NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PROCESS FOR BREAKING DOWN THE LTE SIGNAL TO EXTRACT KEY INFORMATION

by

Chia Sern Wong

September 2013

Thesis Advisor:	Weilian Su
Co-Advisor:	Tri T. Ha

Approved for public release;distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE PROCESS FOR BREAKING DOWN THE LTE SIGNAL TO EXTRACT KEY INFORMATION		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Chia Sern Wong			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release;distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

The increasingly important role of Long Term Evolution (LTE) has increased security concerns among the service providers and end users and made security of the network even more indispensable. The main thrust of this thesis is to investigate if the LTE signal can be broken down in a methodical way to obtain information that would otherwise be private; e.g., the Global Positioning System (GPS) location of the user equipment/base station or identity (ID) of the user. The study made use of signal simulators and software to analyze the LTE signal to develop a method to remove noise, breakdown the LTE signal and extract desired information. From the simulation results, it was possible to extract key information in the downlink like the Downlink Control Information (DCI), Cell-Radio Network Temporary Identifier (C-RNTI) and physical Cell Identity (Cell-ID). This information can be modified to cause service disruptions in the network within a reasonable amount of time and with modest computing resources.

14. SUBJECT TERMS Long Term Evolution (LTE), Security, Vulnerabilities, Eavesdropping, Transmit Power Control, Physical Layer			**15. NUMBER OF PAGES** 89
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release;distribution is unlimited

PROCESS FOR BREAKING DOWN THE LTE SIGNAL TO EXTRACT KEY INFORMATION

Chia Sern Wong
Defence Science and Technology Agency, Singapore
B. Eng. (Computer Engineering), Nanyang Technological University, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ENGINEERING SCIENCE
(ELECTRICAL ENGINEERING)

from the

NAVAL POSTGRADUATE SCHOOL
September 2013

Author: Chia Sern Wong

Approved by: Weilian Su
Thesis Advisor

Tri T. Ha
Thesis Co-Advisor

R. Clark Robertson
Chair, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The increasingly important role of Long Term Evolution (LTE) has increased security concerns among the service providers and end users and made security of the network even more indispensable. The main thrust of this thesis is to investigate if the LTE signal can be broken down in a methodical way to obtain information that would otherwise be private; e.g., the Global Positioning System (GPS) location of the user equipment/base station or identity (ID) of the user. The study made use of signal simulators and software to analyze the LTE signal to develop a method to remove noise, breakdown the LTE signal and extract desired information. From the simulation results, it was possible to extract key information in the downlink like the Downlink Control Information (DCI), Cell-Radio Network Temporary Identifier (C-RNTI) and physical Cell Identity (Cell-ID). This information can be modified to cause service disruptions in the network within a reasonable amount of time and with modest computing resources.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

3G	Third Generation
3GPP	Third Generation Partnership Program
4G	Fourth Generation
ADC	Analog-to-Digital Converter
AKA	Authentication Key and Agreement
AM	Acknowledge Mode
AS	Access Stratum
BCCH	Broadcast Control Channel
BCH	Broadcast Channel
CAPEX	Capital Expenditure
CCCH	Common Control Channel
CCE	Control Channel Elements
CP	Cyclic Prefix
CRC	Cyclic Redundancy Code
C-RNTI	Cell RNTI
CSCF	Call Service Control Functions
DAC	Digital-to-Analog Converter
DCCH	Dedicated Control Channel
DCI	Downlink Control Information (DCI)
DL-SCH	Downlink Shared Channel
DoS	Denial of Service
DRX	Discontinuous Reception
DTCH	Dedicated Traffic Channel
DwPTS	Downlink Pilot Timeslot
EDGE	Enhanced Data rates for Global Evolution
eNB	Enhanced Node-B
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	UMTS Terrestrial Radio Access Network
FDD	Frequency Division Duplexing

