NTNU
Norwegian University of
Science and Technology

Investigation of LTE Privacy Attacks by Exploiting the Paging Mechanism

Shelley Xianyu Zhou

Master of Science in Telematics - Communication Networks and Networked
Submission date: May 2018
Supervisor: Stig Frode Mjølsnes, IIK
Co-supervisor: Øivind Kure, IIK
Ruxandra-Florentina Olimid, IIK

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

NTNU – Trondheim
Norwegian University of
Science and Technology

Investigation of LTE Privacy Attacks by Exploiting the Paging Mechanism

Shelley Xianyu Zhou

Submission date: May 2018
Responsible professor: Stig Frode Mjølsnes, IIK NTNU
Supervisor: Øivind Kure, ITS UiO; Ruxandra F. Olimid, IIK NTNU

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Title:	Investigation of LTE Privacy Attacks by Exploiting the Paging Mechanism
Student:	Shelley Xianyu Zhou

Problem description:

The paging signalling of the mobile access network is used by the core network to locate and notify the mobile equipment of incoming calls and other communications directed to the subscriber. These paging messages contain temporary or fixed identifiers of the mobile equipment and the subscription. The broadcasted paging message and the response message are not cryptographically protected in the current standard schemes. There have been multiple reports of misuse potential of the 2G and 3G mobile systems paging mechanisms to achieve mobile device location detection, tracking, and even Denial of Service (DoS). Recently similar attacks have been published for the LTE system.

This master thesis work will evaluate the LTE vulnerability to privacy by location detection and tracking and similar attacks, with a focus on the air interface mechanisms. The student will review LTE attacks described in the literature, in particular attacks where the paging procedure is exploited. Then the student should validate the attack feasibility, by planning useful experiments, set up the necessary experimental equipment, and perform data collection.

If time permits, the student will study the feasibility of active attacks using paging response masquerade.

Responsible professor:	Stig Frode Mjølsnes, IIK NTNU
Supervisor:	Øivind Kure, ITS UiO; Ruxandra F. Olimid, IIK NTNU

Abstract

In mobile communication in general, and LTE in particular, security should be a main focus, also because of the vulnerabilities introduced by the radio link. Compared to GSM and UMTS, the LTE security has been improved. However, the paging procedure is still not protected in LTE. The unprotected paging unfortunately opens possibility for hackers to gather sensitive information or track the user's location. This thesis studies attacks that are feasible because of the weaknesses of the paging procedure.

A theoretical study of published papers about the attacks making use of the paging procedure is conducted in this thesis. In addition, several published papers proposing countermeasures against the attacks are also studied.

In this thesis, a paging message catcher is set up and catches paging messages from the commercial LTE. A paging message catcher is basically a passive message sniffer. It listens to the paging channel of the LTE air interface, and collects paging messages. The collected paging messages are decoded and analyzed.

By analyzing the collected paging messages, it is confirmed that both Telia's and Telenor's LTE have enabled a non-standardized *smart paging* feature. The smart paging feature is introduced by most LTE vendors to improve the network resource efficiency. The feature essentially enables the network to page a user within one or few latest observed active cells instead of a whole tracking area. It has a side effect though in terms of location tracking by listening to the paging, as a paged user can be located within a much smaller geographical area.

In this thesis, it is verified how often Telia's LTE updates the temporary identity of a UE and what events trigger the updates. Telia is selected because of subscription availability. In LTE, a temporary identity is used to achieve user identity confidentiality. The temporary identity is supposed to get updated often enough to avoid traceability over time.

A paging response feeder is attempted as well in this thesis with the goal of verifying the feasibility and potential consequence for the victim. In contrast to the paging message catcher which is passive, a paging response feeder is an active attacking device. It acts as a UE and tries to feed in paging response impersonating a victim.

Preface

This Master's thesis is the result of the work in Information Security in the final semester of my Master of Science degree in Telematics at Norwegian University of Science and Technology. The thesis is written first under the supervision of Professor Øivind Kure, and then under Professor Stig Frode Mjølsnes and Ruxandra-Florentina Olimid from Department of Information Security and Communication Technology.

I would like to thank Professor Øivind Kure, Stig Frode Mjølsnes and Ruxandra-Florentina Olimid for very valuable guidance and feedback during the work with this thesis.

I would also like to thank Professor Yuming Jiang, who encouraged me to take the Master program and wrote recommendation letter for my application.

Finally, I would like to thank my family who give me ultimate support and courage to finish my thesis and accomplish my master study.

Shelley Xianyu Zhou

Trondheim, Sunday 13th May, 2018

Contents

List of Figures

List of Tables

List of Acronyms

3GPP 3rd Generation Partnership Project.

AK Anonymity Key.

AKA Authentication and Key Agreement.

AMF Authentication Management Field.

AS Access Stratum.

AuC Authentication Center.

AUTN Authentication Token.

BCCH Broadcast Control Channel.

BSC Base Station Controller.

CK Ciphering Key.

CMAS Commercial Mobile Alert Service.

C-RNTI Cell Radio Network Temporary Identifier.

DoS Denial of Service.

EAB Extended Access Barring.

EARFCN E-UTRA Absolute Radio Frequency Channel Number.

ECIES Elliptic Curve Integrated Encryption Scheme.

eDRX Extended Discontinuous Reception.

eKSI Key Set Identifier for E-UTRAN.

EMM EPS Mobility Management.

eNB Evolved NodeB.

EPC Evolved Packet Core.

EPS Evolved Packet System.

EPS AV EPS Authentication Vector.

ETWS Earthquake and Tsunami Warning System.

E-UTRAN Evolved UMTS Terrestrial Radio Access Network.

GPS Global Positioning System.

GSM Global System for Mobile communications.

GUMMEI Globally Unique MME Identifier.

GUTI Globally Unique Temporary UE Identity.

HSS Home Subscriber Server.

IK Integrity Key.

IMEI International Mobile Equipment Identity.

IMEISV IMEI and Software Version Number.

IMSI International Mobile Subscriber Identity.

KDF Key Derivation Function.

KSI Key Set Identifier.

LAU Location Area Update.

LTE Long Term Evolution.

MAC Message Authentication Code.

MCC Mobile Country Code.

MME Mobility Management Entity.

MMEC MME Code.

MMEGI MME Group ID.

MMEI MME Identifier.

MNC Mobile Network Code.

MO Mobile Originating.

MOC Mobile Originating Call.

MO-Data Mobile Originating Data.

MO-SM Mobile Originating Short Message.

MSC Mobile Switching Center.

MSIN Mobile Subscriber Identification Number.

MT Mobile Terminating.

MTC Mobile Terminating Call.

MT-Data Mobile Terminating Data.

M-TMSI Mobile - Temporary Mobile Subscriber Identity.

MT-SM Mobile Terminating Short Message.

NAS Non-Access Stratum.

NAT Network Address Translate.

NH Next Hop.

NMSI National Mobile Subscriber Identity.

PCH Paging Channel.

PDCCH Physical Downlink Control Channel.

PDCP Packet Data Convergence Protocol.

PDSCH Physical Downlink Shared Channel.

PDU Protocol Data Unit.

PHYID Physical Identity.

PLMN Public Land Mobile Network.

PSS Primary Synchronization Signal.

RAB Radio Access Bearer.

RAND Random Number.

RAU Routing Area Update.

RES RESponse.

RNC Radio Network Controller.

RNTI Radio Network Temporary Identifier.

RRC Radio Resource Control.

S1AP S1 Application Protocol.

SGSN Service GPRS Support Node.

SIB System Information Block.

SIB1 System Information Block Type 1.

SIM Subscriber Identity Module.

SMC Security Mode Command.

SNid Serving Network Identity.

SQN Sequence Number.

SRB0 Signaling Radio Bearer Type 0.

SRS Software Radio Systems.

SSS Secondary Synchronization Signal.

S-TMSI System Architecture Evolution Temporary Mobile Subscriber Identity.

TA Tracking Area.

TAC Tracking Area Code.

TAI Tracking Area Identity.

TAU Tracking Area Update.

UE User Equipment.

UICC Universal IC Card.

UMTS Universal Mobile Telecommunications System.

UP User Plane.

USIM Universal Subscriber Identity Module.

VLR Visiting Location Register.

XMAC eXpected Message Authentication Code.

XRES eXpected RESponse.

Chapter 1
Introduction

1.1 Motivation

Mobile communication has become an important infrastructure of the society since its taking into commercial use from early 1990's. Mobile communication technology has developed from voice centric Global System for Mobile communications (GSM), to more data focused Universal Mobile Telecommunications System (UMTS) until today's data centric Long Term Evolution (LTE), to meet the increasing data traffic demanding. Today LTE has been rolled out for most operators worldwide with a subscription base of more than three billions in 2018 [Por]. Because of the radio interface, the security has always been a main focus in mobile communication. Compared to GSM and UMTS, the security mechanism in LTE has been improved significantly. However, there still are a lot of signaling messages sent on the radio interface without security protection. One example of such messages is the paging messages. Paging is a fundamental device discovery function in LTE in order to locate the User Equipment (UE) in idle state whenever needed, for example to deliver data to the user.

Development of mobile communication technology brings the mobile with more and more functionalities, and mobile plays a more and more important role in our daily life. To protect the user identity and location privacy is one of the main focuses of mobile communication, including LTE. However, it turns out that a lot of information still can be gathered about the user by exploiting the unprotected paging messages.

A paging message catcher is basically a passive message collector, targeting at the broadcast paging messages from commercial LTE. Because paging messages are not security protected, the collected paging messages can be decoded, and the information can be analyzed to gather sensitive information about the users.

To improve network resource efficiency, a non-standardized *smart paging* feature is introduced by most LTE vendors. With smart paging, the network pages a user

within one or few cells instead of the whole Tracking Area (TA), and hence improves the network resource efficiency. On the other hand, it brings a disadvantage in terms of user location tracking, because the user can be located within a much smaller geographical area.

In LTE a temporary identity, Mobile - Temporary Mobile Subscriber Identity (M-TMSI), is used to protect the user permanent identity, International Mobile Subscriber Identity (IMSI). The temporary identity M-TMSI is supposed to be renewed often enough to avoid traceability. The network operator decides how often the M-TMSI is renewed.

Unlike passive paging message catcher, a paging response feeder is an active attacking device aiming to reply to the paging, masquerade as the supposed recipient and maybe cause service disturbance for the target. Open source software, which emulates LTE functionality, has been developed and become more and more mature. It might become feasible to build such paging response feeder with open source software.

1.2 Scope and Objectives

This thesis studies how the paging mechanism can be misused to breach the user identity confidentiality and location privacy in LTE, including an theoretical study of published papers and an attempt to build a paging response feeder. In particular, this thesis verifies how the commercial LTE in Norway is deployed to protect the user identity confidentiality and location privacy, including: 1) Verification of user identity used in the paging message. 2) Smart paging feature verification. 3) Temporary user identity update frequency checking.

The primary objectives of this thesis are:

1. Study and review the published attacks which exploit the paging mechanism, and the published corresponding countermeasures.
2. Build and set up a paging message catcher, subsequently use it to capture the paging messages from commercial LTE.
3. Decode and analyze the captured paging messages, and verify what type of user identity is used in the paging messages, the permanent identity or the temporary identity.
4. Verify if the smart paging feature is deployed from the analysis result of the captured paging messages.
5. Study how well Telia's LTE protects user identity confidentiality in terms of M-TMSI refreshment.

6. Study feasibility of building a paging response feeder with currently available open source software and hardware and potential impact to the target victim.

1.3 Work Method

The research methodology adopted in this thesis consists of three parts.

The first part is entirely a theoretical study. The primary sources are specifications produced by 3rd Generation Partnership Project (3GPP), described in Chapter 2. The other main sources are related works, which are described in Chapter 3.

The second part consists of practical experiments. This includes selecting proper tools, setting up the experiment equipment, configuring relevant parameters, updating source code if needed, investigating and troubleshooting faced errors. A paging message catcher is built and setup to capture the paging messages from commercial LTE networks. A paging response feeder is attempted. In addition, M-TMSI refreshment situation is studied.

The third part is about technical analysis. The collected data from the second part is analyzed, the conclusions are drawn accordingly and the findings are discussed.

1.4 Contributions

This thesis contains both a theoretical and a practical study of attacks that exploit the paging mechanism in LTE and make use of the unprotected paging message. The main contributions of this thesis include not only setting up and conducting the experiments, but also the analysis result of the collected data. The analysis results provide an insight of the Norwegian LTE implementation in respects to the user privacy protection. A paging message sniffer is set up and catches paging messages from commercial LTE of three operators in Norway. The user identity used in the paging message is verified. The smart paging feature is verified based on the collected data. During the observation period between Jan - Apr 2018, it is observed that the System Architecture Evolution Temporary Mobile Subscriber Identity (S-TMSI) does not get refreshed often in Telia's LTE. The other contribution is the attempt of paging response feeder, which might lead to further work in the topic.

1.5 Outline

This thesis consists of four chapters excluding this **Introduction** chapter.

Chapter 2 describes security mechanism in LTE, as well as the paging procedure in detail. It also provides definitions of several concepts which appear in the experiments.

The chapter provides necessary background information for a better understanding of this thesis.

Chapter 3 is a theoretical survey of related works, including published attacks and countermeasures in the relevant field.

Chapter 4 is about experimental work, including to build a paging message catcher, paging message analysis, smart paging verification, S-TMSI refreshment frequency checking, and an attempt to build a paging message feeder.

Chapter 5 summarizes the work and proposes potential future works.

Chapter 2
Background

This Chapter provides fundamental background information to this thesis work. The first section contains a general description of security aspects in LTE. The paging is described in detail in the second section. In the end, diverse relevant definitions are provided in the third section.

2.1 Security in LTE

This section describes the security architecture and main security features in LTE in a general level with special focuses on the radio interface and the user privacy. The main features of LTE security include: 1) Privacy of the user and device identities. 2) Mutual authentication between the user and the network. 3) Confidentiality of user and signaling data. 4) Integrity of signaling data [FHMN13, Chapter 6.2.2]. How these security features are achieved in LTE is described in the following subsections.

2.1.1 LTE Security Architecture

The LTE security architecture is illustrated in Figure 2.1. As illustrated, the authentication vector is transferred from the Home Subscriber Server (HSS) to the Mobility Management Entity (MME). The MME then initiates the authentication procedure with the UE, computes an eNB Key and sends it to the eNB. The Non-Access Stratum (NAS) signaling is both integrity and confidentiality protected and the security mechanism is integrated in the NAS protocol. The Access Stratum (AS) signaling is also integrity and confidentiality protected, but the User Plane (UP) is only confidentiality protected. Both AS and UP security protection is realized in the Packet Data Convergence Protocol (PDCP) layer between the UE and the eNB.

The terminal device has two parts: the Universal IC Card (UICC) and the UE. The UICC, or the Subscriber Identity Module (SIM) card known by the general public, is issued by the network operator. The UICC contains the permanent key shared between the network and the user. The UE performs the security calculation of the

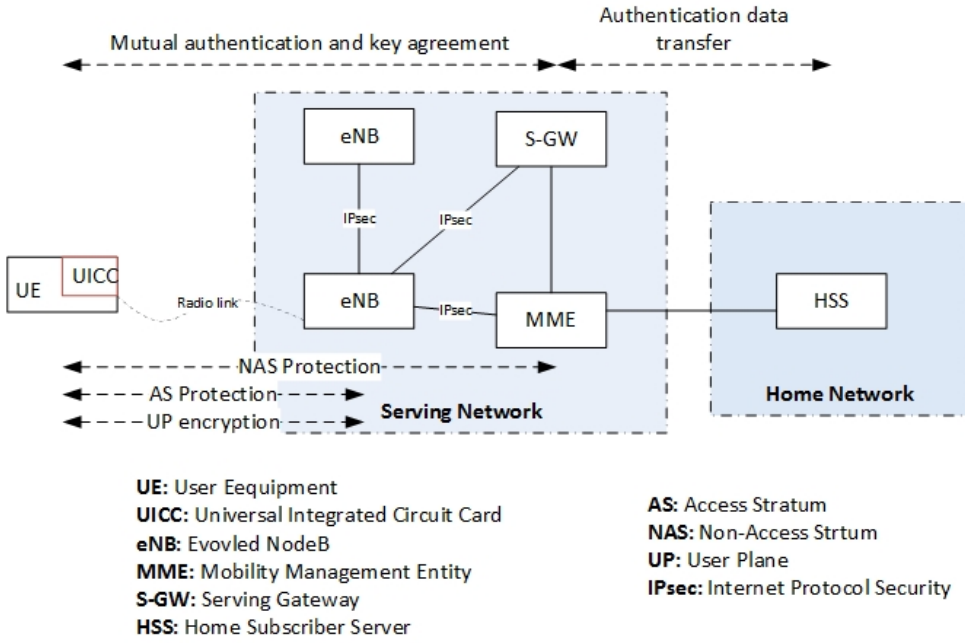

Figure 2.1: LTE security architecture, source [FHMN13, Figure 6.1, p. 80]

NAS, the AS and the UP. On the network side, the NAS protection terminates at the MME, while the AS and UP security protection terminates at the eNB.

2.1.2 Security Key Hierarchy

To achieve LTE security features, there are many keys, used for different purposes. In contrast to GSM and UMTS, where the session key is directly derived from the permanent key, LTE introduces an intermediate master key, $\boldsymbol{K_{ASME}}$, which is used to derive the session keys. The acronym ASME stands for Access Security Management Entity, and MME takes the role of ASME in LTE. The key hierarchy structure is illustrated in Figure 2.2.

On the top of the hierarchy, it is the permanent key, $\boldsymbol{K}$, which is shared between UICC and Authentication Center (AuC) and is never transmitted over the network. The second level is the Ciphering Key (CK) and the Integrity Key (IK), which are directly derived from the permanent key by the UICC and the AuC. They are sent from AuC to HSS on the network side and from UICC to UE on the mobile side. The third level is the intermediate master key, $\boldsymbol{K_{ASME}}$, derived from CK and IK by HSS and sent to MME. The fourth level are keys for NAS confidentiality, integrity protection and eNB/Next Hop (NH), derived by the MME. The MME then sends

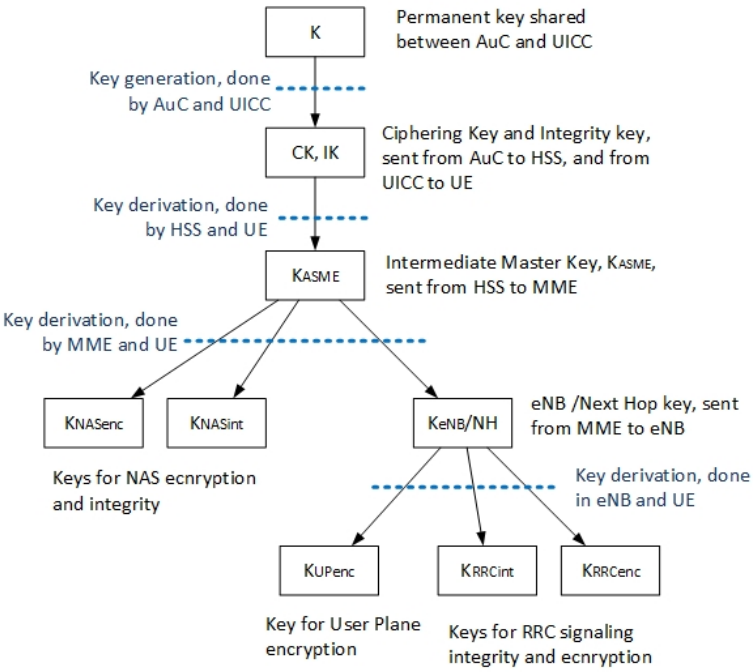

Figure 2.2: LTE Key Hierarchy, source [FHMN13, Figure 7.5, p. 118]

the key for eNB/NH to the eNB. The lowest level are keys for UP confidentiality, AS integrity and confidentiality protection, derived by eNB. On the mobile side, from and including the $\boldsymbol{K_{ASME}}$, all keys downwards are generated by the UE.

The key derivation function is a one-way function, which guarantees that the keys at the lower level do not leak key information at the higher level. During handover, a hash value of $\boldsymbol{K_{eNB}}$ is sent to the next eNB, in this way it avoids involvement of MME and also prevents key backwards exposure whenever possible. Different keys used for different purposes, namely *Key Separation*, not only makes it more difficult for the attackers, but also softens the impact of one compromised leaf key.

The CK and the IK are computed in LTE with two reasons: 1) For backwards compatibility with UMTS, where they are directly used; 2) To make it possible to reuse the Universal Subscriber Identity Module (USIM), which can only compute CK and IK. As soon as the $\boldsymbol{K_{ASME}}$ is generated, the CK and IK are deleted.

