. GNU Radio should be installed before following this tutorial. A guide on how to install GNU Radio on Kali Linux 10.1 is provided in Appendix A.

First install dependencies used by Airprobe.

```
$ sudo apt-get install cmake git libboost-all-dev
libusb-1.0-0 libusb-1.0-0-dev libfftw3-dev swig python-numpy
git-core autoconf automake libtool g++ python-dev swig
libpcap0.8-dev libpcsclite-dev c++-dev
```

Install libosmocore, used by gsm-receiver.

```
$ git clone git://git.osmocom.org/libosmocore.git
$ cd libosmocore
$ autoreconf -i
$ ./configure
$ make
$ sudo make install
$ sudo ldconfig
```

Download Airprobe.

```
$ git clone https://github.com/ksnieck/airprobe.git
```

Build gsm-decode.

```
$ cd airprobe/gsmdecode
$ ./bootstrap
$ ./configure
$ make
```

Build gsm-receiver.

```
$ cd airprobe/gsm-receiver
$ ./bootstrap
$ ./configure
$ make
```

Install tvoid.

```
$ cd airprobe/gsm-tvoid
$ ./bootstrap
$ ./configure
```

Appendix C

OpenBTS Installation Tutorial

A tutorial on how to install OpenBTS is provided in this appendix. A more thorough guide can be found in "Getting Started with OpenBTS"[64].

First download and install Git.

```
$ sudo apt-get install software-properties-common
    python-software-properties
$ sudo add-apt-repository ppa:git-core/ppa
$ sudo apt-get update
$ sudo apt-get install git
```

Download the OpenBTS code.

```
$ git clone https://github.com/RangeNetworks/dev.git
$ cd dev
$ ./clone.sh
```

The code has to be built specifically for the USRP it should be used with. In this thesis, the USRP N200 was used. The following command builds the OpenBTS software for the USRP N200.

```
$ ./build.sh N200
```

After the build script is finished, a new directory called "BUILDS" is created. This directory contains a subdirectory with the build"s timestamp. To install OpenBTS and related software one first need to change into the newly created directory. In the command, "TIMESTAMP" is changed with the timestamp of the build.

```
$ cd dev/BUILDS/TIMESTAMP/
```

Install a set of system configs that will allow a fresh Ubuntu system to work out of the box when installed.

```
$ sudo dpkg -i range-configs_5.0_all.deb
```

Install Asterisk.

```
$ sudo dpkg -i range-asterisk*.deb
$ sudo apt-get install -f
```

Install SIPAuthServe.

```
$ sudo dpkg -i sipauthserve_5.0_i386.deb
$ sudo apt-get install -f
```

Install OpenBTS.

```
$ sudo dpkg -i openbts_5.0_i386.deb
$ sudo apt-get install -f
```

The components can be started with the following commands:

```
$ sudo start asterisk
$ sudo start sipauthserve
$ sudo start smqueue
$ sudo start openbts
```

Note that the interface that communicates with the USRP needs to be on the same subnetwork as the USRP. The IP-address of the USRP is 192.168.10.2. The following command can be run:

```
$ sudo ifconfig eth0 192.168.10.3
```

”eth0” should be replaced with the name of the interface that is connected to the USRP.

Appendix D
CI Change Experiment

Aftenposten claimed in an email correspondence that several types of IMSI-catchers can cause uplink (from MS to BTS) communication by changing the CI that is broadcasted in the system information messages on the BCCH. It was not found any documentation for this claim. For this reason, it was tested with the IMSI-catcher proposed in this thesis.

The goal of the experiment was to determine if a CI change caused uplink communication, and thus a possibility for the IMSI-catcher to request IMSIs.

D.1 Experimental Setup

The following hardware and software were used in the experiment:

- Macbook Pro Early 2011, OSX Yosemite v. 10.10.1 with VirtualBox v. 4.3.20 installed.
- VM with Ubuntu server 12.04.4 installed. OpenBTS, Asterisk, SmQueue, SipAuthServe and tshark were installed on this VM.
- USRP N200 with a SBX 400-4400 MHz Rev 5.1 daughterboard, two VERT900 antennas and GPSDO Kit for USRP N200 Series.
- Samsung Galaxy S4.
- Motorola C118.

- Samsung Galaxy Mini II.
- iPhone 5s.

D.2 Experiment

The IMSI-catcher was set up with the following configuration:

- MNC = 260
- MCC = 03
- LAC = 123
- CI = 199

The MSs were manually set to camp on the cell of the IMSI-catcher. Then *tshark* was set up to log all messages sent to and from the BTS with the following command:

```
$ sudo tshark -i any -f "port 4729" -w ci_change.pcap
```

The CI was changed to 100 while the Samsung Galaxy S4 camped on the cell. All the messages sent to and from the IMSI-catcher in the time around the CI change was logged with tshark.

D.3 Results

The file generated with *tshark* was opened and interpreted in *Wireshark*. No messages sent from the MSs to the IMSI-catcher were observed. We can thus conclude that a CI-change to a valid CI value does not cause uplink communication. An IMSI-catcher will thus not be able to catch the IMSIs of the MSs camped on the IMSI-catcher during a CI change.