FFT	Fast Fourier Transform
GP	Guard Period
GSA	Global mobile Suppliers Association
GSM	Global System for Mobile communications
HARQ	Hybrid Automatic Repeat Request
HeNB	Home eNB
HSDPA	High Speed Downlink Packet Access
HSPA	High Speed Packet Access
HSPA+	High Speed Packet Access Evolution
HSS	Home Subscriber Service
HSUPA	High Speed Uplink Packet Access
ICI	Inter-Carrier Interference
I-CSCF	Interrogating-CSCF
IFFT	Inverse Fast Fourier Transform
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IMT-Advanced	International Mobile Telecommunications Advanced
IP	Internet Protocol
IPSec	IP Security
ISI	Inter-Symbol Interference
ISIM	IMS Subscriber Identity Module
ITU-R	International Telecommunication Union-Radio
LTE	Long Term Evolution
LTE-A	LTE-Advanced
MAC	Medium Access Control
MBMS	Multimedia Broadcast Multicast Services
MCCH	Multicast Control Channel
MCH	Multicast Channel
MIB	Master Information Block
MIMO	Multiple-Input Multiple-Output
MiTM	Man in the Middle

MME	Mobility Management Entity
MTC	Machine Type Communication
MTCH	Multicast Traffic Channel
NAS	Non-Access Stratum
NCC	Next-hop Chaining Counter
OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
OPEX	Operational Expenditure
PAPR	Peak-to-Average Power Ratio
PBCH	Physical Broadcast Channel
PCCH	Paging Control Channel
PCH	Paging Channel
P-CSCF	Proxies-CSCF
PDCCH	Physical Downlink Control Channel
PDCP	Packet Data Convergence
PDN	Packet Data Network
PDSCH	Physical Downlink Shared Channel
P-GW	Packet Data Network Gateway
PHICH	Physical HARQ Indicator Channel
PMCH	Physical Multicast Channel
PRACH	Physical Radio Access Channel
PRB	Physical Resource Block
PSS	Primary Synchronization Signal
PUCCH	Packet Uplink Control Channel
PUSCH	Physical Uplink Shared Channel
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RACH	Random Access Channel
REG	Resource Element Groups
RF	Radio Frequency
RLC	Radio Link Control

RNC	Radio Network Controller
RNTI	Radio Network Temporary Identifier
RRC	Radio Resource Control
SAE	System Architecture Evolution
SC-FDMA	Single Carrier Frequency-Division Multiple Access
S-CSCF	Serving-CSCF
SDU	Service Data Unit
S-GW	Serving Gateway
SIB	System Information Block
SIP	Session Initiation Protocol
SQN	Sequence Number
SSS	Secondary Synchronization Signal
TDD	Time Division Duplexing
TM	Transparent Mode
TMSI	Temporary Mobile Subscriber Identity
TPC	Transmit Power Control
UE	User Equipment
UL-SCH	Uplink Shared Channel
UM	Unacknowledged Mode
UpPTS	Uplink Pilot Timeslot
UTMS	Universal Mobile Telecommunications System
VoIP	Voice over IP
W-CDMA	Wideband Code-Division Multiple Access
WiMAX	Worldwide Interoperability for Microwave Access

EXECUTIVE SUMMARY

The increasing use of data in the mobile environment has led to the need to develop fourth-generation (4G) technologies. In response, the Third Generation Partnership Program (3GPP) came together to develop the Long Term Evolution (LTE) standard. LTE is the current generation of mobile communications standard that is fast becoming the dominant global standard because of its flexibility and high data rates. However, the shift towards an all-IP packet based network in LTE has exposed mobile networks to new security challenges that did not threaten previous generations of mobile technology. With the growing number of implementations of LTE networks, the security of LTE technology has now become a critical area of research.

In this thesis, LTE is explored by expanding upon the architecture, security and technological aspects of the system. Different access technologies, protocol layers and the architectures used within LTE are elaborated on, including orthogonal frequency-division multiple access (OFDMA), single carrier frequency-division multiple access (SC-FCMA) and multiple-input multiple-output (MIMO).

A review of the literature regarding the related security vulnerabilities is discussed, with an in-depth look into the security of the LTE air interface. This includes an elaboration on passive and active air interface attacks like monitoring, jamming, insertion and modification of control signals.