2.1.3 Authentication and Key Agreement

The LTE Authentication and Key Agreement (AKA) procedure achieves two goals: 1) Mutually authenticate the user and the home network, which is one of LTE

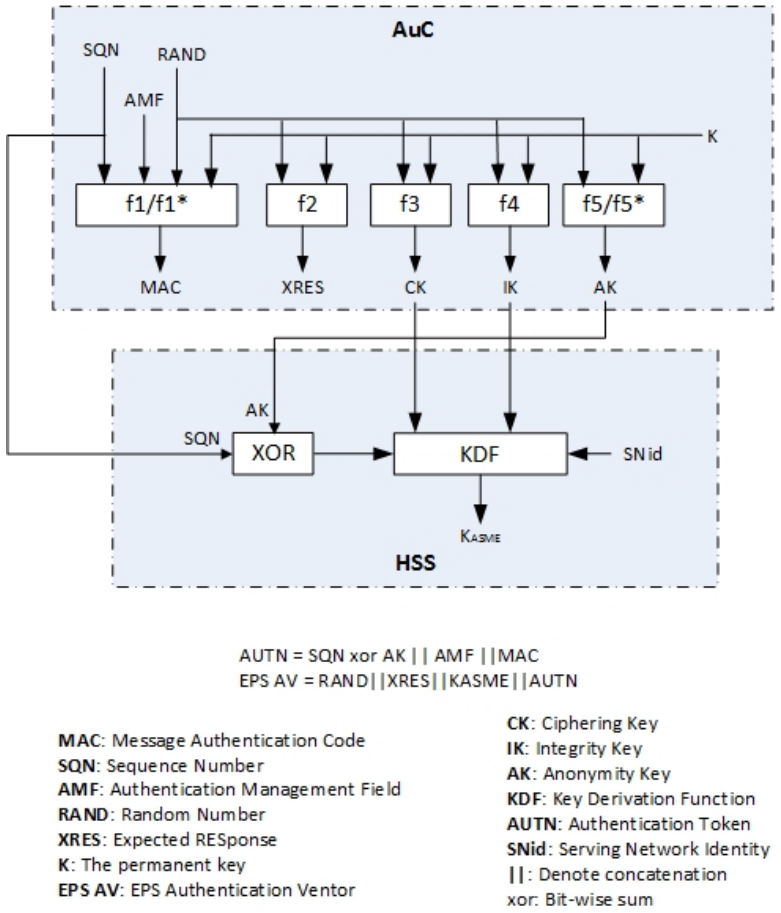

Figure 2.3: LTE Authentication Vector generation, source [FHMN13, Figure 7.2, p. 109]

security features. 2) Establish a fresh shared key between the serving network and the UE. This section describes the AKA procedure and demonstrates how the goals are achieved.

Figure 2.3 shows the generation of EPS Authentication Vector (EPS AV) in AuC/HSS. The key generation functions, *f1 - f5*, run in AuC and UICC, and are completely under the control of the network operator. Therefore, they can be operator proprietary and hence are not standardized. However, the Key Derivation Function (KDF) running in the HSS and the UE to generate the intermediate master key, is standardized in order to ensure interoperability between products from different vendors.

Upon request, the AuC first generates two numbers: a Sequence Number (SQN) and

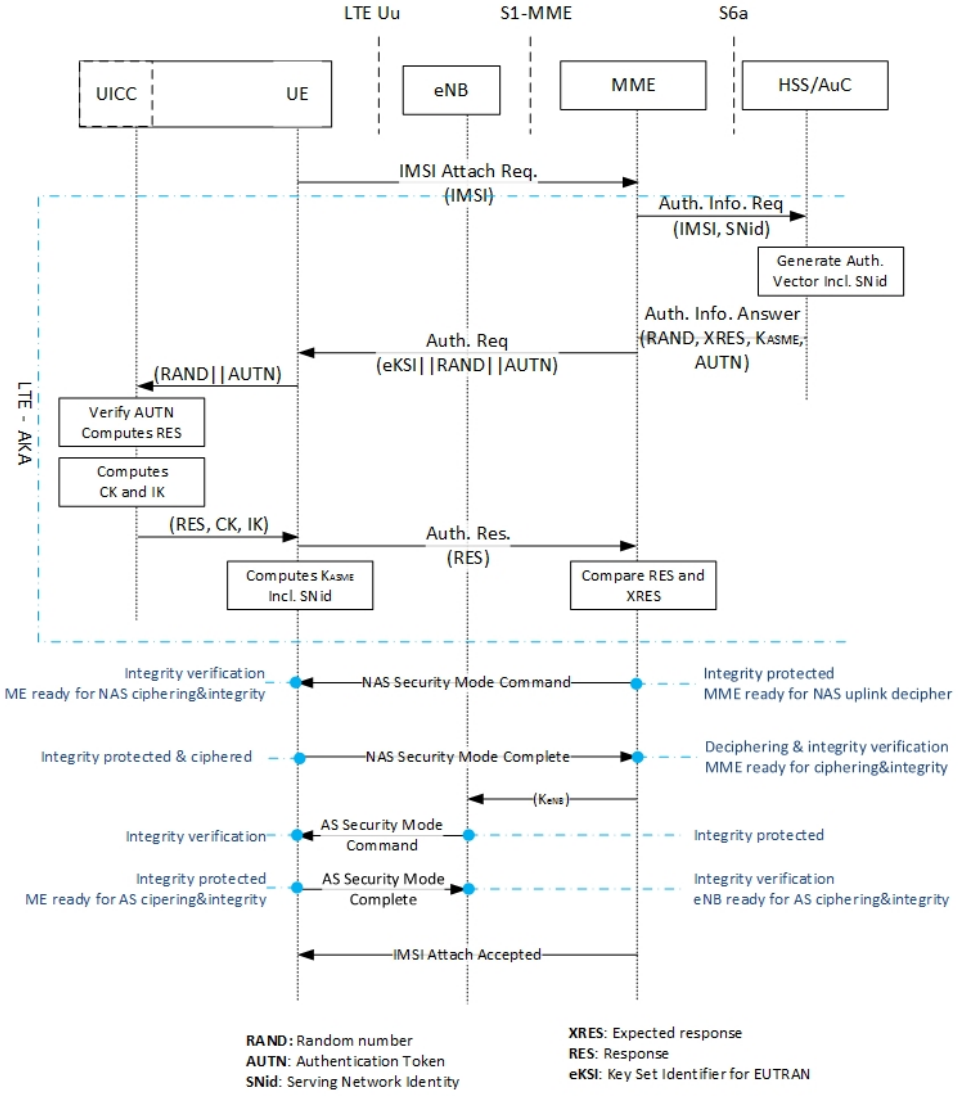

Figure 2.4: An overview of LTE AKA and security activation, source [FHMN13, Figure 7.1, 8.1&8.2]. The messages crossing the eNB are transparently forwarded by the eNB. For clarity and readability reason, only the most relevant parameters of the messages are listed.

a Random Number (RAND). With them, the Authentication Management Field (AMF) and the shared permanent key, the AuC computes the authentication values - an eXpected RESponse (XRES) and a Message Authentication Code (MAC) - and three keys - CK, IK and Anonymity Key (AK). Then the AuC sends them all to the

HSS, which in turn derives the intermediate master key, $\boldsymbol{K_{ASME}}$, with the Serving Network Identity (SNid) as one of the inputs. The Authentication Token (AUTN) contains *(SQN xor AK // AMF // MAC)*, and EPS AV contains *(RAND // XRES // K_{ASME} // AUTN)*, where *'//'* denotes concatenation and *'xor'* denotes bit-wise sum. The XRES is used to authenticate the user while the MAC is used to authenticate the home network, which is described later.

Figure 2.4 shows an overview of the LTE AKA procedure and when the various security protection gets activated, only messages with positive outcome are illustrated in the figure. The AKA procedure is normally triggered by some other specific procedures, for example the Tracking Area Update (TAU) or the IMSI attach. The IMSI attach is illustrated in the figure as an example.

The serving MME sends the Authentication Information Request message to the HSS asking for EPS AV with IMSI and SNid as parameters. The SNid consists of Mobile Country Code (MCC) and Mobile Network Code (MNC). The HSS generates the EPS AV as illustrated in the Figure 2.3, and sends back the EPS AV, containing *(RAND // XRES // K_{ASME} // AUTN)*, in the Authentication Information Answer message. After receiving the EPS AV, the MME sends *(RAND // AUTN)* to the UE in the Authentication Request message.

The UE forwards the received *(RAND//AUTN)* to the UICC. With the received RAND and the shared permanent key, $\boldsymbol{K}$, the UICC computes AK using the function *f5*. With the AK, the UICC extracts the SQN from the received AUTN, since *(SQN xor AK xor AK = SQN)* with assumption that the received data is correct. Now the UICC has all required inputs to compute the eXpected Message Authentication Code (XMAC) using the function *f1*. If the computed XMAC matches the received MAC, which is contained in the AUTN, the UICC will computes the RESponse (RES), CK and IK using the functions *f2, f3, and f4* respectively, and sends them all to the UE. The UE sends the RES further to the serving MME, which will verify if the RES equals the XRES to authenticate the user. The MAC verification ensures that the EPS AV is actually from the home network, while the RES verification authenticates the user. If there is no Authentication Reject message from the serving MME, the UE derives the intermediate master key, $\boldsymbol{K_{ASME}}$. In this way, the UE and the serving network have successfully established a pair of fresh shared key.

After the serving MME has successfully authenticated the UE, the MME sends an integrity protected NAS Security Mode Command (SMC) message to the UE instructing the UE to activate NAS signaling integrity and confidentiality protection. The MME is prepared to receive ciphered uplink NAS messages after sending the SMC message. Among others, the SMC message contains selected security algorithms and the Key Set Identifier for E-UTRAN (eKSI). The UE verifies the integrity of

the received SMC message using the included algorithm and the NAS integrity key, $\boldsymbol{K_{NASint}}$. After successful integrity verification, the UE replies with a ciphered and integrity protected Security Mode Complete message to the MME. The MME deciphers the received message and verifies its integrity. After successful Security Mode Complete message deciphering and integrity verification, all NAS messages exchanged between the UE and MME are integrity protected and ciphered. With successful run of the NAS SMC procedure, the serving network gets implicitly authenticated, as it is proven that the shared key K_{ASME} is identical between the UE and the MME, and the K_{ASME} is derived with the SNid as one input.

Afterwards, the serving MME sends the $\mathrm{K_{eNB}}$ to the eNB, which in turn initiates AS SMC towards the UE. The AS SMC is integrity protected but not ciphered, and it contains selected AS security algorithms. The UE replies an integrity protected AS Security Mode Complete message after successful integrity verification of the received AS SMC. From now on, all AS signaling messages are ciphered and integrity protected provided that the AS Security Mode Complete message arrives the eNB and passes verification. User data ciphering also gets started onwards.

2.1.4 Security Context

When a UE communicates with the network with security protection enabled, the UE and the network have to share a set of identical parameters for security protection, such as keys, algorithms, counters etc. The set of security parameters is called *security context*.

The Evolved Packet System (EPS) security context has two parts: EPS NAS and AS security contexts. The NAS security context is the set of parameters used to protect the NAS messages, while the AS security context is the set of parameters used to protect the AS messages and the UP. The AS security context only exists when the UE is in Radio Resource Control (RRC) CONNECTED state, otherwise it is void [TS3b, 3GPP TS33.401]. This is the reason why all RRC messages before the UE goes to the CONNECTED state are not cryptographically protected. Instead, the EPS NAS security context is stored in the non-volatile memory of the UE and can exist even when the UE is de-registered. The stored security context can be used to protect the integrity of the initial NAS message, e.g. the Service Request and the Attach Request messages.

Based on the origin, a security context can be *'mapped'* when it is converted from a UMTS security context, or *'native'* when it is produced via an EPS AKA procedure. Based on the number of security parameters, a security context can be *'full'* when it contains all security parameters, or *'partial'* when it contains only part of the parameter set. In the Figure 2.4, the obtained security context before the NAS SMC procedure is *'partial'* as it does not contain the K_{NASint} and K_{NASenc} yet, it becomes

'full' after successful NAS SMC completion. Based on if it is in use or not, a security context can be *'current'* when it is currently in use, or *'non-current'* when it is not in use yet and will be taken into use in the future. A *'mapped'* security context is always *'full'* and *'current'*, and it gets discarded as soon as the current session has terminated. Afterwards, a *'native'* and *'non-current'* security context will become *'current'*, meaning being taken into use.

The security context is an important concept, as it helps to understand what messages are security protected and what are not, and hence it helps to identify attacking possibilities.

2.1.5 Identification

The user and terminal identifications are not only fundamental to provide basic voice and data services to the subscribers, they also play an essential role to achieve the security features. Every user has different identifications used in various contexts, some are permanent while others are temporary.

International Mobile Subscriber Identity (IMSI)

The IMSI is a globally unique identifier of a subscriber in LTE, allocated by the network operator. It is static and bound with the UICC. In the LTE security architecture, the IMSI is the identifier of the permanent key.

The structure of the IMSI is showed in the Figure 2.5. As illustrated, the IMSI is composed of the MCC, the MNC and the Mobile Subscriber Identification Number (MSIN), with a total length of no more than 15 digits [23., Chapter 2.2]. The MSIN uniquely identifies a mobile subscriber within one operator. The MNC and the MSIN

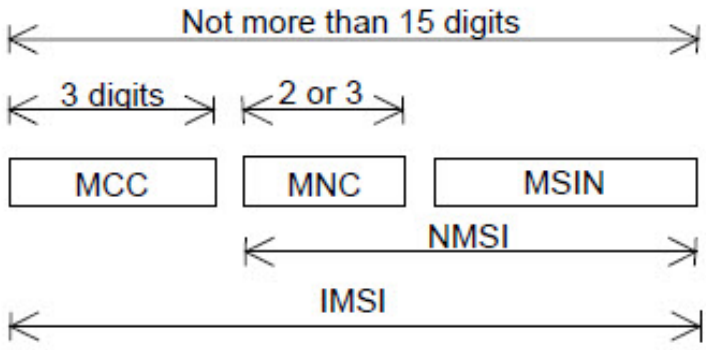

Figure 2.5: IMSI Structure [23., 3GPP TS23.003, Chapter 2.2]

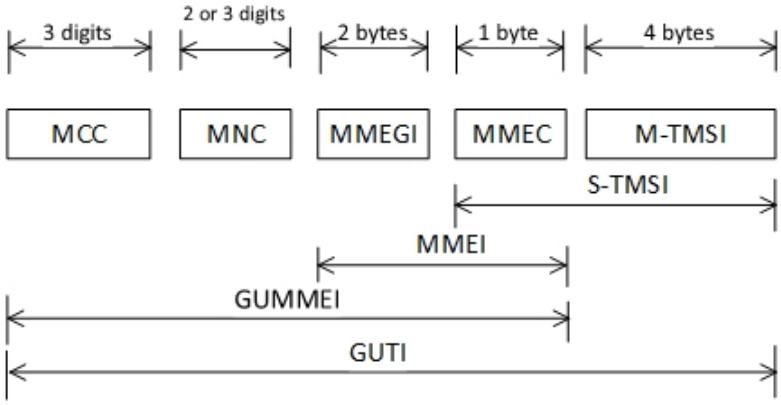

Figure 2.6: GUTI Structure [23., 3GPP TS23.003, Chapter 2.8]

together is National Mobile Subscriber Identity (NMSI), which uniquely identifies a subscriber within one country.

Globally Unique Temporary UE Identity (GUTI)

The Globally Unique Temporary UE Identity (GUTI) is introduced first in the LTE. It is a temporary identity, and is always used to identify a subscriber whenever available, aiming to minimize the usage of the permanent identity, IMSI. The GUTI is used to provide confidentiality of the user identity, one of the LTE features, as it is temporary and refreshed often. If the UE and the network have agreed to use ciphering, the GUTI should always be sent ciphered.

The structure of the GUTI is illustrated in Figure 2.6. The GUTI has two components, the Globally Unique MME Identifier (GUMMEI) and the M-TMSI. The GUMMEI uniquely identifies the MME which has allocated the GUTI, and the M-TMSI uniquely identifies the visiting subscriber within that MME. The GUMMEI is constructed of the MCC, MNC, MME Group ID (MMEGI) and the MME Code (MMEC). The MMEGI and the MMEC together constructs the MME Identifier (MMEI), and the MMEC and the M-TMSI together is called S-TMSI. The shortened S-TMSI is normally used, improving the efficiency of signaling procedure.

International Mobile Equipment Identity (IMEI) and Software Version Number (IMEISV)

An LTE user device is uniquely identified by the International Mobile Equipment Identity (IMEI) or the IMEI and Software Version Number (IMEISV). The IMEI/IMEISV is static and bound to the user device. As a user commonly keeps using the device for a long period, the IMEI/IMEISV can be used to track the user. That's why the

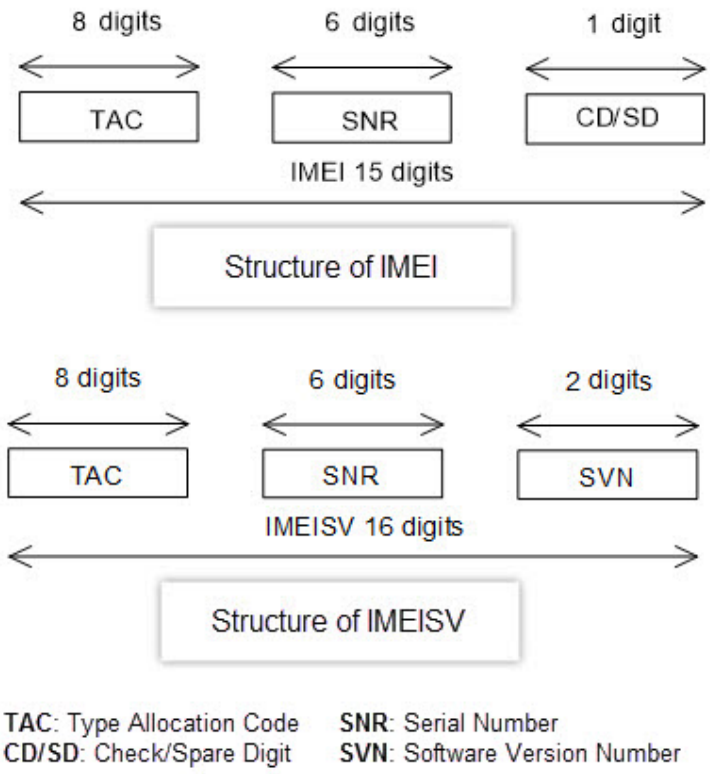

Figure 2.7: IMEI and IMEISV Structure [23., 3GPP TS23.003, Chapter 6.2].

IMEI/IMEISV should never been sent before a valid security context gets established and activated. Besides, if configured as such, the network might block a user device to access network based on the IMEI/IMEISV, for example to prevent a stolen device from being taken into use.

The structure of the IMEI and the IMEISV are showed in the Figure 2.7. Both IMEI and IMEISV contain an eight-digit Type Allocation Code and a six-digit Serial Number. The last digit of the IMEI is a Check Digit/Spare Digit, while the last two digits of the IMEISV is the Software Version Number. The Type Allocation Code is allocated by the GSM Association to the mobile device manufacturer, who in turn allocates a unique Serial Number within the same Type Allocation Code. The manufacture also assigns the software version number.

2.1.6 Active versus Passive Attack

By common sense, an attack is said to be active when the attacking device in any way communicates or reacts with the concerned target; while an attack is said to be passive when the attacking device does not communicate with the concerned target but only listens to the traffic, captures data etc. In practice, the passive attack is much more difficult to be detected than active attack, and the impact of passive attack might not be noticed at all.

Some examples of active attacks are Denial of Service (DoS) attacks, traffic spoofing, replay attack, Man-in-the-middle attack, and endless other attacks. The passive attack examples could be eavesdropping, traffic sniffer, data collection, traffic pattern analysis and so on. In this thesis work, the first part of the experiment is passive, as it only captures broadcast messages; while the second part to feed the paging response is active, because it replies the paging request impersonating the victim.

With GUTI and signaling confidentiality protection, provided with proper implementation, the LTE security architecture is capable of protecting user identity privacy against passive attacks, such as eavesdropping, user tracking via following the GUTI. However, it is not capable of protecting against active attacks, as it is proven that the IMSI Catcher can be built in the LTE [Jov16, Sør17].

2.2 Paging

One fundamental function of the mobile network is mobility management to provide seamless service for the users under movement. When a mobile switches on, it runs the attach procedure to connect to the network and informs its location. Afterwards it informs the network about its location, either when it moves to a different tracking area or periodically.

When a mobile is in the idle mode, the network initiates the paging procedure when it needs to know the accurate location of the mobile or to deliver services to the mobile. The concept of paging is maintained the same from GSM, UMTS and further to LTE, although different terms are used in different generations of mobile networks. This chapter describes the paging procedure in detail using the terms in LTE.

2.2.1 Paging Procedure

Same as in GSM and UMTS, when a mobile turns on, it initiates the IMSI attach procedure to gain network access and to inform about its location to the network. Later on, the mobile sends TAU to update its location to the network, either periodically or when it comes to a different TA. The corresponding procedure is

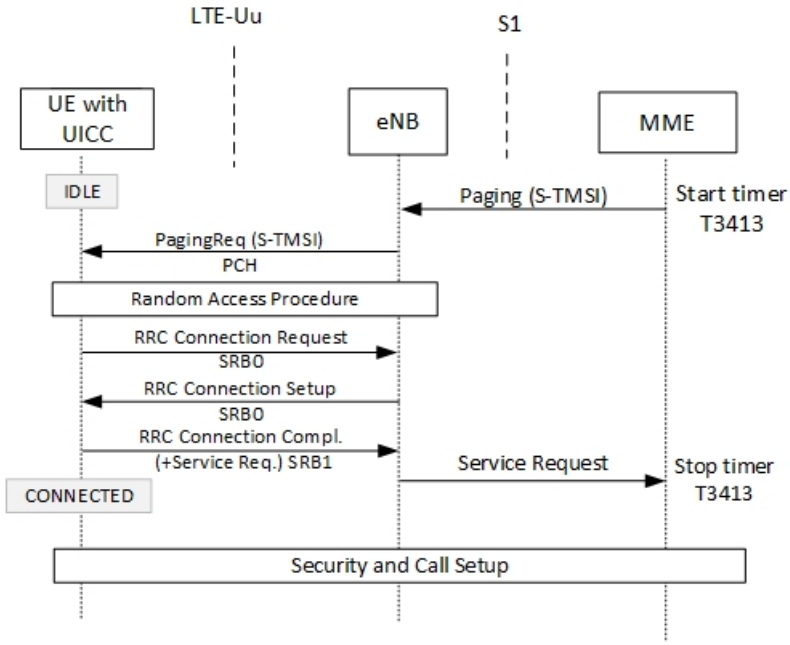

Figure 2.8: LTE Paging Procedure, source [SBA+15, Fig.2]

Routing Area Update (RAU) in UMTS and Location Area Update (LAU) in GSM. In this way, the mobile keeps informing the network about its location.

Since the mobile in idle state informs about its location to the network only when it comes into a different TA, the network knows in which TA the mobile locates, but not in which cell. When the network needs to know the precise location, i.e. in which cell, of the mobile, it pages the mobile to all cells in the latest known TA. If there is no response from the mobile, the network might page to all TAs. On NAS level, the paging procedure is described in the 3GPP specification TS 24.301 [TS2b, Chapter 5.6.2]. On RRC level, the paging procedure is described in the 3GPP specification TS 36.331 [TS3g, Chapter 5.3.2].

The paging procedure for the most common scenario, i.e. to request the establishment of a NAS signaling connection with a UE, is illustrated in the Figure 2.8.

The serving MME sends the paging message to all eNBs within the TA over the S1 interface and starts the timer T3413. The concerned eNBs process it and send it further to the radio interface on the Paging Channel (PCH) to all cells under its control and within the TA. The paging massage is neither integrity nor confidentiality protected.

Table 2.1: Paging Message content on the S1 interface, [TS3h, Chapter 9.1.6]. The **M** and **O** in the Presence column stands for Mandatory and Optional respectively.

Field Name	**Presence**	**Description**
Message Type	M	Message Type, coded for Paging Message
UE Identity Index Value	M	Used to calculate Paging Frame Number
UE Paging Identity	M	UE Identity (IMSI or TMSI)
CN Domain	M	Normally PS
List of TAIs	M	At least one TAI should be included
Other optional fields when applicable	O	Other parameters for other circumstances

All UEs in the idle mode listen to the paging channel and check the identity included in the paging message. The UE detecting its identity will first initiate the Random Access procedure to gain one Signaling Radio Bearer Type 0 (SRB0), then the RRC Connection Establishment procedure to establish the RRC connection, and in the end will initiate the Service Request procedure to gain a NAS connection with the MME. The timer T3413 stops when the Service Request message arrives the MME.

Table 2.1 shows the paging message content on the S1 interface between MME and eNB. Among others, the UE Identity and a list of Tracking Area Identities (TAIs) are included. As the table shows, there is no security related parameter in the paging message. All fields of the paging message on the S1 interface are included in the paging message on the air interface except the TAI list.

2.2.2 RRC Paging Message Type

There are following paging message types defined in 3GPP TS36.331 [TS3g]:

- pagingRecord - To transmit paging information initiated from MME to UE. Typically, terminating services, such as voice call, text message or incoming data, trigger paging from MME. One RRC paging message can contain up to 16 pagingRecords.

- systemInfoModification - To inform UE of a Broadcast Control Channel (BCCH) modification other than SIB10, SIB11, SIB12 and SIB14. This indication does not apply to UEs using Extended Discontinuous Reception (eDRX) cycle longer than the BCCH modification period.

- etwsIndication - To notify UE of an Earthquake and Tsunami Warning System (ETWS) primary and/or secondary notification.
- cmasIndication - To notify UE of a Commercial Mobile Alert Service (CMAS) notification.
- eabParameterModification - Inform UE of an Extended Access Barring (EAB) parameters (SIB14) modification.
- redistributionIndication - To inform UE to trigger Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) inter-frequency redistribution procedure as specified in 3GPP TS36.304.
- systemInfoModification-eDRX - To inform UE of a BCCH modification other than SIB10, SIB11, SIB12 and SIB14. This indication applies only to UEs using eDRX cycle longer than the BCCH modification period.

The type of paging messages studied in this thesis work is dominantly pagingRecord.

2.2.3 Paging Response

As illustrated in Figure 2.8, upon reception of a paging message, the target UE sends the Service Request message to the MME after having established the RRC connection. The Service Request message is typically piggybacked in the RRC Connection Complete message with RRC Establishment Cause 'mt-Access' indicating that it is a paging response [TS2b, Annex D.1]. On the S1 interface, the Service Request message is carried in S1 Application Protocol (S1AP) NAS Transport Message with Initial UE Message type Protocol Data Unit (PDU) [TS3h, Chapter 8.6.2.1].

The content of the NAS Service Request message is listed in the Table 2.2. The Security Header Type tells how the message is protected, either integrity protected, integrity and confidentiality protected or not protected at all. The Service Request message is a non-standard L3 message, and has value in binary *1100* for the Security Header Type. The Key Set Identifier (KSI) indicates which key is used to calculate the MAC. The Sequence Number is also one of the inputs to computes the MAC. In the end, it contains a two bytes short form MAC protecting its integrity. *"The integrity protection shall include octet 1 and 2 of the SERVICE REQUEST message. ... Only the 2 least significant octets of the resulting message authentication code are included in the information element."* [TS2b, Chapter 9.9.3.28]. If the integrity check fails in the MME, the Service Request will get rejected with the cause #9 - "UE identity can not be derived by the network" in case of non-emergency bearer service [TS2b, Chapter 4.4.3].

Table 2.2: NAS Service Request Message Content [TS2b, Table 8.2.25.1]. The **M** and **O** in the Presence column stands for Mandatory and Optional respectively.

Field Name	**Presence**	**Description**
Protocol discriminator	M	Encoded based on [TS2a, 3GPP TS24.007].
Security header type	M	Indicating Security type. Encoded as 1 1 0 0 in binary for NAS Service Request message
eKSI and Sequence Number	M	Key Set Identifier (3-bit) and Sequence Number (5-bit)
Message authentication code (short)	M	Two bytes short form MAC.

2.2.4 Paging Performance

The purpose of the paging procedure is to locate the user efficiently and quickly. Based on this, paging performance can be measured with several parameters, as described in [ZB07]:

- **Paging delay:** It's the time starting from when the paging message leaves the MME to the time when the paging message reaches the target UE. The shorter the delay is, the better it is.
- **Success rate:** The likelihood of paging the precise cell where the UE locates. When the paging message is broadcasted to the whole TA, the success rate should be very close to 100%. Only the UEs without getting its TA properly updated would fail.
- **Cost of paging:** It is measured by the total number of paged cells until the UE is successfully paged.
- **Cost of location management:** The cost of resources to keep the UE updated about its location. Basically, it is the cost of location updating. The more often a UE updates its location, the more the cost becomes.

Normally there is a trade-off between the cost of location management and the cost of paging. For example, with maximum cost of location management when a UE updates its location whenever it crosses a cell border, there is no need for paging, i.e. the cost of paging is zero. On the other extreme end, with maximum cost of paging when paging message is broadcasted to the whole network, there is no need of location updating, i.e. the cost of location management becomes zero. The network operator needs to plan the network carefully to get optimal results.

Sometimes there is trade-off between other performance parameters, for example the paging delay and the cost of paging. The smart paging feature which is described later, significantly decreases the cost of paging but slightly increases the paging delay, which is fortunately negligible.

2.2.5 Smart Paging

As described in Clause 2.2.1, the paging message is normally broadcasted to a whole TA, which contains many cells. Consequently, the paging message is sent to many cells unnecessarily and hence causes resource waste. To improve the resource efficiency, with cost of potential paging delay, the smart paging feature is introduced [Nok]. Instead of sending the paging message to the whole TA, the network sends it only to the cell where a UE is latest observed active or to few neighbor cells around based on certain algorithms. If there is no response received within the timer, the network then sends the paging message to the whole TA or even to the whole network, if configured as such.

With the smart paging feature, the paging traffic gets reduced significantly. On the other hand, from security point of view, the location of a user can be limited within one cell, typically two km^2, via passively sniffing the paging message of the user. This thesis verifies if the smart paging feature is deployed in the main Norwegian LTEs.

2.2.6 User Identity in Paging Message

To protect user privacy, the S-TMSI is used whenever possible to identify a user in the paging message. The serving MME keeps track of the S-TMSI of a UE, and it should refresh the S-TMSI often enough to prevent against location tracking via observing the S-TMSI. The MME initiates the GUTI Reallocation procedure to reallocate a new S-TMSI to the UE.

At rare cases, the network might page a UE with its permanent identifier IMSI. This is an abnormal scenario and is only used for error recovery in the network. Upon reception of a paging message with its IMSI, the UE should discard all EPS security contexts if any, terminate all running specific procedures, and then initiate the attach procedure to regain network access.

2.3 Diverse Related Information

2.3.1 Radio Network Temporary Identifier

The Radio Network Temporary Identifier (RNTI) is a unique identifier of a RRC connection and scheduling. As listed in Table 2.3, there are several types of RNTI

Table 2.3: Type of RNTI and its value range [TS3f, 3GPP TS36.321 Chapter 7.1]

Value in Hex	**RNTI Type**
0000	Not in use
0001 - FFF3	Cell Radio Network Temporary Identifier (C-RNTI), RA-RNTI
FFF4 - FFF8	Reserved for future use
FFF9	SI-RNTI
FFFA	SC-N-RNTI
FFFB	SC-RNTI
FFFC	CC-RNTI
FFFD	M-RNTI
FFFE	P-RNTI
FFFF	SI-RNTI

[TS3f, 3GPP TS36.321]. The detail usage of each type of RNTI can be found in 3GPP TS36.321 [TS3f, Table 7.1-2].

For the experiments, the RNTIs of our interest are P-RNTI and SI-RNTI, which are used for the paging message and the System Information Blocks (SIBs) respectively. When run the srsLTE example application *pdsch_ue* to capture the paging message and the System Information Block Type 1 (SIB1), the respective value needs to be specified.

2.3.2 Cell Physical Identity (PHYID)

The Cell Physical Identity is a physical layer identity of a cell, and is used to scramble the data on physical layer helping the mobile to separate the information from different transmitters. A Physical Identity (PHYID) has a range 0 - 503 and is calculated as Equation (2.1).

$$PHYID = Cell_{NO} + 3 * Group_{NO} \tag{2.1}$$

where $Cell_{NO}$ is the cell number within the group with the range 0 - 2, and $Group_{NO}$ is the group number with the range 0 - 167.

The $Cell_{NO}$ determines the Primary Synchronization Signal (PSS) sequence while the $Group_{NO}$ determines the Secondary Synchronization Signal (SSS) sequence, for detail see [TS3e, Chapter 6.11].

In the experiment work in Chapter 4, the PHYID of the target cells are listed.

2.3.3 E-UTRA Absolute Radio Frequency Channel Number (EARFCN)

The E-UTRA Absolute Radio Frequency Channel Number (EARFCN) designates the carrier frequency in the uplink and downlink and is in the range 0 – 262 143. The relation between EARFCN and the carrier frequency in MHz for the downlink is given by the Equation (2.2). The relation between EARFCN and the carrier frequency in MHz for the uplink is given by the Equation (2.3). The N_{DL} and N_{UL} are the downlink and uplink EARFCN respectively, and F_{DL_low}, NO_{ffs-DL}, F_{UL_low} and NO_{ffs-UL} are given in [TS3d, Table 5.7.3-1, Chapter 5.7.3].

$$F_{DL} = F_{DL\_low} + 0.1 * (N_{DL} - NO_{ffs-DL}) \tag{2.2}$$

$$F_{UL} = F_{UL\_low} + 0.1 * (N_{UL} - NO_{ffs-UL}) \tag{2.3}$$

In the experimental work in Chapter 4, the downlink EARFCN of the concerned cells are given.

2.3.4 LTE Operators in Norway

There are three main LTE operators in Norway - Telenor, Telia and IceNet. The network operator is identified by the Public Land Mobile Network (PLMN), which is constructed of MCC and MNC. For Norway, the MCC is 242. And the MNCs are 01, 02, and 14 for Telenor, Telia and IceNet respectively. The operators are also listed in the Table 2.4.

Table 2.4: LTE operators in Norway

Operator	**MCC**	**MNC**
Telenor	242	01
Telia	242	02
IceNet	242	14

Chapter 3
Related Work

This chapter reviews several published papers related to the paging attack against mobile networks. The attacks presented in the papers can be categorized as passive or active depending on how attack is performed. The attacks can also be differentiated based on where the attack is initiated from, either from the radio interface side or from the Internet side. In addition, there are papers analyzing the impact of paging attack on Paging Channel and network elements. In the end, several published papers proposing the countermeasures are studied.

The reviewed papers are sorted briefly by publication date, and from GSM, UMTS to today's LTE. The concept of paging procedure is kept the same in GSM, UMTS and LTE, and hence the attacks taking advantage of the paging procedure in GSM and UMTS are also valid in LTE. Therefore it makes sense to review the paging attacks performed in GSM and UMTS even though this thesis focuses on LTE.

3.1 Active Attack from Radio Interface on GSM network

N. Golde, K. Redon, and J.P. Seifert, in the paper [GRS13], presented several attacks related to the paging procedure in GSM networks. First, they used a cheap mobile device with baseband software to reply the paging request before the legitimate mobile did, perform an invalid authentication procedure and stop, causing the legitimate mobile not being able to receive the supposed service. Second, they cracked the session key, impersonated the victim mobile and received the data. In the end, they used the attacking mobile to send Detach Request after replying the Paging Request, causing the victim mobile going to the detached state. The victim mobile had to re-attach to gain back network services.

Several weaknesses were taken advantage of in the attacks presented in [GRS13]. First the paging response message is not cryptographically protected in the GSM, so that the attacker can reply the paging request and get accepted by the network. Second the session key in GSM is too short to prevent a brute force attack with today's computer

power, i.e. the attacker can simply test all possible values of the session key and eventually obtain the correct key. Third the network doesn't run the authentication procedure before delivering the MT-service (Mobile Terminating), which can be avoided if the network is reconfigured to run the authentication procedure before service delivery.

3.2 Active Attack Launched from Internet towards 3G Network

Serror, J., Zang, H., Bolot, J.C. of the paper [SZB06] and M. Oğul, S. Baktır of the paper [CKG+11] performed attacks from Internet aiming to increase the paging traffic load. While the authors of [SZB06] focused on the paging channel overload impact, the authors of [CKG+11] focused on the impact of network nodes Radio Network Controller (RNC) and Service GPRS Support Node (SGSN). In both papers, the authors flooded small IP packets from Internet towards the mobile subscribers triggering the paging procedure, then measured the load on paging channel in [SZB06] and RNC/SGSN in [CKG+11] respectively.

The authors of [SZB06] had built a queue model to simulate the paging message queue. The queue model demonstrated that paging channel overload would quickly lead to delay on the legitimate paging message delivery and hence delay call setup. The paper demonstrated the vulnerability but did not suggest any solution.

The authors of [CKG+11] had additionally suggested one solution: to use filtering rules on the network border to filter out the malicious traffic and hence mitigate unnecessary paging traffic.

This kind of attack can be avoided with combination of two measures: 1) Assign the mobile device with a private IP address, which is not addressable from the Internet. 2) Deny initiating traffic from outside on the Network Address Translate (NAT) border. With this approach, the mobile devices are not directly addressable from Internet and the NAT gateway only allows traffic initiated from the mobile, which consequently mitigates the possibility for the attackers to spoof IP packets by just scanning the IP address ranges.

3.3 Privacy and DoS Attack from Radio Interface in LTE

LTE is supposed to be much more secure comparing with GSM and UMTS. However, several papers have been published recently deploying privacy and the DoS attack in LTE from radio interface. Due to open source projects implementing LTE stack, it becomes feasible to perform practical security exploits against LTE.

A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi and J.-P. Seifert, in the paper [SBA+15], presented both passive and active attacks against LTE to track user movement and cause DoS. They built their attacking device with open source software and hardware.

They first presented a passive attack to track the user movement over time via following the S-TMSI and obtain user location information. They set up their attacking device to receive and decode messages broadcasted in the paging channel. Then they made use of social applications, Facebook Messenger and WhatsApp, to trigger silent paging towards the target UE. By monitoring the paging message towards the target, they obtained the coarse location information, i.e. they knew the target was within the tracking area or the cell if the smart paging feature is activated. Once they had obtained the coarse location information, they deployed their attacking device as a fake eNB to capture the Measurement Report and the Radio Link Failure (RLF) report messages. The power level of nearby eNBs and optionally Global Positioning System (GPS) location information are included in these report messages. From the reports, they could obtain the accurate location of the user either with radio trilateration or directly from the GPS coordinators if available.

They could follow the user movement with S-TMSI, as they observed that the S-TMSI did not get updated for several days. This was caused by an improper implementation of the network and could be prevented if the network is configured to update the S-TMSI more often.

Then they performed DoS attacks, to deny either LTE service only or to deny all network services, including LTE, UMTS and GSM, as they chose. They gathered the Tracking Area Code (TAC) and Cell ID information via passively listening to the broadcasted SIBs messages, which contain the TAC and Cell ID. Afterwards they configured their fake eNB with a different TAC from what the legitimate eNB has, set it with a much stronger power level and a higher priority frequency than what the legitimate eNB has. Mobiles detecting the stronger signal over threshold or higher priority frequency would try to attach to the fake eNB and send TAU request because of the different TACs. The TAU request is integrity protected but not encrypted, meaning that the fake eNB could interpret the request message without a valid key. Upon reception of the TAU request, the fake eNB replied with a TAU Reject message indicating LTE service unavailable, which would cause the mobile to use 3G and/or 2G networks, hence the attacker could mount attacks effective in less secure 2G/3G networks. The TAU Reject message might indicate no LTE, 3G nor 2G service available, forcing the mobile to go into the deregistered state and the mobile has to re-attach to gain network access again.

In the end they presented a possible attack for denying selected services, which they did not perform though because there was no baseband software available for an LTE UE, but theoretically it is feasible. When a mobile attaches to the network, it sends an Attach Request to the network. The Attach Request message contains information about mobile's network capabilities, telling which technologies the mobile supports. However, the Attach Request message is not cryptographically protected. With the fake eNB, the attacker could alter the mobile's network capability information and forward the manipulated message further to the network. The network will run AKA procedure to complete the attach procedure, but with the altered capability information.

The DoS attacks succeeded because of weaknesses in the specification itself. The TAU Reject message can be accepted by the UE even when the integrity check fails or without integrity protection, as defined in [TS2b, Clause 4.4.4.2, 3GPP TS24.301]. The last attack with an altered Attach Request message takes advantage of another integrity check exception as defined in [TS2b, Clause 4.4.4.3, 3GPP TS24.301], and there is no confirmation of mobile's network capabilities after the security context has been established. These two attacks can not be prevented unless the specification is amended.