Expanding on prior work, a method of attack on the air interface that allows the attacker to maliciously modify the Transmit Power Control (TPC) field in the Downlink Control Information (DCI) or cause the User Equipment (UE) to desynchronize with the enhanced Node-B (eNB) is proposed in this thesis. This study illustrates how an attacker can make use of unencrypted and unauthenticated physical layer control signals to disrupt services in an LTE network.

The proposed attack is made up of four stages. In stage one, the attacker accesses the network as a legitimate UE to obtain the cell specific parameters for the eNB. In stage two, the attacker eavesdrops on the air interface to scan for a victim UE's Cell Radio

Network Temporary Identifier (C-RNTI). In stage three, the attacker chooses either to carry out a targeted attack against a specific UE to change the TPC field maliciously or to broadcast a false synchronization signal, forcing all UEs within range to synchronize with the attacker's signal instead. Lastly, in stage four, he/she can then inject malicious DCI messages either to cause a single victim UE or a group of UEs to increase or decrease their transmit power unnecessarily.

A detailed explanation of how this attack may be accomplished by the attacker is presented and MATLAB tools are developed to simulate the required LTE signals. Based on the simulation of stage two, it was found that by using a brute force scan of the downlink signal, the attacker can obtain one or more UE's C-RNTI within a reasonable time frame of less than two hours. Similarly, broadcasting a false synchronization signal in stage three is possible but for a very limited range as the malicious signal requires at least 13 times the power of legitimate signal to overcome it.

For stage four, the simulation results also show that, on average, the malicious signal requires 1.57 times (single antenna configuration) and 11.13 times (multiple antenna configuration) the power of the eNB signal to be decoded accurately by the victim UE. In addition, it was noted that it requires significantly less power to command the UE to reduce its transmit power by sending the '01' bit combination. This indicates a possible weakness in the encoding of the DCI message within the downlink signal.

ACKNOWLEDGMENTS

I would like to express my heartfelt thanks my thesis advisors, Prof. Tri Ha and Prof. Weilian Su, for their guidance and motivation to complete this thesis.

I would also like to thank my wonderful wife, Esther, my family, and friends for their continuous support and understanding during my study in Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Long Term Evolution (LTE) belongs to the Global System for Mobile communications (GSM) path for mobile broadband, and evolved from Enhanced Data rates for Global Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), High Speed Packet Access (HSPA) and HSPA Evolution (HSPA+). The evolutionary path is illustrated in Figure 1.

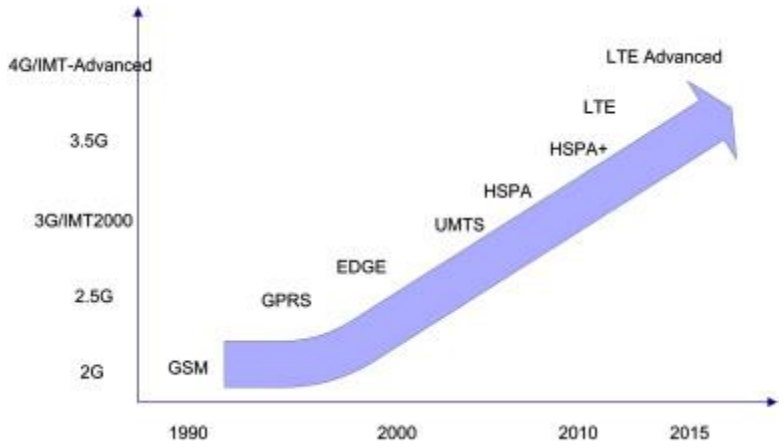

Figure 1. 3GPP family technology evolution. From [1].

GSM, the first digital cellular network standard, was introduced to the market in the 1990s. In the 2000s, it became apparent that data traffic was growing in popularity. This sparked the demand for third generation (3G) wireless networks. The first release of 3G in 2000 (Release 99) defines the Wideband Code-Division Multiple Access (W-CDMA) and UMTS standards. In 2001, UMTS evolved to Release 4, which added an all Internet Protocol (IP) core network and a maximum downlink speed of 384 kbps.

From 2002 to 2005, Release 5 and Release 6 (HSPA), introduced High Speed Downlink Packet Access (HSDPA) and the High Speed Uplink Packet Access (HSUPA), increasing the maximum downlink speed to 14 Mbps. This was marketed as “3.5G” wireless technology. Release 7 introduced HSPA+ (or Evolved HSPA) in 2007 and primarily dealt with the development of specifications like latency and Quality of Service

(QoS) improvement and real time applications with a doubled maximum downlink speed of 28 Mbps.

Although HSPA systems offered significant improvements in performance over previous systems, it was apparent that they were limited by a lack of backward compatibility with the original UMTS specification. In addition, UMTS technology was incompatible with the other 3G technology, CDMA. Globally, the use of these two technical standards effectively fragmented the market and forced operators to choose either one or the other, preventing the formation of a truly global operating standard. Together with the emergence of more advanced competing packet-based technologies like Worldwide Interoperability for Microwave Access (WiMAX), it became apparent that continuing to develop independent technologies based on UMTS and CDMA could not be sustained.

The concept of a new standard was discussed in detail in 2004 and resulted in a feasibility study launched by the Third Generation Partnership Program (3GPP) on the plausibility of designing and implementing in a timely way a high-speed packet optimized wireless data network with low latency and quick turnaround times. LTE fulfills these requirements by using an all-IP converged architecture, which is able to work across multiple access networks by allowing for a common IP based infrastructure. LTE was first introduced in 3GPP Release 8 in 2008, while Release 9 added System Architecture Evolution (SAE) enhancements and the interoperability of LTE and WiMAX. To ensure operators are able to migrate their networks and users smoothly to LTE, efforts were made to ensure LTE can coexist with HSPA and other previous networks with the scalable bandwidth functionality of LTE. LTE also introduced the use of orthogonal frequency-division multiplexing (OFDM), orthogonal frequency-division multiple access (ODFMA) and single carrier frequency-division multiple access (SC-FDMA).

Despite the increased performance of LTE, it still is not considered fully compliant with fourth generation (4G) requirements as defined in the International Mobile Telecommunications Advanced (IMT-Advanced) specification by the International Telecommunications Union-Radio communications sector (ITU-R). This

led to the development of the LTE-Advanced (LTE-A) Release 10 standard in 2011, which is backward compatible with LTE.

The comparison of peak data rates and other parameters among LTE-A, LTE and its predecessors are shown in Table 1.

Table 1. Parameters of LTE-A, LTE and its predecessors. After [2] and [3].

	WCDMA (UMTS)	**HSPA (HSDPA/HSUPA)**	**HSPA+**	**LTE**	**LTE-A**
Maximum downlink speed (bps)	384 k	14 M	28 M	100 M	1 G
Maximum uplink speed (bps)	128 k	5.76 M	11 M	50 M	200 M
Latency round trip time (approximate)	150 ms	100 ms	<50ms	~10 ms	<10 ms
3GPP releases	Rel. 99/4	Rel. 5/6	Rel. 7	Rel. 8	Rel. 10
Approximate years of initial roll out	2003/4	2005/6 HSDPA 2007/8 HSUPA	2008/9	2009-Present	N.A.
Access methodology	CDMA	CDMA	CDMA	OFDMA/ SC-FDMA	OFDMA/ SC-FDMA

There are many compelling reasons why operators are motivated to upgrade to LTE. These include user demand for higher data rates and QoS, a packet-switched optimized system, continued demand for reduced Capital and Operational Expenditures (CAPEX and OPEX), low complexity, and avoidance of unnecessary fragmentation of technologies for paired and unpaired band operation [4].

A report published by Global mobile Suppliers Association (GSA) dated May 10, 2013 [5], confirms that 371 LTE network deployments are planned or in progress in 116 countries, including 175 networks which are commercially launched in 70 countries.

The GSA report also highlights that a further 53 operators in ten countries have or are engaged in trials, technology testing or studies. This means a total of 424 operators in 126 countries are investing in LTE networks, suggesting that the operators worldwide are committed to LTE technology, with a forecast of 248 commercial LTE networks in 87 countries by the end of 2013. The countries with deployed LTE services are indicated in Figure 2.

Figure 2. 3GPP LTE evolution country map. From [6].