Based on the same protocol exploits as in [SBA+15], R.P. Jover of the paper [Jov16] had implemented an IMSI catcher, passive message sniffer and active DoS attack on LTE, using open source program OpenLTE [For] and low cost hardware. With the same concept, and as described in [MO17], the author of Master Thesis [Sør17] had implemented an IMSI Catcher without much difficulties.

Additionally, the author in [Jov16] discovered an unprecedented method of tracking user via following the C-RNTI of a UE. The C-RNTI is an identifier of RRC connection and scheduling, two bytes long and is unique per device within a cell, see the Table 2.3 for different types of RNTIs. The C-RNTI is in all message header, unencrypted, regardless of control plane or user plane messages. It was observed not being changed as long as the user stayed within the cell. The author had also observed, in the commercial LTE networks in USA, that even at a mobility handover, the allocated C-RNTI from the target eNB could be found in the RRC Connection Reconfiguration message unencrypted. Consequently, it was possible to follow the user from cell to cell via following the C-RNTI.

Although there is no specific guideline on how often the C-RNTI should be updated, the specification - 3GPP TS36.331 [TS3g, Chapter 5.3.5.2] - explicitly specifies that the *mobilityControlInfo* containing C-RNTI for the target eNB should only be included in the RRC Connection Reconfiguration message when the AS security context has been established. If the operator has configured the network strictly

following the specification, the location tracking by following the C-RNTI during handover would be prevented. The operator should configure the network to assign a new C-RNTI whenever a UE goes from Idle to Connected state, to prevent against location tracking via C-RNTI within one cell.

3.4 Countermeasures

To mitigate the privacy and DoS attacks as described in above reviewed papers, there have been published papers proposing countermeasures. The main category of the solutions is to enhance the paging capacity, either by increasing the paging channel capacity or by decreasing the number of paging messages. Another category to enhance the user identity privacy is to encrypt the permanent identity, IMSI, and hence mitigate the IMSI leakage either from the paging or from the initial Attach message. The most novel solution is to not send paging message at all, but to page the user with a user identification tag on the physical layer [PBS08], which not only enhances the user identity privacy but also improve radio channel bandwidth usage. This subclause reviews several published relevant countermeasures.

As it is presented in [SZB06] and [OB13], the paging attack can cause both PCH and network elements such as RNC and SGSN overloaded, which in turn could cause degraded services or even blocked services. In the paper [CKG+11], the authors presented three solutions to overcome the impact of paging and signaling attacks in 3G CDMA. Although it is targeted for 3G CDMA, the concept is valid for the other mobile networks as well.

The three solutions the authors presented are: 1) Randomization of the timer for mobility state changing from Active to Standby and Radio Access Bearer (RAB) inactivity release. 2) Fragmentation of IP address subsets. 3) Paging Channel traffic abnormality detection to detect attacks. The timer randomization would make it much more difficult for an attacker to perform the paging and signaling attack with maximum impact, because the attacker can not trigger paging immediately after the user devices go to standby state when the timer is random. The IP address fragmentation would decrease the impact as the number of affected subscribers becomes less. Through monitoring paging channel traffic pattern over time, the abnormality detection approach would detect potential attacks and notify the operation staff, who can take interventions accordingly. In addition, the authors analyzed the effectiveness of the solutions analytically.

I would argue, however, that the effectiveness of the timer randomization would not be as much as what the authors stated, because the authors seemed to ignore that the starting point of the timer for different users is random. Even though the timer is fixed and the attacker has found out the timer value, it is not possible to trigger the

paging towards all users immediately after they become standby state with certain interval, because not all users would go to standby state simultaneously. Regarding the abnormality detection, it would be much more effective to mount the detection at the network border towards the Internet instead of on the paging channels. The network border is where the malicious traffic originates from, it would much better to monitor the entering point than the destination point. Besides, there is one paging channel per cell, to monitor one paging channel covers only one cell, to monitor the network border covers whole network.

The authors of the paper [CMZC09] introduced an enhancement to the paging record encoding mechanism to decrease user identifier length, which consequently increases the paging channel capacity as it can send more paging messages. Although the paper targeted at CDMA2000, the concept can be adopted to the other mobile networks. Briefly, the idea is to use a locally unique identifier instead of a globally unique identifier, and hence requires much shorter identifier length. The authors proposed *"series of methods for shortening terminal IDs by leveraging the knowledge of the population size in a paging area, by grouping terminals based on paging channel slots, and by using special Bloom filters in quick paging."*, [CMZC09, Introduction, P.2]. Applying the approaches in CDMA2000, the user identifier length can be shortened from 34 bits to 7 bits. Since the header and tailer are kept unchanged, the total paging message length decreases from 58 to 31 bits, and effectively doubles the paging channel capacity.

One uncertainty about the solution is how the locally unique identifier is maintained. In the paper, the authors mentioned *Paging Controller* to maintain the user identifier, without further clarification. In mobile networks, the network element with mobility management function maintains the user identifier for paging, for example the Mobile Switching Center (MSC)/Visiting Location Register (VLR) in GSM, the MME in LTE. The authors did not explain where the *Paging Controller* would locate in CDMA2000 architecture, and how it would work together with other network elements. From the description, most logically the *Paging Controller* is part of MSC/VLR functionality. But then it requires that the MSC/VLR has the knowledge of the paging channel slot of a user, which normally is only radio network knowledge. It means that the solution requires the radio network somehow to send the information to the MSC/VLR. Another approach is to put the *Paging Controller* functionality in the Base Station Controller (BSC). The MSC/VLR sends the paging message to a BSC using the globally unique user identifier, and the BSC replaces the globally unique identifier with the locally unique identifier and forwards the paging message on the radio interface. No matter which alternative the authors intended to, the paper would have become more complete if the authors had provided more information about the *Paging Controller*.

To increase the paging capacity, the authors of the paper [ZB07] went for another approach, i.e. to decrease the number of paged cells based on user mobility profiles. They collected mobility and service data from a commercial CDMA2000 network for whole February 2006 in two cities in USA. Based on the collected data, they developed static and dynamic mobility profiles used for paging. Afterwards they evaluated the paging performances - paging delay, paging success rate and amount of paging signaling messages - if the paging profile would have been deployed. The success rate would be on average above 90% for one city and 85% for the other. The amount of paging signaling messages would decrease by 85% or 90%, at a cost of a slightly longer paging delay. The authors introduced a *smart paging* concept, which means only the latest visited N cells being paged for data calls. It could further decrease the number of paged cells with cost of the paging delay. Maybe this is the origin of the 'Smart Paging' feature used in LTE today. Interestingly, the paging success rate for data calls was much better than that of text messages and voice calls, which makes the approach very suitable for data-centric LTE.

In LTE, the usage of the GUTI has minimized the exposure of the permanent identity, IMSI, but it does not exclude the IMSI usage completely. In the initial Attach Request, the IMSI is used. Some IMSI catchers collect IMSI by catching the Attach Request message. Sometimes the IMSI is used as user identity in the paging message, which causes the IMSI to be leaked to an eavesdropper. To mitigate these weaknesses, the authors of the paper [JNNN17] suggested several enhancements. To avoid the IMSI exposure in the initial Attach Request message, they suggested to use encrypted IMSI. Then they evaluated that the extra computation overhead of the en-/decryption does not degrade the service performance noticeably for the user. To mitigate the exposure of the IMSI in the paging message, they suggested two variants: 1) Use a short-term pseudonym, which is assigned by the HSS during the AKA and sent to MME. 2) Use the encrypted IMSI from the previous Attach. Either way, it avoids the IMSI being sent as clear in the paging message. Another weakness in the LTE is that some bits of the IMSI get revealed by the UE Identity Index *(IMSI mod 1024)*. To overcome this weakness, they suggested to compute the UE Identity Index using the pseudonym for the first variant and the encrypted IMSI for the second variant. In this way the UE Identity Index varies over time as both the pseudonym and the encrypted IMSI are short-term numbers and hence no information of the IMSI is revealed. The last enhancement they suggested is to use a freshly encrypted IMSI to reply the paging with IMSI, and hence to avoid the correlation between the paging and the paging response. For the IMSI ciphering, they suggested to use the Elliptic Curve Integrated Encryption Scheme (ECIES) without MAC (denoted as ECIES*) algorithm, which requires a public ephemeral key. The enhancements they suggested require additional computation for encryption and decryption, and bandwidth for sending the public ephemeral key, but they evaluated that it is acceptable.

Their suggestions indeed have prevented the IMSI exposure in the initial Attach Request and Paging messages. There is one missing scenario though, namely the Identity Response to the Identity Request where the IMSI is requested. Actually the author of [Sør17] took advantage of this scenario and successfully built an IMSI catcher. The IMSI is obtained by sending the Identity Request asking for the IMSI. Their suggestion can be extended to send the encrypted IMSI in the Identity Response as well if no other constraints which do not allow it. In fact, their suggestion of encrypted IMSI including this extension part is adopted in the 5G specification to avoid the permanent identity revealing [TS3c, Chapter 6.12].

The most novel solution so far would be the solution proposed by the authors in the paper [TB13]. Instead of focusing on the higher signaling layer as in the other approaches, the authors went down to the physical layer. With physical layer identification, their idea was *"to embed users' unique tags onto the downlink paging signal waveforms so that the tags are stealthy and robust"* [TB13, Abstract]. They proposed to use the user's unique temporary ID as an input to generate a unique tag for that user, and superimpose the tag onto the Physical Downlink Control Channel (PDCCH) waveform with so low power level that it can only be detected but not be decoded. In case several UEs are paged simultaneously, the tags for the different users should be uncorrelated. The UE detecting its tag knows it is paged and does not need to check the paging record in the Physical Downlink Shared Channel (PDSCH). Without degrading the current PDCCH signal quality, they approved that the detection success rate reached 99%, with simultaneous four tags. This approach does require additional signaling processing to embed the tag on the eNB and to detect the tag on the UE, with benefit of enhanced privacy protection and the bandwidth used for the paging records in the PDSCH can be freed.

The physical layer tag embedding solution looks very promising if it could realize the results as it is described. If the approach had been deployed on LTE, all attacks relying on listening to the paging message would have become infeasible because of no more meaningful paging messages to listen to.

3.5 Summary

This section reviews several relevant published papers, both attacks and countermeasures. Among the published countermeasures, the most novel one is to use physical layer identification tag to prevent against user identity leakage. The one with an encrypted IMSI in the Attach, and pseudonym or encrypted IMSI in the Paging looks promising as well. It is interesting to see if the suggested solutions would be deployed in LTE systems or the coming 5G network. In fact, the solution of encrypted IMSI presented in the paper [JNNN17] is adopted in the 5G specification to avoid the permanent identity disclosure [TS3c, Chapter 6.12].

Chapter 4
Experimental Work

The goal of the experiments presented in this chapter is to explore how well Norwegian operators implement their LTE networks in respect of protection of user privacy and against location tracking with focus on the paging procedure. In addition, a paging response feeder is experimented with the goal of verifying if it is feasible to feed in paging response impersonating a legitimate user in LTE and the possible consequence.

4.1 Ethics/Privacy Concerns

The paging message catcher is a passive message sniffer for a cell of the commercial network which covers the lab area. It does not send any message nor affect any services. For the paging response feeding lab, the author's own subscription is used and it does not disturb the service for any other users. In addition, the experiments are performed in research and educational scope only. Besides, all sensitive information in the illustration examples is masked out.

4.2 Tools

For LTE functionalities, the experiments use the *srsLTE* open source software, which is developed by Software Radio Systems (SRS) [SRSa]. The *srsLTE* is compliant with LTE Release 8, implements the LTE stacks for eNB, Evolved Packet Core (EPC), UE and contains several example applications [SRSb]. In the experiments, the broadcast message catcher uses two example applications: one for cell searching, *cell_search*, and one for broadcast message sniffer, *pdsch_ue*. The paging response feeder uses the UE stack application *srsUE*.

The radio interface hardware uses USRP B200Mini, which has a USB3.0 interface connecting with a host streaming data. It supports frequency range from 70 MHz - 6 GHz [Ett].

A widely used network protocol analyzer, *Wireshark*, is used to decode and analyze the captured LTE messages [Wir].

The main used software and hardware are listed below:

- Desktop computer, Dell OptiPlex 7040
  - Memory - 32 GiB
  - Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz x 4
  - Graphics - Gallium 0.4 on NV117
- Ubuntu 14.04 LTS, 3.19.0-031900-Low latency kernel
- srsLTE
  - cell_search
  - pdsch_ue
  - srsUE
- Wireshark
- USRP B200mini, 70 MHz - 6 GHz frequency range, full duplex and USB 3.0 bus-powered

In addition, there are several dependent software for srsLTE to work properly, which can be found from the GitHub srsLTE master branch [Git]. Follow the instructions there to install the srsLTE and its dependent software. For reference, one article from ShareTechNote also provides detailed installation instruction for srsLTE and the required prerequisites [Sha].

4.3 Paging Message Analysis for Norwegian PLMN

4.3.1 Experiment Setup

The experiment topology is illustrated in Figure 4.1. The host runs Ubuntu Linux v14.04 Low Latency Kernel, and srsLTE example applications *pdsch_ue* and *cell_search*. The application *cell_search* scans the cells covering the lab area, and *pdsch_ue* captures the broadcast messages. The radio interface is emulated by USRP B200mini. The USRP B200mini connects with the host on a USB3.0 port using the USB cable.

The main steps to capture the paging message and decode it are described in the following subclauses.

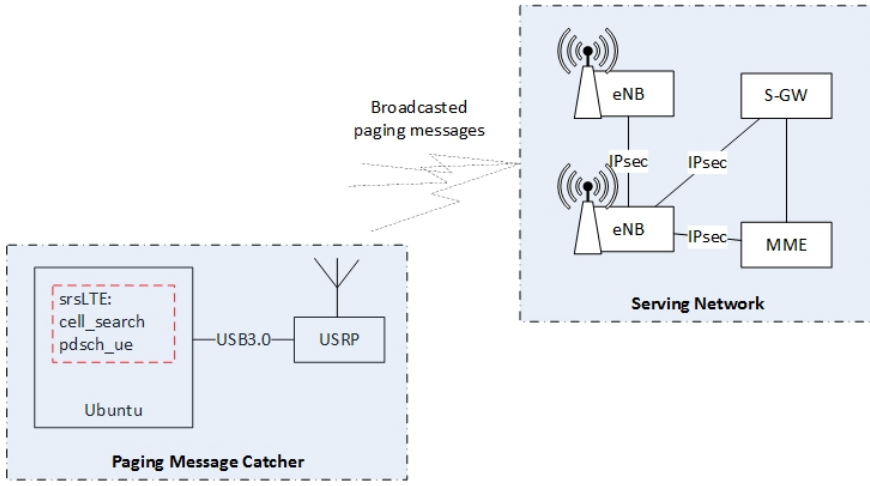

Figure 4.1: Paging Message Catcher Topology

1. **Find the frequency band for the cells covering the target area**

   The used frequency band for each cell can be found from FinnSender [NKOa]. Figure 4.2 shows the map of Gløshauge campus with locations of cell transmitters. On the web page, place the mouse on the cell transmitter icon, the

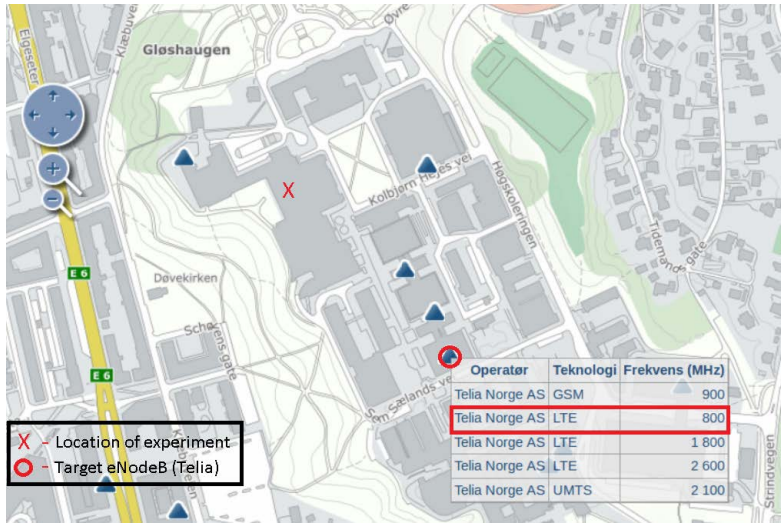

Figure 4.2: Overview of the neighboring LTE eNodeBs to the experiment location. The red "X" represents the location of the experiment, and the red "O" represents the location of the target cell [Sør17, Figure 4.5].

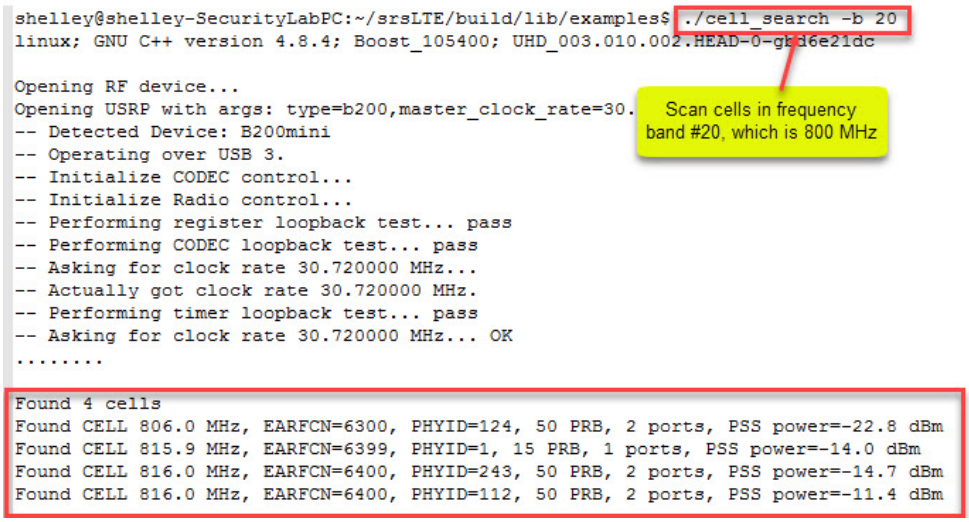

Figure 4.3: Screenshot of *cell_search* result, running in the security lab at NTNU E-Building

information window will appear showing the operator name, technology and frequency band for that cell, as illustrated in the Figure 4.2.

2. **Obtain the precise frequency of the target cells**

   The example application *cell_search* of srsLTE is used to acquire the information. Figure 4.3 is a screenshot of the searching result on the frequency band number 20, which is the 800 MHz frequency band. As shown in the figure, four cells are found within the radio band number 20, the exact downlink frequency, the downlink EARFCN and the cell PHYID are displayed.

3. **Find out which operator the target cell belongs to**

   Since the same frequency band is used by different PLMNs but at different frequency, it needs to find out which PLMN the cell belongs to. The SIB1 contains the information, and it is broadcasted in the Broadcast Channel with RNTI value 0xffff. To capture the SIB1 message, the example application *psdch_ue* of srsLTE is used. Figure 4.4 shows an example of one captured SIB1, which is decoded with an online tool "Marben LTE ASN.1 Deoder" [Mar]. As the figure shows, the cell in the example with Physical ID 124 at the downlink frequency 806 MHz belongs to Telia Norway.

   After repeating the steps 2 and 3 several times, several cells are detected. The detected cells are listed in the Table 4.1. The table lists the cell PHYID, downlink EARFCN, downlink frequency, and the operator.