As can be seen, LTE is the next generation wireless data communications standard and is poised to become the 4G technology of choice for both commercial and military applications. With the growing number of implementations of LTE networks, the security of the technology cannot be ignored. For commercial applications, any security breaches can jeopardize the reputation and cause loss of revenue to a service provider. In military applications, security is an even greater concern as the integrity and accuracy of data are of utmost importance and any compromise may result in failure of the mission or loss of life.

B. PROJECT OBJECTIVE

With the increasing usage of the LTE standards, security within the LTE system is vital to ensure privacy and integrity of communications. Hence, the security and robustness of the LTE standard, especially that of its control channels, need to be further examined.

C. SCOPE OF THESIS

The scope of the thesis includes the review of the LTE protocol standards and an assessment of existing threats to the LTE system, followed by the development and use of MATLAB tools to simulate a method of manipulating the Physical Downlink Control Channel (PDCCH) without user knowledge. This thesis research can also serve as a guide to use MATLAB simulation tools for analyzing and testing security aspects of the LTE system.

D. APPROACH AND STRUCTURE

In Chapter II, the technical aspects of LTE are discussed, and technologies employed in LTE are explored. This is followed by a general overview of LTE architecture, LTE's security architecture, the different protocol layers and their interaction within the LTE network. Details of sub-layer protocols within the LTE network's Layer 2 protocol are also elaborated on.

Available literature related to security issues and security vulnerabilities is highlighted in Chapter III. The LTE specifications are also examined, and potential security weaknesses of the control channels within the LTE protocols are identified. The LTE trust model is presented as well.

In Chapter IV, the proposed method of manipulating LTE's PDCCH is presented, and the generation of the LTE signal using specifically developed MATLAB tools to simulate an attack on User Equipment (UE) is demonstrated. This chapter concludes by evaluating the feasibility of such an attack based on the simulation results.

In Chapter V, the results of the thesis are summarized and follow-on research areas related to the security of LTE are discussed.

THIS PAGE INTENTIONALLY LEFT BLANK

II. TECHNICAL BACKGROUND

A. OVERVIEW

Some technical aspects of 3GPP LTE are explained in this chapter. A brief description of the techniques used in the LTE physical layer to facilitate multiple access, namely OFDM, OFDMA, SC-FDMA and multiple-input multiple-output (MIMO), are discussed in Section B. This discussion is followed by an overview of the LTE architecture and the details of its Layer 1 and Layer 2 protocols.

The aim of this chapter is to provide readers with a brief technical background on LTE that aids them in understanding the problems discussed in the later chapters.

B. MULTIPLE ACCESS TECHNIQUES

The LTE physical layer (Layer 1) employs several technologies to communicate control and data information between the enhanced NodeB (eNB) and multiple UEs. These techniques include OFDM, OFDMA, SC-FDMA and MIMO transmission.

1. OFDM

OFDM is a method of encoding digital data using a large number of closely spaced orthogonal sub-carrier signals, which are used to carry data on several parallel data streams or channels. Each sub-carrier is modulated at a low symbol rate using a conventional modulation method such as quadrature phase-shift keying (QPSK) or quadrature amplitude modulation (QAM). The primary advantage of OFDM over traditional single-carrier schemes is its ability to cope with more severe channel conditions (like frequency-selective fading and narrowband interference) without the use of complex filters. This technique is used in LTE to overcome the multi-path fading problem common in urban deployments of cellular systems. A traditional single-carrier and an ODFM transmission in the frequency domain using the same bandwidth is depicted in Figure 3.

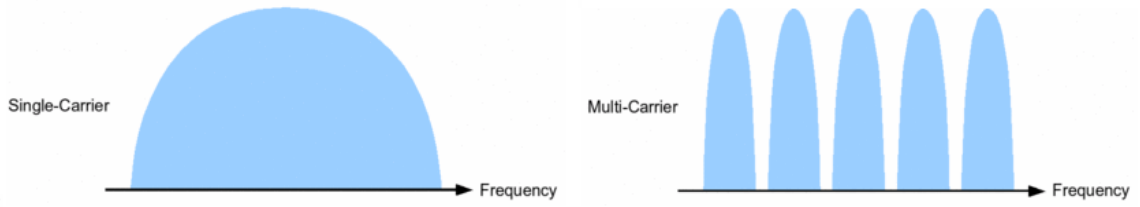

Figure 3. Single-carrier and OFDM transmissions represented in the frequency domain. From [7].