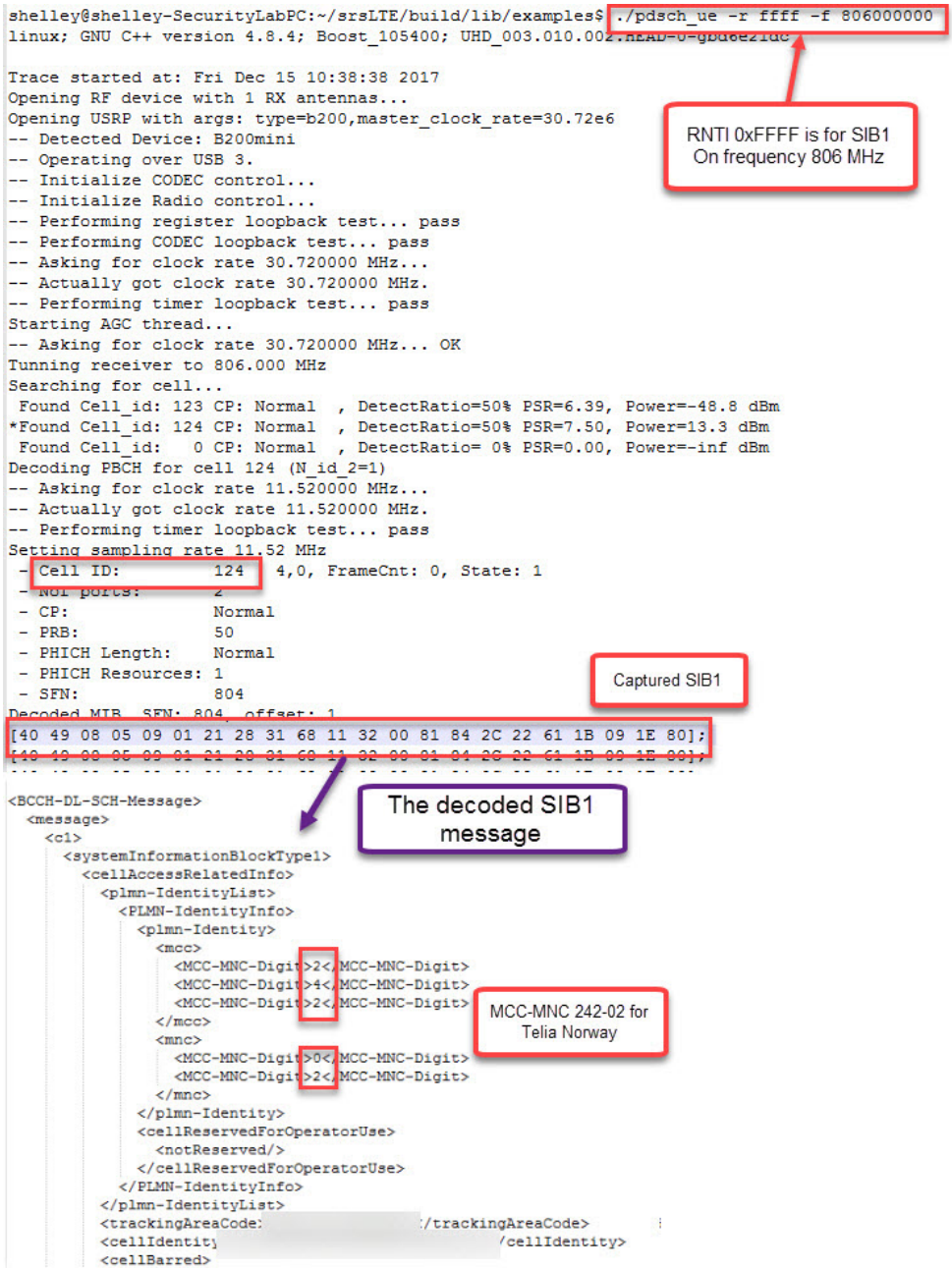

Figure 4.4: Example of one captured SIB1 message. Among all information, the MCC and the MNC are included in the SIB1.

Table 4.1: List of cells covering the security lab, which is located at NTNU E-building.

PLMN	**Cell PHYID**	**Downlink EARFCN**	**Downlink Frequency**
Telia	123	6300	806 MHz
	124	6300	806 MHz
	124	1650	1850 MHz
Telenor	112	6400	816 MHz
	243	6400	816 MHz
	298	1450	1830 MHz
IceNet	78	6200	796 MHz

4. **Capture paging messages**

   After finding out the cell ID and the precise frequency, the example application *psdch_ue* of srsLTE is used to capture the paging messages. Figure 4.5 shows the capture of several paging messages.

```
Tunning receiver to 806.000 MHz
Searching for cell...
 Found Cell_id: 123 CP: Normal  , DetectRatio=100% PSR=7.54, Power=-45.5 dBm
*Found Cell_id: 124 CP: Normal  , DetectRatio=83% PSR=9.26, Power=13.0 dBm
 Found Cell_id:   0 CP: Normal  , DetectRatio= 0% PSR=0.00, Power=-inf dBm
Decoding PBCH for cell 124 (N_id_2=1)
-- Asking for clock rate 11.520000 MHz...
-- Actually got clock rate 11.520000 MHz.
-- Performing timer loopback test... pass
Setting sampling rate 11.52 MHz
Finding PSS... Peak:      1,3, FrameCnt: 0, State: 0
Finding PSS... Peak:      1,1, FrameCnt: 0, State: 0
Finding PSS... Peak:      1,1, FrameCnt: 0, State: 0
Finding PSS... Peak:      4,0, FrameCnt: 0, State: 1
 - Cell ID:         124
 - Nof ports:       2
 - CP:              Normal
 - PRB:             50
 - PHICH Length:    Normal
 - PHICH Resources: 1
 - SFN:             380
Decoded MIB. SFN: 380, offset: 3
Captured at: Thu Jan 18 15:33:05 2018
[40 03 8E 07 9B A3 20 00 00];
Captured at: Thu Jan 18 15:33:05 2018
[40 04 0F 3A 49 37 C0 00 00];
Captured at: Thu Jan 18 15:33:05 2018
[40 04 0F 46 C4 BF 50 00 00];
```

One example of captured paging

Figure 4.5: Example of several captured paging messages

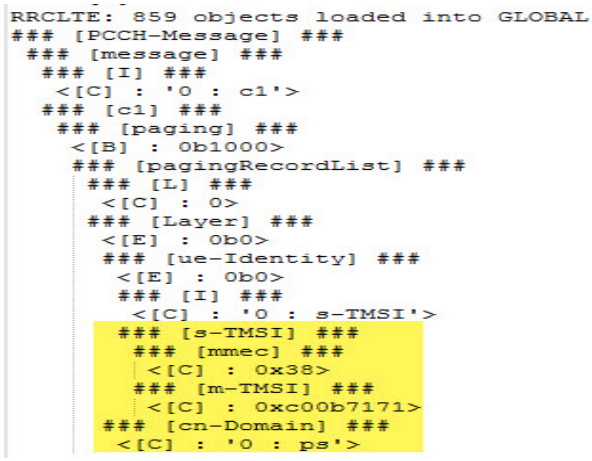

Figure 4.6: Example of one decoded paging message using the Python script

The original source code does not print out the captured data and timestamp. To do it, the source code has been changed, as shown in Appendix B.

5. **Decode the captured paging message**

   To decode the paging message, the code from [Sør17] is used. It is written in Python and is attached in Appendix A. Figure 4.6 shows one example of a decoded paging message. As it shows, the S-TMSI is used as the UE identity in this example.

4.3.2 Paging Message Analysis

In the thesis work of [Sør17], it was observed that the amount of paging messages of Telia is significantly less than that of Telenor, which could not be explained. This leads to this experimental work to figure out the reason behind.

For Telia, the same frequency is selected as what my mobile uses at the moment of experiment, which is 806 MHz. For Telenor and IceNet, the frequency in the same frequency band as Telia's is selected, which is 816 MHz and 796 MHz respectively. The sniffed cell is selected automatically by the sniffing application at the specific frequency. When there are two cells with the same frequency covering the lab area, the cell with the stronger signal strength is selected.

The captured paging messages are decoded, then the paging records and notifications contained in the paging messages are counted. The amount presented in the result is the number of paging records or notifications. One paging message can contain up to 16 paging records besides other notifications, such as ETWS, CMAS and so on

Table 4.2: Number of paging records, captured within one hour at different times of a week

PLMN	**Cell PHYID and Frequency**	**Time**	**No. of Paging Records**	**No. of systemModification**
Telia	124 806.0 MHz	15.Jan.2018, Mon 09:49:35 - 10:49:35	27 138	-
		18.Jan.2018, Thu 15:32:59 - 16:32:50	23 485	-
		19.Jan.2018, Fri 08:54:34 - 09:54:34	26 332	-
Telenor	112 816.0 MHz	15.Jan.2018, Mon 08:43:19 - 09:43:19	65 058	-
		18.Jan.2018, Thu 16:54:32 - 17:54:32	43 642	-
		19.Jan.2018, Fri 10:22:45 - 11:22:45	72 743	115
ICE Net	78 796.0 MHz	26.Apr.2018, Thu 11:00:00 - 11:59:59	2 356	-
		27.Apr.2018, Fri 08:35:00 - 09:34:59	2 205	-
		30.Apr.2018, Mon 08:13:00 - 09:12:59	1 840	- -

[TS3g]. During the experiments, the observed longest paging message contains five paging records.

4.3.3 Result and Discussion

Table 4.2 lists the number of paging records and notifications for the three LTEs in Norway, within one cell for a period of one hour. The table lists the time when the paging messages are captured, the cell PHYID, the cell downlink frequency, and the number of paging records and notifications.

In order to get a representative picture, the capturing has been done three times at different times of a week. As the Table 4.2 shows, the amount of paging records for Telia in one cell for one hour, is around 25 thousands, which is about seven

paging records per second. For Telenor, the amount is about 70 thousands, which is about 20 paging records per second, although for one occasion it is much less as the capturing time extends out of the office hour. For IceNet, the amount of paging records is around two thousands for a whole hour, which is very small comparing with the other two operators. One reason is that IceNet has much less subscribers, the other is that IceNet might share LTE network with other operators.

Expectedly, there is no paging message with indication of CMAS or ETWS. Telenor has 115 systemModification messages during one observation period, indicating some changes of the system information. Of all captured paging messages for all three operators, none of them has IMSI as the user identity, which proves that paging with IMSI is a very seldom case.

In contrast to the result from the thesis work of [Sør17, Table 4.3], the amount of paging records from Telia is actually in proportion of the number of subscribers in comparison with which of Telenor [NKOb]. The sniffed cell in [Sør17] was the cell with PHYID 123, while it is the cell with PHYID 124 in my experiment. In the smart paging verification experiment in the Chapter 4.4, the paging messages from cell 123 are also captured, and the result is shown in the Table 4.3. The amount is 3 713, which is on the same level as the result from [Sør17, Table 4.3] with amount 2 770. Based on the amount of paging records, the cell 123 seems to be a sort of backup or extension of neighbor cells.

4.4 Smart Paging Verification

This experiment is to verify if the smart paging feature is implemented in Norwegian LTE networks. With smart paging, the network pages a UE only in the latest observed active cell or few neighbor cells, instead of the whole TA [Nok]. This leads to that the location tracking becomes much more accurate, because it means a paged user is within the coverage area of one cell, typically of two km^2, instead of the whole TA which is typically 100 km^2 [SBA+15]. Although it is not completely certain that a paged user is indeed in the area without knowing if the user has replied the paging, the probability is very high.

4.4.1 Experiment Setup

In order to verify the smart paging feature, it requires to catch paging messages from at least two cells within same TA in parallel and compare the captured paging records from each cell. Without smart paging, the two sets of paging records should be identical since the paging is supposed to be sent to whole TA. With smart paging, most of the two sets of paging records should be different from each other, since the paging is sent only to the latest observed active cell. To achieve this, two paging

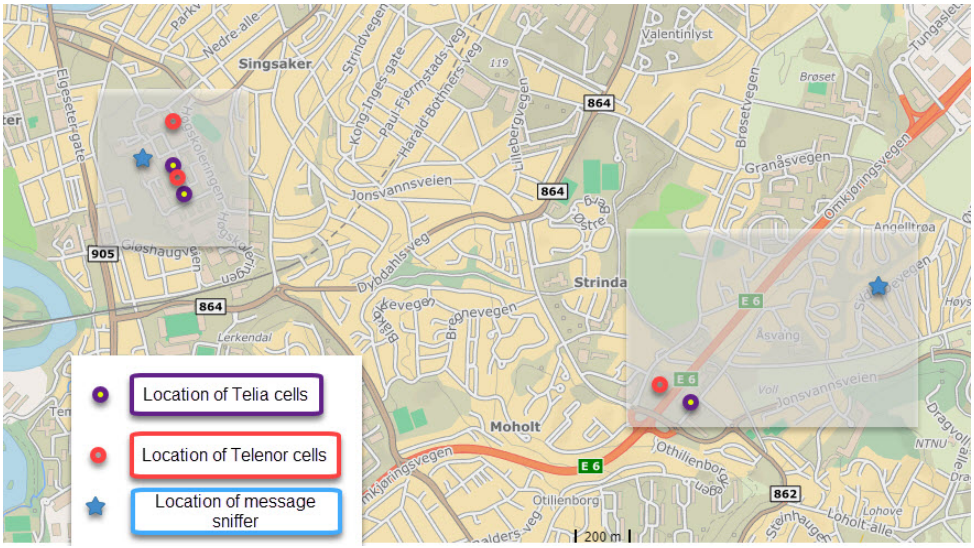

Figure 4.7: Locations of cell transmitter and lab sniffing equipment

message sniffers are set up to capture the paging messages from two cells in parallel with a minimum time period of 30 minutes. First, paging messages from two neighbor cells are captured and analyzed. Second, paging messages from two cells with about 2.2 kilometers distance but still within same TA are captured and analyzed.

The frequency and cells are selected with same principle as in the Chapter 4.3.2. As the capturing has been done at different times, the sniffed cells in this experiment might not be the same as those in the Chapter 4.3.2.

The locations of the cell transmitter and sniffing equipment are shown in Figure 4.7. The two neighbor cells are both located in NTNU Gløshaugen campus. The two cells with some distance, one is located in NTNU Gløshaugen campus and the other is located at Moholt East beside the Omkjøringsveien.

As described in the Chapter 4.3.1, the source code is updated to timestamp the captured paging messages. The captured paging messages with timestamp are decoded, then the user identities contained in the paging messages are extracted. By comparing the user identities and the timestamp, we get to know if the paging towards same target is broadcasted to both cells at the same time.

4.4.2 Result and Discussion

Table 4.3 and Table 4.4 show the result for Telia and Telenor respectively. Each table contains the total number of paging records in each cell, and the number of

paging records which are towards same target and are broadcasted in both cells simultaneously.

The experiment result is based on the assumption that the same S-TMSI is for the same UE during the capturing period. As the result shows, there are small amount of paging records which are towards same target and are broadcasted in the neighbor cells at the same time. But no paging record towards the same target is broadcasted at the same time in the cells away from each other but still within the same TA. Based on the result, it is proven that the smart paging feature is implemented in both Telia's and Telenor's LTE. Since the smart paging feature is deployed, a paged user can be located within the coverage of one cell, which is much smaller than a whole TA.

Besides the smart paging feature verification, there are several interesting observations from the paging messages captured in the neighbor cells.

1. Noticeably, the amount of paging records for one cell is significantly less than that of the other cell for both Telia and Telenor, which gives a hint that one cell is a sort of extension or backup of the other cell.
2. Paging messages towards some targets are first sent to one cell only, and later to both cells. This implies that no response is received from the first cell in the beginning and hence the paging is broadcasted in both cells trying to reach the target.
3. Paging messages towards some targets are captured in one cell, then paging messages towards the same targets are captured in the other cell later. This scenario indicates that the UE moves from one cell to the other.

Table 4.3: Number of paging records from different cells, captured within the time frame, for Telia Norway.

Telia		
Cell	**Two Neighbor Cells**	
	Cell 124 (806 MHz)	**Cell 123 (806 MHz)**
Time Range	20.01.2018 10:37:25 - 11:19:30	20.01.2018 10:38:57 - 11:19:24
Number of paging records	16 648	3 713
Number of paging records broadcasted in both cells at the same time	2 811	
Cell	**Two Cells with about 2 KM distance but within the same TA**	
	Cell 124 (806 MHz)	**Cell 280 (806 MHz)**
Time Range	27.01.2018 19:37:00 - 20:37:59	27.01.2018 19:37:00 - 20:37:59
Number of paging records	33 675	33 946
Number of paging records broadcasted in both cells at the same time	0	

Table 4.4: Number of paging records from different cells, captured within the time frame, for Telenor Norway

Telenor		
Cell	**Two Neighbor Cells**	
	Cell 112 (816 MHz)	**Cell 298 (1 830 MHz)**
Time Range	19.01.2018 15:32:26 - 16:09:19	19.01.2018 15:29:58 - 16:07:29
Number of paging records	22 752	8 259
Number of paging records broadcasted in both cells at the same time	1 078	
Cell	**Two Cells with about 2 KM distance but within the same TA**	
	Cell 243 (816 MHz)	**Cell 106 (816 MHz)**
Time Range	27.01.2018 16:15:00 - 17:15:59	27.01.2018 16:15:00 - 17:15:59
Number of paging records	77 318	39 935
Number of paging records broadcasted in both cells at the same time	0	

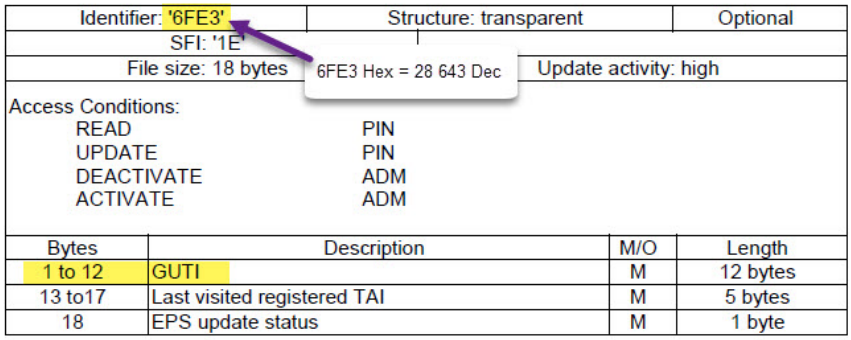

Figure 4.8: EPS Location Information encoding in USIM field [TS3a, Chapter 4.2.91].

4.5 M-TMSI Refreshment Analysis

The M-TMSI is a short-term identity and is supposed to be renewed often enough to avoid traceability of the UE. This experiment verifies how often the M-TMSI is updated and what event triggers the update. In the experiment, my own subscription, from Telia Norway, with iPhone7 is used.

The EPS Location Information is saved in the USIM field with the identifier value 6FE3 in hexadecimal and 28 643 in decimal [TS3a, 3GPP TS31.102]. The EPS Location Information contains the GUTI, the last visited registered TAI and the EPS update status. The encoding of EPS Location information is shown in Figure 4.8. As it shows, the first 12 bytes represent the GUTI, of which the last four bytes represent the M-TMSI.

For iPhone7, the EPS location information can be read from the iPhone 'Field Test Mode' by dialing *3001#12345#*, as illustrated in the Figure 4.9. The value of the identifier in iPhone is in decimal. As shown in the figure, the M-TMSI can be directly read there.

By reading the M-TMSI before and after an applied event, it is easy to find out if the event triggers M-TMSI update. In LTE, the M-TMSI gets updated with an EPS Mobility Management (EMM) procedure - GUTI Reallocation [TS2b, 3GPP TS24.301, Chapter 5.4.1].

4.5.1 Periodic Tacking Area Update

In LTE, the timer T3412 decides the periodic TAU frequency, with a default value of 54 minutes [TS2b, 3GPP TS24.301, Chapter 10.2]. However, the network can set it at a different value or deactivate it completely. Typically, the GUTI Reallocation

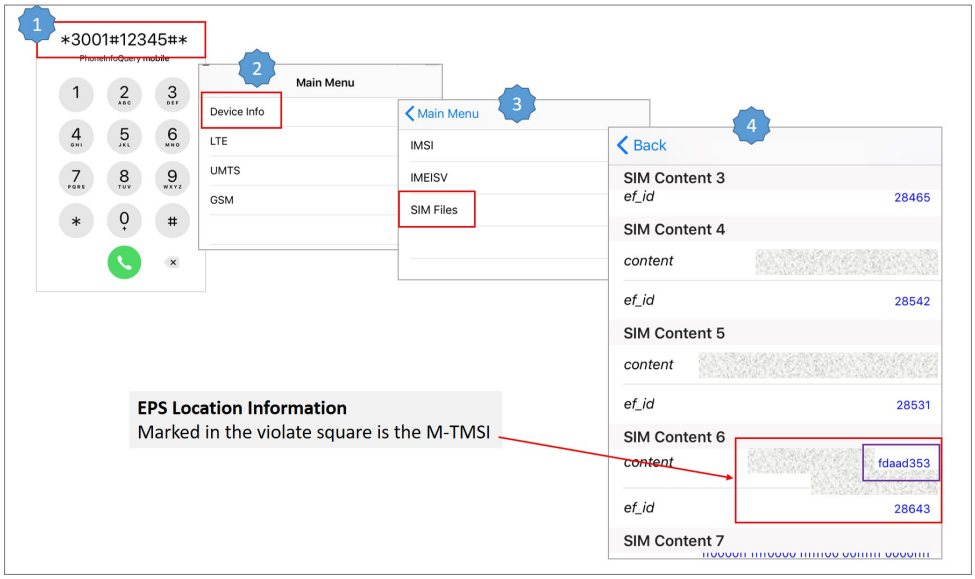

Figure 4.9: Read EPS Location Information from USIM with iPhone 7

procedure runs together with the periodic TAU, and hence the M-TMSI gets renewed, which is the reason that the periodic TAU timer is of our interest.

In order to check the periodic TAU timer, the UE needs to stay at EMM-IDLE state. To keep the mobile staying in EMM-IDLE state without sending or receiving data, mobile-data is turned on in the mobile but is disabled for all applications, so that the applications would not initiate any data traffic in the background.

4.5.2 Result and Discussion

Table 4.5 lists the verified events and if they trigger M-TMSI update in the LTE of Telia Norway. As expected, switching the mobile off then on, and turning the flight mode on then off trigger the M-TMSI update, because the mobile needs to re-attach to the network. Both Mobile Originating (MO)- and Mobile Terminating (MT) voice call triggers M-TMSI reallocation as well. The TAU when a mobile comes into a different TA also triggers M-TMSI update.

From the observation result regarding the periodic TAU, there are two scenarios to explain it. 1) If Telia's LTE indeed refreshes the M-TMSI in connection to the periodic TAU, then the periodic timer must be longer than 48 hours and 28 minutes. 2) Telia's LTE has deactivated periodic TAU or does not refresh the M-TMSI in connection to it. Whichever the scenario is, it is not a good practice to keep the M-TMSI not updated for more than 48 hours.

Table 4.5: List of verified events and if they trigger M-TMSI update in Telia's LTE

Event	**M-TMSI Refreshed? (Y:Yes; N:No)**	**Comment**
Mobile switch off/on	Y	
Mobile Flight Mode on/off	Y	
Mobile Originating Call (MOC)	Y	
Mobile Terminating Call (MTC)	Y	
Mobile Originating Short Message (MO-SM)	N	
Mobile Terminating Short Message (MT-SM)	N	
Mobile Originating Data (MO-Data)	N	
Mobile Terminating Data (MT-Data)	N	
Periodic TAU	-	Uncertain. Observed longest time without M-TMSI refreshment is 48 hour 28 minutes, until an incoming call (MTC). See the text for more information.
TAU	Y	TMSI gets updated when moving between TAs with TAC 2305 in Trondheim and 2307 in Hommelvik

The authors of the paper [SBA+15] performed location tracking attack by following the GUTI because the GUTI was observed kept the same for several days. The same kind of attack can be applied here, i.e. to track a user by just following the M-TMSI.

4.6 Paging Response Feeding

As described in the Chapter 3.1, the authors of [GRS13] built an attacking device to reply the paging request, cracked the session key, and received the service impersonating the victim in GSM. Inspired by their attacks, this experiment is attempted with these intentions: 1) To verify if the open source software UE can establish

communication with the commercial LTE and manage to send in the paging response masquerading as the victim; 2) To verify how the commercial LTE would handle the duplicate paging responses; 3) To verify what consequence it might cause by the duplicate paging responses. Unlike the attacks in [GRS13], this experiment does not aim at cracking the session keys, nor trying to receive the service on behalf of the victim.

Typically, a paged UE sends the Service Request message to the network as paging response. As described in the Chapter 2.2.3, the Service Request is integrity protected. If the integrity verification fails, the network will reject the request by sending the Service Reject message with cause #9 ("UE identity can not be derived by the network") to the UE. The UE receiving the Service Reject with cause #9 will go to Deregistered state and will normally initiate the Attach procedure to re-gain network access [TS2b, Chapter 5.6.1.5]. Sometimes it might require user interaction if the UE can not manage to re-gain network access automatically.

In this experiment, the Service Request fed by the attacking device is supposed to fail the integrity verification. So in best case, the paging response feeder could cause the target victim loosing network access until manual interaction.

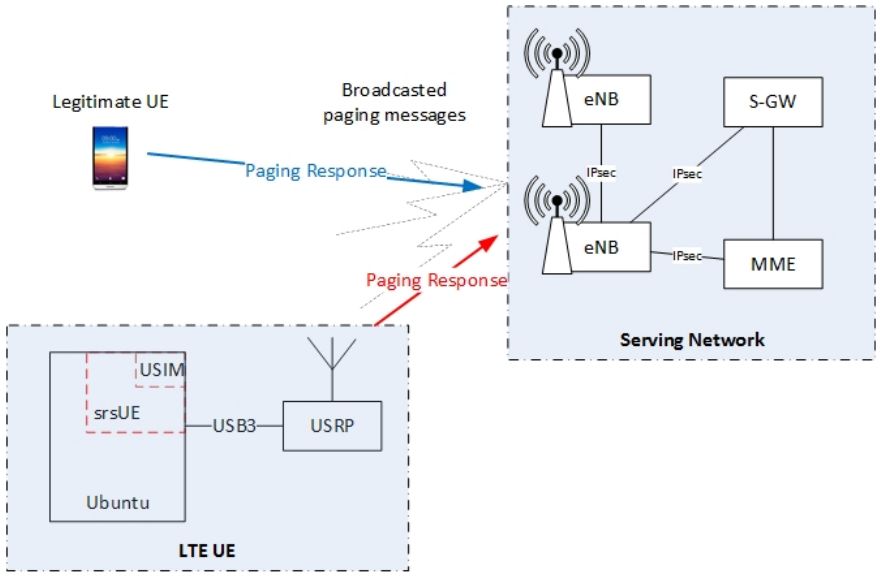

Figure 4.10: Experiment setup topology for paging response feeder

4.6.1 Experiment Setup

For this experiment, the software UE *srsUE* application from *srsLTE* is used. The hardware is the same as in the previous experiment, with the USRP B200mini as the radio interface. Figure 4.10 illustrates the lab setup topology.

The functionality of *srsUE* is illustrated in the Figure 4.11. The source code is modular and well organized to implement each functionality block. This makes it easy and convenient to change the source code for a specific purpose. However there are flaws in the source code which need to be fixed if needed. Whenever the source code is changed in the experiment, it is specified. The source code in this experiment

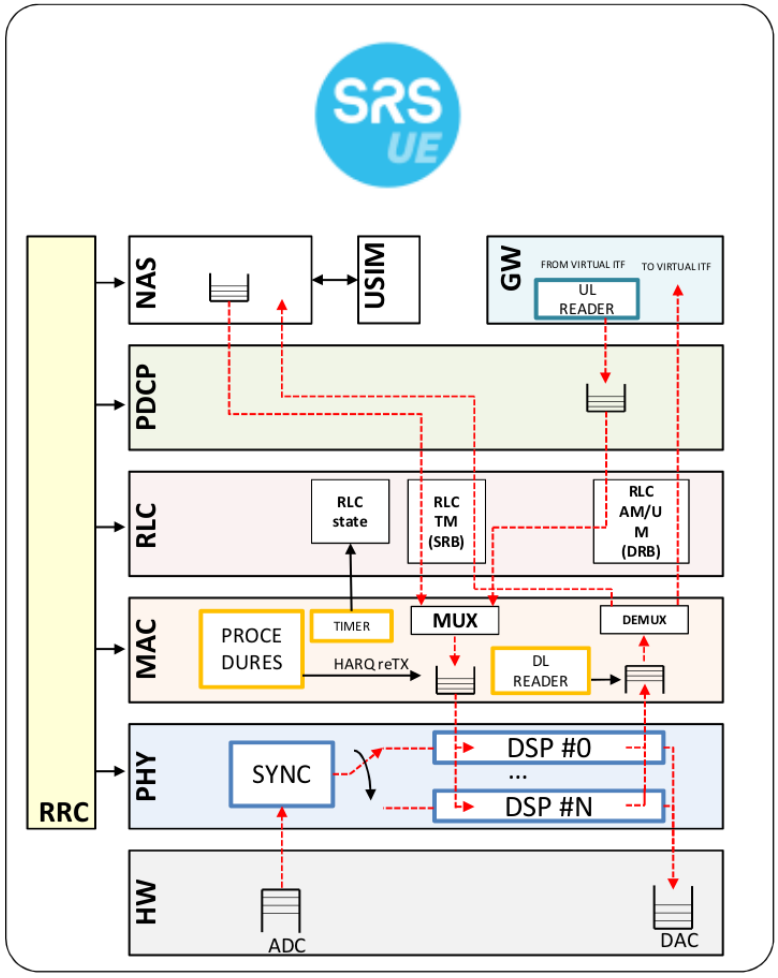

Figure 4.11: The *srsUE* application functionality block [SRSc].

Code 4.1: Set S-TMSI in the source code

```
nas::nas()
  // have_guti is changed from original 'false' to 'true'
  : state(EMM_STATE_DEREGISTERED), plmn_selection(PLMN_SELECTED),
      ↪ have_guti(true), have_ctxt(false), ip_addr(0), eps_bearer_id
      ↪ (0)
...
bool nas::get_s_tmsi(LIBLTE_RRC_S_TMSI_STRUCT *s_tmsi) {
  if (have_guti) {
    // The original code commented out
    // s_tmsi->mmec = ctxt.guti.mme_code;
    // s_tmsi->m_tmsi = ctxt.guti.m_tmsi;
    s_tmsi->mmec = 0x40; // MME code
    // M-TMSI of my mobile at the time of experiment
    s_tmsi->m_tmsi = 0xfb5dd3fc;
    return true;
  } else {
    return false;
  }
}
```

is downloaded from GitHub [Git] on 17/Mar/2018.

The experiment approach is to set the S-TMSI same as my mobile in advance for the *srsUE*, let it run and listen to the paging messages. Once it detects a paging message towards the S-TMSI, it will attempt to reply the paging request via sending a NAS Service Request to the MME after it has established RRC connection with the eNB. To achieve this, the source code for the NAS functionality (*nas.cc*) is updated as shown in the Code 4.1 to hard code the S-TMSI.

The *srsUE* application requires a configuration file as well, which contains many configurable parameters. The complete configuration file with default parameters is attached in Appendix C. For this experiment, the IMSI, the IMEI, the downlink EARFCN, and traces are configured accordingly, as listed in the Code 4.2.

In the source code for RRC functionality (*rrc.cc*), the Cause for RRC-Connection-Request has only 'MO_SIGNALING', which is meant for MO activities. For the purpose of paging response, this is changed to 'MT_ACESS'. The changed code is shown in the Code 4.3.

Code 4.2: srsUE Configuration

```
...
// Set the downlink EARFCN same as the target cell
dl_earfcn = 6300
...
[pcap] // To enable the packet capture
enable = true
filename = /home/shelley/Trace4Lab2/20180320/ue.pcap
nas_enable = true
nas_filename = /home/shelley/Trace4Lab2/20180320/nas.pcap
...
[log] // To enable logging and set logging level
all_level = debug
phy_lib_level = none
all_hex_limit = 32
filename = /home/shelley/Trace4Lab2/20180320/ue.log
file_max_size = -1
...
[usim]
...
// Set a dummy IMSI with Telia as home PLMN
imsi = 24202xxxxxxxxxx
imei = 35533xxxxxxxxxx // Set IMEI same as my mobile's
```

Code 4.3: RRC Connection Cause changed to 'MT_ACCESS'

```
void rrc::send_con_request() {
...
// Original code, MO-signaling only
  // ul_ccch_msg.msg.rrc_con_req.cause =
      ↪ LIBLTE_RRC_CON_REQ_EST_CAUSE_MO_SIGNALLING;
  // Changed to MT_ACCESS for paging response
    ul_ccch_msg.msg.rrc_con_req.cause =
        ↪ LIBLTE_RRC_CON_REQ_EST_CAUSE_MT_ACCESS;
  send_ul_ccch_msg();
}
```

4.6.2 Scenario Analysis

There is a race condition here, i.e. which paging response would reach the network first, the one from the legitimate UE or the one from the attacker, as illustrated in Figure 4.12. If the paging response from the legitimate UE would reach the network

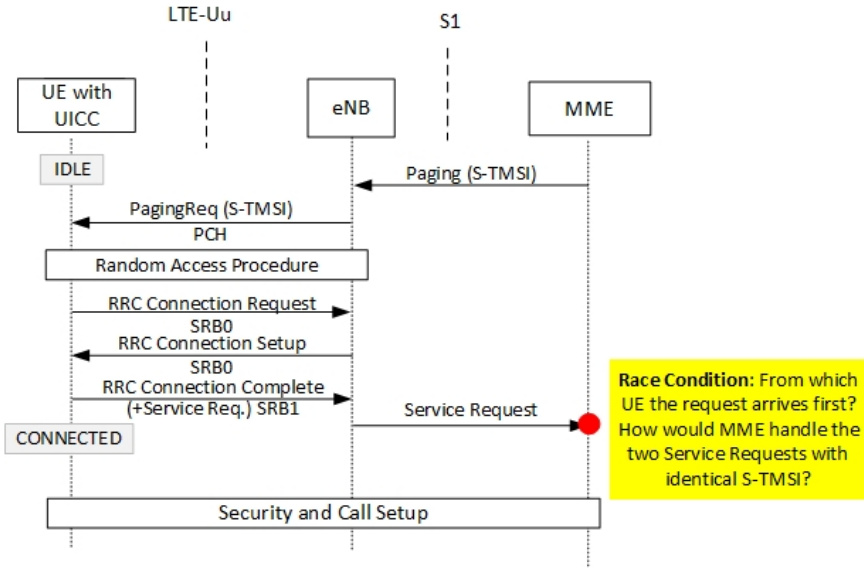

Figure 4.12: Race point in connection to paging responses from the legitimate UE and the adversary.

first, the attack would not cause any harm. But then it would be interesting to know how the network reacts when it receives the duplicate paging response, which can be verified by analyzing the trace taken by the *srsUE*. If the paging response from the attacker reaches the network first, which is what we wish, we can verify if it causes the legitimate UE not to receive its service, by checking if the legitimate UE receives the test data in time.

4.6.3 Result and Discussion

After setting up the *srsUE* application properly, it is started with command *"srsue ue.conf"* at the directory where the execution file *srsue* locates. The application starts to listen to paging messages. Then paging to my mobile is triggered by sending some data to it, for example, a Facebook message. Once the software UE has detected the pre-configured S-TMSI in the paging message, it initiates the Random Access Procedure to gain SRB0, processes Random Access Response, then sends RRC Connection Request to the eNB. However, no response is received and hence the application goes back to the IDLE state after time-out.

The messages sent between the *srsUE* application and the network is traced and saved as a capture file, which can be analyzed with Wireshark afterwards. The traced messages are open with Wireshark, and the list of messages are shown in the Figure

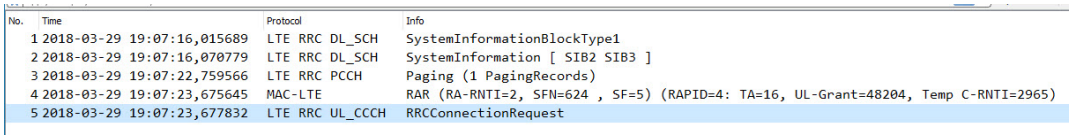

Figure 4.13: Captured messages between the UE and the network

.

4.13. The first two messages are SIBs, which provide necessary information for the UE to camp on the cell. The third message is the paging with the pre-configured S-TMSI as the ue-Identity. Upon reception of the paging message, *srsUE* initiates the Random Access procedure. The fourth message is the received Random Access Response, which among others allocates the temporary RNTI to the UE. Note that the Random Access Request is not shown in the trace, because it is just a physical waveform. The last message is the RRC Connection Request sent from *srsUE* on the allocated temporary RNTI. The decoded trace is attached in Appendix D.

There is no the expected RRC Connection Setup from the network, and hence the message flow stops here and the paging response can not get sent. The reason is unknown. To figure out the possible reasons, some troubleshooting has been performed, which is described in the next subclauses.

4.6.4 Troubleshooting

To figure out why there is no response from the network after RRC Connection Request, troubleshooting is done to find out the possible reasons.

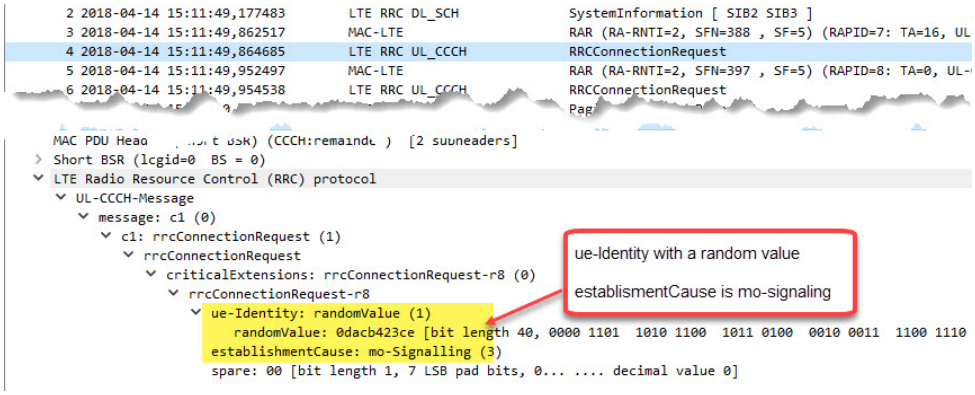

Figure 4.14: Decoded RRC Connection Request, which has a random value as ue-Identity

.

Attach Attempt

During paging response attempt, the ue-Identity in the RRC Connection Request is identical with the request from the legitimate UE. The eNB might ignore the request arrived later. To verify it, an Attach Request is attempted. The updates in the Code 4.1 and Code 4.3 are configured back to the original values, i.e. no pre-configured S-TMSI and RRC Connection Cause with 'MO_Signaling'. The software UE sets a random value as ue-Identity in the RRC Connection Request, which is shown in Figure 4.14. Still no response is received from the network, indicating that it might not be caused by the identical ue-Identity in the RRC Connection Request.

Attach Attempt Towards Telenor's LTE

For comparison, an Attach Request is attempted towards Telenor's LTE. To connect to Telenor's LTE, the configuration parameters changed in the configuration file are listed in the Code 4.4. Same as in the Attach Request attempt towards Telia, the software UE sets a random value as ue-Identity in the RRC Connection Request.

Interestingly, the eNB from Telenor does reply to the RRC Connection Request. And the Attach Request gets through until it, as expected, gets rejected because of the invalid IMSI, which is taken from the configuration file. The traced message flow is shown in the Figure 4.15.

Code 4.4: srsUE Configuration for the connection to Telenor LTE

```
...
// Set the downlink EARFCN same as the target cell
dl_earfcn = 6400 // For Telenor cell
...
[usim]
...
// Set a dummy IMSI with Telenor as home PLMN
// Set IMEI same as my mobile's
imsi = 24201xxxxxxxxxx
imei = 35533xxxxxxxxxx
```

Time	Protocol	Info
2018-04-29 12:12:05,429523	LTE RRC DL_SCH	SystemInformationBlockType1
2018-04-29 12:12:05,486468	LTE RRC DL_SCH	SystemInformation [SIB2 SIB3]
2018-04-29 12:12:05,512796	LTE RRC UL_CCCH	RRCConnectionRequest
2018-04-29 12:12:05,522472	LTE RRC DL_CCCH	RRCConnectionSetup
2018-04-29 12:12:05,531850	LTE RRC UL_DCCH/NAS-EPS	RRCConnectionSetupComplete, Attach request, PDN connectivity request
2018-04-29 12:12:05,702917	LTE RRC DL_DCCH	RRCConnectionRelease [cause=other]

Figure 4.15: Traced Message flow under attach attempt towards Telenor's LTE.

Why the *srsUE* application works better towards Telenor's LTE is unknown. The GitHub srsLTE web page [Git] lists the tested and validated eNBs, which works well with the *srsUE*. Probably the eNB in Telenor's LTE is one of the validated eNBs, while the eNB in Telia's LTE is not validated. It seems that the eNB in Telia's LTE does not directly work well with the *srsUE* application.

4.6.5 Summary

Because of no response from Telia's LTE to the RRC Connection Request, the paging response can not get fed into the network. Because of time limitation, no further tuning towards Telia's LTE is tried.

Towards Telenor's LTE, response to the RRC Connection Request is received during the Attach attempt. However no paging response is attempted because of lack of subscription from Telenor .

A future work can continue to tune the *srsUE* application to make it work well with Telia's LTE and try again. Alternatively buy a Telenor's subscription and try it towards Telenor's LTE instead.

Chapter 5
Summary

This chapter summarizes the thesis work and suggests several potential future works. The summary and conclusions from the experimental work are described in the first section, and the suggested future works are described in the second section.

5.1 Conclusion

Both a theoretical study and practical experiments are performed in this thesis. The theoretical study includes a review of LTE attacks with focus on the paging procedure. The practical experiments implement a page message catcher and a paging response feeder, capture and analyze paging messages for three LTE operators in Norway, verify the smart paging feature, and analyze S-TMSI refreshment frequency in Telia's LTE.

The theoretical study in Chapter 3 reviews the LTE attacks and the corresponding countermeasures described in the literature, with focus on the attacks where the paging procedure is exploited. Due to the development of open source software and hardware, more and more security exploits and experiments have been performed towards LTE systems, corresponding countermeasures and enhancements have been proposed and verified. Whether the discovered weaknesses shall be overcome in the future mobile network should be valued carefully. If and which of the proposed countermeasures shall be used, should also be considered.

In Chapter 4.3.1, a broadcast message catcher is setup to capture the broadcast messages. The collected data is carefully analyzed and the results are presented in the Chapter 4.3.2. It is proven that with open source software and affordable hardware, with some efforts, it is practically feasible to mount a passive broadcast message catcher towards any LTE systems and collect data. The collected data reveals important information about both the network setup and the user private information such as location and identity. Of the all captured paging messages, none

has IMSI as the user identity, which proves that paging with IMSI is a very seldom case.

The smart paging feature is verified in the Chapter 4.4. The collected data proves that the smart paging feature is deployed in both Telia's and Telenor's LTE. With the smart paging feature on, the cost for paging decreases significantly, since the network pages a user only within one or few cells instead of a whole tracking area. However, it becomes worse for the location privacy in case of the paging attack, because the user can be located within a much smaller geographical area.

In Chapter 4.5, this thesis verifies how well Telia's LTE protects the user identity and location privacy with respect to M-TMSI update frequency. As shown in the Table 4.5 with an observation period Jan - Apr 2018, the observed longest period without M-TMSI update is 48 hours and 28 minutes. To keep the M-TMSI unchanged for more than two days, is definitely a weak point with respect to the location tracking by following the M-TMSI.

Inspired by the attacks performed in GSM as presented in [GRS13], an attempt to build a paging response feeder is performed in Chapter 4.6. The goal is to verify the feasibility to perform such attacks in the LTE with currently available open source software and hardware. Open source software implementing the LTE UE stack, *srsUE*, is used to conduct this experiment. The attempt is performed towards Telia's LTE, because of availability of a subscription from Telia. The attempt does not succeed because the *srsUE* can not establish a stable connection with Telia's LTE. Although the *srsUE* can establish a stable connection with Telenor's LTE, no paging response is attempted towards Telenor's LTE because of no Telenor subscription to experiment with. The different behavior of *srsUE* towards Telia's and Telenor's LTE indicates no direct compatibility between the *srsUE* and the eNB from Telia.

5.2 Future Work

M-TMSI Update Frequency Check in Telenor's LTE

In Chapter 4.5, the M-TMSI update frequency in Telia's LTE is studied and it is found out that the M-TMSI does not get updated often, which is not a good practice as it leaves room to track a user by following the M-TMSI.

The current work does not study how it is in the LTE from Telenor, who is the biggest LTE service provider in Norway. Thus the M-TMSI update frequency in Telenor's LTE, or other Norwegian operators, can be studied in a future work.

Paging Response Feeding

The paging response feeding in this thesis does not succeed because the software *srsUE* can not establish a RRC connection with the eNB from Telia. Because of time limitation, no further tuning of the *srsUE* has been tried to make it work. Consequently, further work can be done to tune the *srsUE* to make it work towards Telia's LTE and then try to feed in the paging response.

Alternatively future work could try to feed the paging response towards Telenor's LTE against a LTE subscription from Telenor, because the *srsUE* indeed can establish the RRC connection with the eNB from Telenor.

Paging with IMSI - to Drill Down Mobile Battery

As described in Chapter 2.2.6, at very rare cases the IMSI can be used as the user identity in the paging message, for network error recovery. Upon reception of the paging with IMSI, the UE should terminate all running specific procedures if any, detach locally, and then initiate the attach procedure to regain network access [TS2b, Chapter 5.6.2.2.2]. Consequently, to mount a fake eNB and keep paging with IMSI, will not only disturb services, but also drill down the terminal battery. While the terminal keeps on detaching and attaching caused by the paging, it consumes much more battery than otherwise staying at the idle state. Therefore, a future work might include experimenting with battery consumption by keeping paging with IMSI towards a target from a fake eNB.

Selected Service Attack

The authors in [SBA+15], which is reviewed in the Chapter 3.3, had discussed the theoretical feasibility to perform selected service attack via manipulating the terminal capability included in the Attach Request message. They did not perform practical implementation because of lack of LTE UE baseband software. Now there is LTE UE baseband software available, such as *srsLTE*. Thus, a practical implementation of such attack could be performed in a future work to verify the practical feasibility.

References

[23.] 3GPP TS 23.003. 3GPP Numbering, addressing and identification, Release 15.2.0. http://www.3gpp.org/ftp//Specs/archive/23_series/23.003/23003-f20.zip.

[CKG+11] Mukesh Chandra, Neeraj Kumar, Rahul Gupta, Sunil Kumar, Vijay K Chaurasia, and Vivek Srivastav. Protection from paging and signaling attack in 3G CDMA networks. In *Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on*, pages 406–410. IEEE, 2011.

[CMZC09] Liang Cai, Gabriel Maganis, Hui Zang, and Hao Chen. Mitigating DoS Attacks on the Paging Channel by Efficient Encoding in Page Messages. In *International Conference on Security and Privacy in Communication Systems*, pages 1–20. Springer, 2009.

[Ett] Ettus. USRP B200mini. https://www.ettus.com/product/details/USRP-%%B200mini. [Online; Last Access Date: 07.01.2018].

[FHMN13] Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller, and Valtteri Niemi. *LTE Security*. John Wiley and Sons Ltd, 2013.

[For] Source Forge. OpenLTE - An open source implementation of the 3GPP LTE specifications. https://sourceforge.net/projects/openlte/. [Online; Last Access Date: 30.04.2018].

[Git] GitHub. GitHub srsLTE. https://github.com/srsLTE/srsLTE. [Online; Last Access Date: 14.04.2018].

[GRS13] Nico Golde, Kévin Redon, and Jean-Pierre Seifert. Let Me Answer That for You: Exploiting Broadcast Information in Cellular Networks. In *USENIX Security Symposium*, pages 33–48, 2013.

[JNNN17] Enrique Cobo Jiménez, Prajwol Kumar Nakarmi, Mats Näslund, and Karl Norrman. Subscription identifier privacy in 5G systems. In *Selected Topics in Mobile and Wireless Networking (MoWNeT), 2017 International Conference on*, pages 1–8. IEEE, 2017.

[Jov16] Roger Piqueras Jover. LTE security, protocol exploits and location tracking experimentation with low-cost software radio. *arXiv preprint arXiv:1607.05171*, 2016.

[Mar] Marben. Marben LTE ASN.1 Decoder. http://www.marben-products.com/decoder-asn1-lte/. [Online; Last Access Date: 30.04.2018].

[MO17] Stig F. Mjølsnes and Ruxandra F. Olimid. Easy 4G/LTE IMSI Catchers for Non-Programmers. *arXiv preprint arXiv:1702.04434*, 2017.

[NKOa] NKOM. Finnsenderen. http://www.finnsenderen.no. [Online; Last Access Date: 09.01.2018].

[NKOb] NKOM. Norwegian Communication Authority Statistics. https://www.nkom.no/marked/ekomtjenester/statistikk/det-norske-ekommarkedet-rapporter/_attachment/30658?_ts=15f7167389b. [Online; Last Access Date: 03.03.2018].

[Nok] Nokia. Nokia Managing Signaling Traffic. https://insight.nokia.com/managing-lte-core-network-signaling-traffic. [Online; Last Access Date: 27.01.2018].

[OB13] Murat Oğul and Selçuk Baktır. Practical attacks on mobile cellular networks and possible countermeasures. *Future Internet*, 5(4):474–489, 2013.

[PBS08] L. Yu Paul, John S. Baras, and Brian M. Sadler. Physical-layer authentication. *IEEE Transactions on Information Forensics and Security*, 3(1):38–51, 2008.

[Por] Statista The Statistics Portal. Number of LTE subscriptions worldwide by region from 2011 to 2023 (in millions). https://www.statista.com/statistics/641510/lte-mobile-subscriptions-worldwide/. [Online; Last Access Date: 04.05.2018].

[SBA+15] Altaf Shaik, Ravishankar Borgaonkar, N Asokan, Valtteri Niemi, and Jean-Pierre Seifert. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. *arXiv preprint arXiv:1510.07563*, 2015.

[Sha] ShareTechNote. srsLTE Build Process. http://www.sharetechnote.com/html/SDR_srsLTE_Build.html. [Online; Last Access Date: 17.12.2017].

[Sør17] Christian Sørseth. Location Disclosure in LTE Networks by using IMSI Catcher. Master's thesis, NTNU, 2017.

[SRSa] SRS. Software Radio Systems. http://www.softwareradiosystems.com. [Online; Last Access Date: 01.04.2018].

[SRSb] SRS. srsLTE. http://www.softwareradiosystems.com/products/#srslte. [Online; Last Access Date: 01.04.2018].

[SRSc] SRS. srsUE. http://www.softwareradiosystems.com/products/#srsue. [Online; Last Access Date: 01.04.2018].

[SZB06] Jérémy Serror, Hui Zang, and Jean-Chrysostome Bolot. Impact of paging channel overloads or attacks on a cellular network. In *Workshop on Wireless Security*, pages 75–84, 2006.

[TB13] Tuan Ta and John S. Baras. Enhancing privacy in LTE paging system using physical layer identification. In *Data Privacy Management and Autonomous Spontaneous Security*, pages 15–28. Springer, 2013.

[TS2a] 3GPP TS24.007. 3GPP Mobile radio interface signalling layer 3; General Aspects, Release 14.0.0. http://www.3gpp.org/ftp//Specs/archive/24_series/24.007/24007-e00.zip.

[TS2b] 3GPP TS24.301. Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS), Release 14.4.0. http://www.3gpp.org/ftp//Specs/archive/24_series/24.301/24301-e40.zip.

[TS3a] 3GPP TS31.102. Characteristics of the Universal Subscriber Identity Module (USIM) application, Release 14.4.0. http://www.3gpp.org/ftp//Specs/archive/31_series/31.102/31102-e40.zip.

[TS3b] 3GPP TS33.401. 3GPP System Architecture Evolution (SAE); Security architecture, Release 15.0.0. http://www.3gpp.org/ftp//Specs/archive/33_series/33.401/33401-f00.zip.

[TS3c] 3GPP TS33.501. Security architecture and procedures for 5G System. http://www.3gpp.org/ftp//Specs/archive/33_series/33.501/33501-f00.zip.

[TS3d] 3GPP TS36.101. Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception (Release 14). http://www.3gpp.org/ftp//Specs/archive/36_series/36.101/36101-e50.zip.

[TS3e] 3GPP TS36.211. Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation (Release 15). http://www.3gpp.org/ftp//Specs/archive/36_series/36.211/36211-f10.zip.

[TS3f] 3GPP TS36.321. Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification (Release 14). http://www.3gpp.org/ftp//Specs/archive/36_series/36.213/36213-e40.zip.

[TS3g] 3GPP TS36.331. Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification, Release 14.3.0. http://www.3gpp.org/ftp//Specs/archive/36_series/36.331/36331-e30.zip.

[TS3h] 3GPP TS36.413. Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP), (Release 14), v14.3.0. http://www.3gpp.org/ftp//Specs/archive/36_series/36.413/36413-e30.zip.

[Wir] WireShark. WireShark Network Protrocol Analyzer. https://www.wireshark.org/. [Online; Last Access Date: 11.04.2018].

[ZB07] Hui Zang and Jean C Bolot. Mining call and mobility data to improve paging efficiency in cellular networks. In *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pages 123–134. ACM, 2007.

Appendix A
Paging Message Decoder

```
#!/usr/bin/python

from libmich.asn1.processor import *

def decodePCCH(pcchHex):
        load_module('RRCLTE')
        ASN1.ASN1Obj.CODEC=PER
        PER.VARIANT='U'
        pcch=GLOBAL.TYPE['PCCH-Message']
        buf=pcchHex.decode('hex')
        pcch.decode(buf)
        show(pcch)

with open('/home/shelley/PagingMsg_sorted.txt') as fp:
        for line in fp:
                if line.startswith("["):
                        line=line[1:-3]
                        line=line.replace("␣","")
                        decodePCCH(line)
```

Appendix B

Paging Message Capture Source Code Update

```
/* Print out the data if any */
/* Print timestamp for each captured data */
/* Added to get Time - Zhou: 20180118 */

time_t rawtime;
struct tm * timeinfo;

time ( &rawtime );
timeinfo = localtime ( &rawtime );
printf ( "Captured␣at:␣%s", asctime (timeinfo) );

printf("[%02X",data[0]);
for(int d=1;d < n/8;d++) printf("␣%02X",data[d]);
   printf("];␣\n");
/* End of added part - Zhou: 20180118*/
```

Appendix C

Configuration File for the UE Application srsUE

```
#####################################################################
# srsUE configuration file
#####################################################################
# RF configuration
#
# dl_earfcn: Downlink EARFCN code.
# freq_offset: Uplink and Downlink optional frequency offset (in Hz)
# tx_gain: Transmit gain (dB).
# rx_gain: Optional receive gain (dB). If disabled, AGC if enabled
#
# Optional parameters:
# dl_freq: Override DL frequency corresponding to dl_earfcn
# ul_freq: Override UL frequency corresponding to dl_earfcn
# nof_rx_ant: Number of RX antennas (Default 1, supported 1 or 2)
# device_name: Device driver family. Supported options: "auto" (uses
    ↪ first found), "UHD" or "bladeRF"
# device_args: Arguments for the device driver. Options are "auto" or
    ↪  any string.
# Default for UHD: "recv_frame_size=9232,send_frame_size=9232"
# Default for bladeRF: ""
# #time_adv_nsamples: Transmission time advance (in number of samples
    ↪ ) to compensate for RF delay
# from antenna to timestamp insertion.
# Default "auto". B210 USRP: 100 samples, bladeRF: 27.
# burst_preamble_us: Preamble length to transmit before start of
    ↪ burst.
# Default "auto". B210 USRP: 400 us, bladeRF: 0 us.
#####################################################################
[rf]
```

```
dl_earfcn = 3400
freq_offset = 0
tx_gain = 80
rx_gain = 40

#nof_rx_ant = 1
#device_name = auto
#device_args = auto
#time_adv_nsamples = auto
#burst_preamble_us = auto


#####################################################################
# MAC-layer packet capture configuration
#
# Packets are captured to file in the compact format decoded by
# the Wireshark mac-lte-framed dissector and with DLT 147.
# To use the dissector, edit the preferences for DLT_USER to
# add an entry with DLT=147, Payload Protocol=mac-lte-framed.
# For more information see: https://wiki.wireshark.org/MAC-LTE
#
# enable: Enable MAC layer packet captures (true/false)
# filename: File path to use for packet captures
#####################################################################
[pcap]
enable = false
filename = /tmp/ue.pcap
nas_enable = false
nas_filename = /tmp/nas.pcap

#####################################################################
# Log configuration
#
# Log levels can be set for individual layers. "all_level" sets log
# level for all layers unless otherwise configured.
# Format: e.g. phy_level = info
#
# In the same way, packet hex dumps can be limited for each level.
# "all_hex_limit" sets the hex limit for all layers unless otherwise
# configured.
# Format: e.g. phy_hex_limit = 32
```

```
#
# Logging layers: phy, mac, rlc, pdcp, rrc, nas, gw, usim, all
# Logging levels: debug, info, warning, error, none
#
# filename: File path to use for log output. Can be set to stdout
# to print logs to standard output
# file_max_size: Maximum file size (in kilobytes). When passed,
    ↪ multiple files are created.
# If set to negative, a single log file will be created.
##########################################################################
[log]
all_level = info
phy_lib_level = none
all_hex_limit = 32
filename = /tmp/ue.log
file_max_size = -1

##########################################################################
# USIM configuration
#
# algo: Authentication algorithm (xor/milenage)
# op: 128-bit Operator Variant Algorithm Configuration Field (hex)
# amf: 16-bit Authentication Management Field (hex)
# k: 128-bit subscriber key (hex)
# imsi: 15 digit International Mobile Subscriber Identity
# imei: 15 digit International Mobile Station Equipment Identity
##########################################################################
[usim]
algo = xor
op = 63BFA50EE6523365FF14C1F45F88737D
k = 00112233445566778899aabbccddeeff
imsi = 001010123456789
imei = 353490069873319


##########################################################################
# RRC configuration
#
# ue_category: Sets UE category (range 1-5). Default: 4
# feature_group: Hex value of the featureGroupIndicators field in the
# UECapabilityInformation message. Default 0xe6041c00
```

```
#####################################################################
[rrc]
#ue_category = 4
#feature_group = 0xe6041c00

#####################################################################
# NAS configuration
#
# apn:  Set Access Point Name (APN)
#####################################################################
[nas]
# apn = internetinternet


[gui]
enable = false

#####################################################################
# Expert configuration options
#
# ip_netmask: Netmask of the tun_srsue device. Default: 255.255.255.0
# rssi_sensor_enabled: Enable or disable RF frontend RSSI sensor.
    ↪ Required for RSRP metrics but
# can cause UHD instability for long-duration testing. Default true.
# prach_gain: PRACH gain (dB). If defined, forces a gain for the
    ↪ tranmsission of PRACH only.,
# Default is to use tx_gain in [rf] section.
# cqi_max: Upper bound on the maximum CQI to be reported. Default 15.
# cqi_fixed: Fixes the reported CQI to a constant value. Default
    ↪ disabled.
# snr_ema_coeff: Sets the SNR exponential moving average coefficient
    ↪ (Default 0.1)
# snr_estim_alg: Sets the noise estimation algorithm. (Default refs)
# Options: pss: use difference between received and known pss signal,
# refs: use difference between noise references and noiseless (after
    ↪ filtering)
# empty: use empty subcarriers in the boarder of pss/sss signal
# pdsch_max_its: Maximum number of turbo decoder iterations (Default
    ↪ 4)
# attach_enable_64qam: Enables PUSCH 64QAM modulation before
    ↪ attachment (Necessary for old
```

```
# Amarisoft LTE 100 eNodeB, disabled by default)
# nof_phy_threads: Selects the number of PHY threads (maximum 4,
    ↪ minimum 1, default 2)
# equalizer_mode: Selects equalizer mode. Valid modes are: "mmse", "
    ↪ zf" or any
# non-negative real number to indicate a regularized zf coefficient.
# Default is MMSE.
# time_correct_period: Period for sampling time offset correction.
    ↪ Default is 10 (ue_sync.c),
# good for long channels. For best performance at highest SNR reduce
    ↪ it to 1.
# sfo_correct_disable: Disables phase correction before channel
    ↪ estimation to compensate for
# sampling frequency offset. Default is enabled.
# sss_algorithm: Selects the SSS estimation algorithm. Can choose
    ↪ between
# {full, partial, diff}.
# estimator_fil_w: Chooses the coefficients for the 3-tap channel
    ↪ estimator centered filter.
# The taps are [w, 1-2w, w]
# metrics_period_secs: Sets the period at which metrics are requested
    ↪  from the UE.
#
# pregenerate_signals: Pregenerate uplink signals after attach.
    ↪ Improves CPU performance.
#
# average_subframe_enabled: Averages in the time domain the channel
    ↪ estimates within 1 subframe.
# Needs accurate CFO correction.
#
# sic_pss_enabled: Applies Successive Interference Cancellation to
    ↪ PSS signals when searching for neighbour cells.
# Must be disabled if cells have identical channel and timing, for
    ↪ instance if generated from
# the same source.
#
# metrics_csv_enable: Write UE metrics to CSV file.
#
# metrics_csv_filename: File path to use for CSV metrics.
#
```

```
# cfo_integer_enabled: Enables integer CFO estimation and correction.
    ↪  This needs improvement
# and may lead to incorrect synchronization. Use with caution.
# cfo_correct_tol_hz: Tolerance (in Hz) for digial CFO compensation.
    ↪ Lower tolerance means that
# a new table will be generated more often.
#
# cfo_pss_ema: CFO Exponential Moving Average coefficient for PSS
    ↪ estimation during TRACK.
# cfo_ref_ema: CFO Exponential Moving Average coefficient for RS
    ↪ estimation after PSS acquisition
# cfo_ref_mask: Bitmask for subframes on which to run RS estimation (
    ↪ set to 0 to disable, default sf=[1, 5])
# cfo_loop_bw: CFO feedback loop bandwidth for samples from PSS or RS
# cfo_loop_pss_tol: Tolerance (in Hz) of the PSS estimation method.
    ↪ Below this value, PSS estimation does not feeds back the loop
# and RS estimations are used instead (when available)
# cfo_loop_ref_min: Tolerance (in Hz) of the RS estimation method.
    ↪ Below this value, RS estimation does not feeds back the loop
# cfo_loop_pss_timeout: After the PSS estimation is below
    ↪ cfo_loop_pss_tol for cfo_loop_pss_timeout times consecutively,
# RS adjustments are allowed.
#
###############################################################################
[expert]
#ip_netmask = 255.255.255.0
#rssi_sensor_enabled = false
#prach_gain = 30
#cqi_max = 15
#cqi_fixed = 10
#snr_ema_coeff = 0.1
#snr_estim_alg = refs
#pdsch_max_its = 4
#attach_enable_64qam = false
#nof_phy_threads = 2
#equalizer_mode = mmse
#time_correct_period = 5
#sfo_correct_disable = false
#sss_algorithm = full
#estimator_fil_w = 0.1
#average_subframe_enabled = true
```

```
#sic_pss_enabled = true
#pregenerate_signals = false
#metrics_csv_enable = false
#metrics_csv_filename = /tmp/ue_metrics.csv

# CFO related values
#cfo_integer_enabled = false
#cfo_correct_tol_hz = 1.0
#cfo_pss_ema = 0.05
#cfo_ref_mask = 1023
#cfo_loop_bw_pss = 0.05
#cfo_loop_bw_ref = 0.01
#cfo_loop_pss_tol = 400
#cfo_loop_ref_min = 0
#cfo_loop_pss_conv = 20

###############################################################################
# Manual RF calibration
#
# Applies DC offset and IQ imbalance to TX and RX modules.
# Currently this configuration is only used if the detected device is
    ↪ a bladeRF
#
# tx_corr_dc_gain: TX DC offset gain correction
# tx_corr_dc_phase: TX DC offset phase correction
# tx_corr_iq_i: TX IQ imbalance inphase correction
# tx_corr_iq_q: TX IQ imbalance quadrature correction
# same can be configured for rx_*
###############################################################################
[rf_calibration]
tx_corr_dc_gain = 20
tx_corr_dc_phase = 184
tx_corr_iq_i = 19
tx_corr_iq_q = 97
```

Appendix D
Decoded Wireshark Trace

The decoded messages sent between the srsUE and the network during paging response feeding

```
No. Time Protocol
    1 2018-03-29 19:07:16,015689 LTE RRC DL_SCH
        ↪ SystemInformationBlockType1

Frame 1: 37 bytes on wire (296 bits), 37 bytes captured (296 bits)
  Encapsulation type: USER 0 (45)
  Arrival Time: Mar 29, 2018 19:07:16.015689000 Vest-Europa (
      ↪ sommertid)
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1522343236.015689000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 37 bytes (296 bits)
  Capture Length: 37 bytes (296 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: user_dlt:mac-lte-framed:mac-lte:lte_rrc]
DLT: 147, Payload: mac-lte-framed (mac-lte-framed)
MAC-LTE BCH PDU (22 bytes, on DL-SCH transport)
  [Context (RNTI=65535)]
    [Radio Type: FDD (1)]
    [Direction: Downlink (1)]
    [System Frame Number: 882]
    [Subframe: 5]
    [RNTI: 65535]
```

```
    [RNTI Type: SI-RNTI (4)]
    [Length of frame: 22]
    [CRC Status: OK (1)]
    [Carrier Id: Primary (0)]
  [Transport channel: DL-SCH (4)]
LTE Radio Resource Control (RRC) protocol
  BCCH-DL-SCH-Message
    message: c1 (0)
      c1: systemInformationBlockType1 (1)
        systemInformationBlockType1
          cellAccessRelatedInfo
            plmn-IdentityList: 1 item
              Item 0
                PLMN-IdentityInfo
                  plmn-Identity
                    mcc: 3 items
                      Item 0
                        MCC-MNC-Digit: 2
                      Item 1
                        MCC-MNC-Digit: 4
                      Item 2
                        MCC-MNC-Digit: 2
                    mnc: 2 items
                      Item 0
                        MCC-MNC-Digit: 0
                      Item 1
                        MCC-MNC-Digit: 2
                  cellReservedForOperatorUse: notReserved (1)
            trackingAreaCode: 0901 [bit length 16, 0000 1001 0000
                ↪ 0001 decimal value 2305]
            cellIdentity: 21283160 [bit length 28, 4 LSB pad bits,
                ↪ 0010 0001 0010 1000 0011 0001 0110 .... decimal
                ↪ value 34767638]
            cellBarred: notBarred (1)
            intraFreqReselection: allowed (0)
            .... ..0. csg-Indication: False
          cellSelectionInfo
            q-RxLevMin: -132dBm (-66)
          freqBandIndicator: 20
          schedulingInfoList: 5 items
            Item 0
```

```
              SchedulingInfo
                si-Periodicity: rf8 (0)
                sib-MappingInfo: 1 item
                  Item 0
                    SIB-Type: sibType3 (0)
            Item 1
              SchedulingInfo
                si-Periodicity: rf64 (3)
                sib-MappingInfo: 1 item
                  Item 0
                    SIB-Type: sibType4 (1)
            Item 2
              SchedulingInfo
                si-Periodicity: rf64 (3)
                sib-MappingInfo: 1 item
                  Item 0
                    SIB-Type: sibType5 (2)
            Item 3
              SchedulingInfo
                si-Periodicity: rf64 (3)
                sib-MappingInfo: 1 item
                  Item 0
                    SIB-Type: sibType6 (3)
            Item 4
              SchedulingInfo
                si-Periodicity: rf64 (3)
                sib-MappingInfo: 1 item
                  Item 0
                    SIB-Type: sibType7 (4)
          si-WindowLength: ms10 (3)
          systemInfoValueTag: 3

Frame (37 bytes):
0000 01 01 04 02 ff ff 03 00 00 04 37 25 07 01 01 40 ..........7%...@
0010 49 08 05 09 01 21 28 31 68 11 32 00 81 84 2c 22 I....!(1h.2...,"
0020 61 1b 09 18 c0 a....
Bitstring tvb (2 bytes):
0000 09 01 ..
Bitstring tvb (4 bytes):
0000 21 28 31 60 !(1‘
No. Time Protocol
```

```
    2 2018-03-29 19:07:16,070779 LTE RRC DL_SCH SystemInformation [
       ↪ SIB2 SIB3 ]

Frame 2: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
  Encapsulation type: USER 0 (45)
  Arrival Time: Mar 29, 2018 19:07:16.070779000 Vest-Europa (
      ↪ sommertid)
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1522343236.070779000 seconds
  [Time delta from previous captured frame: 0.055090000 seconds]
  [Time delta from previous displayed frame: 0.055090000 seconds]
  [Time since reference or first frame: 0.055090000 seconds]
  Frame Number: 2
  Frame Length: 52 bytes (416 bits)
  Capture Length: 52 bytes (416 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: user_dlt:mac-lte-framed:mac-lte:lte_rrc]
DLT: 147, Payload: mac-lte-framed (mac-lte-framed)
MAC-LTE BCH PDU (37 bytes, on DL-SCH transport)
  [Context (RNTI=65535)]
    [Radio Type: FDD (1)]
    [Direction: Downlink (1)]
    [System Frame Number: 888]
    [Subframe: 0]
    [RNTI: 65535]
    [RNTI Type: SI-RNTI (4)]
    [Length of frame: 37]
    [CRC Status: OK (1)]
    [Carrier Id: Primary (0)]
  [Transport channel: DL-SCH (4)]
  LTE Radio Resource Control (RRC) protocol
    BCCH-DL-SCH-Message
      message: c1 (0)
        c1: systemInformation (0)
          systemInformation
            criticalExtensions: systemInformation-r8 (0)
              systemInformation-r8
                sib-TypeAndInfo: 2 items
                  Item 0
                    sib-TypeAndInfo item: sib2 (0)
```

```
sib2
  radioResourceConfigCommon
    rach-ConfigCommon
      preambleInfo
        numberOfRA-Preambles: n52 (12)
      powerRampingParameters
        powerRampingStep: dB4 (2)
        preambleInitialReceivedTargetPower: dBm
            ↪ -110 (5)
      ra-SupervisionInfo
        preambleTransMax: n10 (6)
        ra-ResponseWindowSize: sf10 (7)
        mac-ContentionResolutionTimer: sf64 (7)
      maxHARQ-Msg3Tx: 4
    bcch-Config
      modificationPeriodCoeff: n2 (0)
    pcch-Config
      defaultPagingCycle: rf128 (2)
      nB: oneT (2)
    prach-Config
      rootSequenceIndex: 608
      prach-ConfigInfo
        prach-ConfigIndex: 19
        ..0. .... highSpeedFlag: False
        zeroCorrelationZoneConfig: 15
        prach-FreqOffset: 4
    pdsch-ConfigCommon
      referenceSignalPower: 18dBm
      p-b: 1
    pusch-ConfigCommon
      pusch-ConfigBasic
        n-SB: 1
        hoppingMode: interSubFrame (0)
        pusch-HoppingOffset: 0
        .1.. .... enable64QAM: True
      ul-ReferenceSignalsPUSCH
        ..1. .... groupHoppingEnabled: True
        groupAssignmentPUSCH: 0
        0... .... sequenceHoppingEnabled: False
        cyclicShift: 0
    pucch-ConfigCommon
```

```
                deltaPUCCH-Shift: ds1 (0)
                nRB-CQI: 6
                nCS-AN: 0
                n1PUCCH-AN: 8
              soundingRS-UL-ConfigCommon: release (0)
                release: NULL
              uplinkPowerControlCommon
                p0-NominalPUSCH: -103dBm
                alpha: al1 (7)
                p0-NominalPUCCH: -117dBm
                deltaFList-PUCCH
                  deltaF-PUCCH-Format1: deltaF0 (1)
                  deltaF-PUCCH-Format1b: deltaF3 (1)
                  deltaF-PUCCH-Format2: deltaF0 (1)
                  deltaF-PUCCH-Format2a: deltaF0 (1)
                  deltaF-PUCCH-Format2b: deltaF0 (1)
                deltaPreambleMsg3: 12dB (6)
              ul-CyclicPrefixLength: len1 (0)
              uplinkPowerControlCommon-v1020
                deltaF-PUCCH-Format3-r10: deltaF0 (1)
                deltaF-PUCCH-Format1bCS-r10: deltaF2 (1)
              pusch-ConfigCommon-v1270
                enable64QAM-v1270: true (0)
            ue-TimersAndConstants
              t300: ms1000 (5)
              t301: ms400 (3)
              t310: ms2000 (6)
              n310: n20 (7)
              t311: ms3000 (1)
              n311: n1 (0)
            freqInfo
              additionalSpectrumEmission: 1
            timeAlignmentTimerCommon: infinity (7)
      Item 1
        sib-TypeAndInfo item: sib3 (1)
          sib3
            cellReselectionInfoCommon
              q-Hyst: dB4 (4)
            cellReselectionServingFreqInfo
              s-NonIntraSearch: 16dB (8)
              threshServingLow: 10dB (5)
```

```
                        cellReselectionPriority: 5
                      intraFreqCellReselectionInfo
                        q-RxLevMin: -132dBm (-66)
                        s-IntraSearch: 62dB (31)
                        allowedMeasBandwidth: mbw50 (3)
                        .... .1.. presenceAntennaPort1: True
                        neighCellConfig: The MBSFN subframe
                            ↪ allocations of all neighbour cells are
                            ↪ identical to or subsets of that in the
                            ↪ serving cell (2)
                        t-ReselectionEUTRA: 1s

Frame (52 bytes):
0000 01 01 04 02 ff ff 03 00 00 04 37 80 07 01 01 00 ..........7.....
0010 80 4c 95 bf 64 a6 04 de 12 72 00 60 00 30 01 01 .L..d....r.‘.0..
0020 7e a5 57 81 d0 0c a0 0c 02 bd c8 01 c2 25 05 ac ~.W..........%..
0030 27 de 20 00 ’. .
Bitstring tvb (1 byte):
0000 80 .
No. Time Protocol
    3 2018-03-29 19:07:22,759566 LTE RRC PCCH Paging (1 PagingRecords
        ↪ )

Frame 3: 24 bytes on wire (192 bits), 24 bytes captured (192 bits)
  Encapsulation type: USER 0 (45)
  Arrival Time: Mar 29, 2018 19:07:22.759566000 Vest-Europa (
      ↪ sommertid)
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1522343242.759566000 seconds
  [Time delta from previous captured frame: 6.688787000 seconds]
  [Time delta from previous displayed frame: 6.688787000 seconds]
  [Time since reference or first frame: 6.743877000 seconds]
  Frame Number: 3
  Frame Length: 24 bytes (192 bits)
  Capture Length: 24 bytes (192 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: user_dlt:mac-lte-framed:mac-lte:lte_rrc]
DLT: 147, Payload: mac-lte-framed (mac-lte-framed)
MAC-LTE PCH PDU (9 bytes)
  [Context (RNTI=65534)]
```

```
    [Radio Type: FDD (1)]
    [Direction: Downlink (1)]
    [System Frame Number: 533]
    [Subframe: 0]
    [RNTI: 65534]
    [RNTI Type: P-RNTI (1)]
    [Length of frame: 9]
    [CRC Status: OK (1)]
    [Carrier Id: Primary (0)]
  LTE Radio Resource Control (RRC) protocol
    PCCH-Message
      message: c1 (0)
        c1: paging (0)
          paging
            pagingRecordList: 1 item
              Item 0
                PagingRecord
                  ue-Identity: s-TMSI (0)
                    s-TMSI
                      mmec: 40 [bit length 8, 0100 0000 decimal value
                          ↪ 64]
                      m-TMSI: f3f3d379 [bit length 32, 1111 0011 1111
                          ↪ 0011 1101 0011 0111 1001 decimal value
                          ↪ 4092842873]
                  cn-Domain: ps (0)

Frame (24 bytes):
0000 01 01 01 02 ff fe 03 00 00 04 21 50 07 01 01 40 ..........!P...@
0010 04 0f 3f 3d 37 90 00 00 ..?=7...
Bitstring tvb (1 byte):
0000 40 @
Bitstring tvb (4 bytes):
0000 f3 f3 d3 79 ...y
No. Time Protocol
    4 2018-03-29 19:07:23,675645 MAC-LTE RAR (RA-RNTI=2, SFN=624 , SF
        ↪ =5) (RAPID=4: TA=16, UL-Grant=48204, Temp C-RNTI=2965)

Frame 4: 22 bytes on wire (176 bits), 22 bytes captured (176 bits)
  Encapsulation type: USER 0 (45)
  Arrival Time: Mar 29, 2018 19:07:23.675645000 Vest-Europa (
      ↪ sommertid)
```

```
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1522343243.675645000 seconds
  [Time delta from previous captured frame: 0.916079000 seconds]
  [Time delta from previous displayed frame: 0.916079000 seconds]
  [Time since reference or first frame: 7.659956000 seconds]
  Frame Number: 4
  Frame Length: 22 bytes (176 bits)
  Capture Length: 22 bytes (176 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: user_dlt:mac-lte-framed:mac-lte]
DLT: 147, Payload: mac-lte-framed (mac-lte-framed)
MAC-LTE RAR (RA-RNTI=2, SFN=624 , SF=5) (RAPID=4: TA=16, UL-Grant
    ↪ =48204, Temp C-RNTI=2965)
  [Context (RNTI=2)]
    [Radio Type: FDD (1)]
    [Direction: Downlink (1)]
    [System Frame Number: 624]
    [Subframe: 5]
    [RNTI: 2]
    [RNTI Type: RA-RNTI (2)]
    [Length of frame: 7]
    [CRC Status: OK (1)]
    [Carrier Id: Primary (0)]
  RAR Headers: (1 RARs)
    RAR Header: (RAPID=4)
      0... .... = Extension: 0x0
      .1.. .... = Type: RAPID present (0x1)
      ..00 0100 = RAPID: 0x04 (4)
    [Number of RAPIDs: 1]
  RAR Body: (RAPID=4: TA=16, UL-Grant=48204, Temp C-RNTI=2965)
    0... .... = Reserved: 0x0
    .000 0001 0000 .... = Timing Advance: 16
      [Expert Info (Note/Sequence): RAR Timing advance not zero (16)]
        [RAR Timing advance not zero (16)]
        [Severity level: Note]
        [Group: Sequence]
    .... 0000 1011 1100 0100 1100 = UL Grant: 48204
      .... 0... = Hopping Flag: 0
      .... .000 1011 110. = Fixed sized resource block assignment: 94
      .... ...0 010. .... = Truncated Modulation and coding scheme: 2
```

```
      ...0 11.. = TPC command for scheduled PUSCH: 0 dB (3)
      .... ..0. = UL Delay: 0
      .... ...0 = CQI Request: 0
    Temporary C-RNTI: 2965
  [Padding length: 0]

0000 01 01 02 02 00 02 03 00 00 04 27 05 07 01 01 44 ..........'....D
0010 01 00 bc 4c 0b 95 ...L..
No. Time Protocol
    5 2018-03-29 19:07:23,677832 LTE RRC UL_CCCH RRCConnectionRequest

Frame 5: 24 bytes on wire (192 bits), 24 bytes captured (192 bits)
  Encapsulation type: USER 0 (45)
  Arrival Time: Mar 29, 2018 19:07:23.677832000 Vest-Europa (
      ↪ sommertid)
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1522343243.677832000 seconds
  [Time delta from previous captured frame: 0.002187000 seconds]
  [Time delta from previous displayed frame: 0.002187000 seconds]
  [Time since reference or first frame: 7.662143000 seconds]
  Frame Number: 5
  Frame Length: 24 bytes (192 bits)
  Capture Length: 24 bytes (192 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: user_dlt:mac-lte-framed:mac-lte:lte_rrc]
DLT: 147, Payload: mac-lte-framed (mac-lte-framed)
MAC-LTE UL-SCH: (SFN=625 , SF=1) UEId=0 (Short BSR) (CCCH:remainder)
  [Context (RNTI=2965)]
    [Radio Type: FDD (1)]
    [Direction: Uplink (0)]
    [System Frame Number: 625]
    [Subframe: 1]
    [RNTI: 2965]
    [RNTI Type: C-RNTI (3)]
    [Length of frame: 9]
    [Uplink grant size: 9]
    [CRC Status: OK (1)]
    [Carrier Id: Primary (0)]
    [UL UE in TTI: 1]
  MAC PDU Header (Short BSR) (CCCH:remainder) [2 subheaders]
```

```
    Sub-header (lcid=Short BSR)
      0... .... = SCH reserved bit: 0x0
      .0.. .... = Format2: Data length is < 32768 bytes
      ..1. .... = Extension: 0x1
      ...1 1101 = LCID: Short BSR (0x1d)
    Sub-header (lcid=CCCH, length is remainder)
      0... .... = SCH reserved bit: 0x0
      .0.. .... = Format2: Data length is < 32768 bytes
      ..0. .... = Extension: 0x0
      ...0 0000 = LCID: CCCH (0x00)
  Short BSR (lcgid=0 BS = 0)
    00.. .... = Logical Channel Group ID: 0
    ..00 0000 = Buffer Size: BS = 0 (0)
  LTE Radio Resource Control (RRC) protocol
    UL-CCCH-Message
      message: c1 (0)
        c1: rrcConnectionRequest (1)
          rrcConnectionRequest
            criticalExtensions: rrcConnectionRequest-r8 (0)
              rrcConnectionRequest-r8
                ue-Identity: s-TMSI (0)
                  s-TMSI
                    mmec: 40 [bit length 8, 0100 0000 decimal value 64]
                    m-TMSI: f3f3d379 [bit length 32, 1111 0011 1111
                        ↪ 0011 1101 0011 0111 1001 decimal value
                        ↪ 4092842873]
                establishmentCause: mt-Access (2)
                spare: 00 [bit length 1, 7 LSB pad bits, 0... ....
                    ↪ decimal value 0]

Frame (24 bytes):
0000 01 00 03 02 0b 95 03 00 00 04 27 11 07 01 01 3d ..........'....=
0010 00 00 44 0f 3f 3d 37 94 ..D.?=7.
Bitstring tvb (1 byte):
0000 40 @
Bitstring tvb (4 bytes):
0000 f3 f3 d3 79 ...y
Bitstring tvb (1 byte):
0000 00 .
```