In a single-carrier system, the delay caused by multi-path transmission can result in a symbol from a delayed path to interfere with a subsequent symbol that arrived at the receiver via the shortest path. This effect is known as inter-symbol interference (ISI). For a single-carrier system, as the data rate increases, the symbol time decreases. This makes it possible for ISI to affect a second or even third subsequent symbol. To overcome this interference, single-carrier systems often use guard bands and complex equalization filters [8].

In an OFDM system, the sub-carrier frequencies for each channel are chosen so that they are orthogonal to each other. Hence, cross-talk between the channels is eliminated and inter-carrier guard bands are not required, greatly simplifying the design of the transmitter and receiver.

The generation of the OFDM signal is based on the inverse fast Fourier transform (IFFT), as illustrated in Figure 4, while the opposite, a fast Fourier transform (FFT), is carried out in the receiver to demodulate the signal. The IFFT converts a number of frequency domain symbol streams to an equal number of complex time domain samples which are then serialized to create the time domain signal.

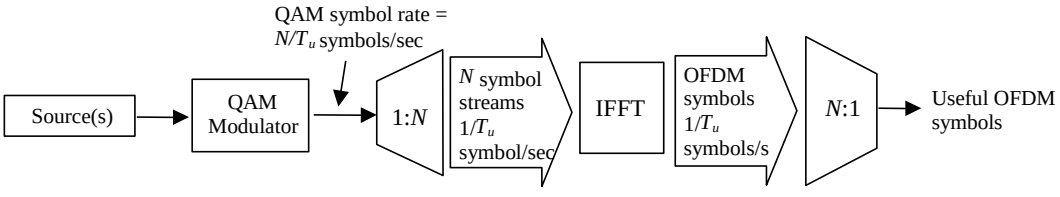

Figure 4. OFDM signal generation. From [9].

By splitting the high data rate stream into multiple low data rate parallel streams, the time per data symbol is relatively long compared to the channel time characteristics. This modification makes it feasible to insert a guard interval between each OFDM symbol, thus eliminating the ISI and the need for a pulse shaping filter. This guard interval is created by transmitting a cyclic prefix, which is a duplication of the end bits of the OFDM symbol equivalent to the length in time of the guard interval. The reason that the guard interval consists of a copy of the end of the OFDM symbol is so that the receiver can integrate over an integer number of sinusoid cycles for each of the multi-paths when it performs OFDM demodulation with the FFT [8].

OFDM, however, has two major weaknesses compared to single-carrier systems: OFDM is sensitive to sub-carrier frequency shifts, and it has a large signal peak-to-average power ratio (PAPR).

OFDM requires very accurate frequency synchronization between the receiver and the transmitter as any frequency deviation results in the sub-carriers no longer being orthogonal to one another, causing inter-carrier interference (ICI). Common causes of frequency deviations are Doppler shifts due to movement or by mismatched local oscillators in the transmitter and receiver. While Doppler shifts alone can usually be compensated for at the receiver, the combination of Doppler shifts and multi-path reflections (common in most cell phone urban usage scenarios) worsens the situation and limits the use of OFDM in high speed vehicles [8].

An OFDM signal exhibits a high PAPR because the independent phases of the sub-carriers (due to orthogonality) mean that they will often combine constructively. A high PAPR requires a high dynamic range analog-to-digital converter (ADC) and digital-to-analog converter (DAC) and reduces the efficiency of the transmitter's radio frequency (RF) power amplifier [8].

2. OFDMA

OFDMA is used in the downlink (eNB to UE) of the LTE system. OFDMA is a multi-user version of OFDM, where different users are served by different subsets of sub-carriers simultaneously, with each user allocated a specific time-frequency resource. An

illustration of how the different sub-carriers are used to serve different users at the same time is shown in Figure 5.

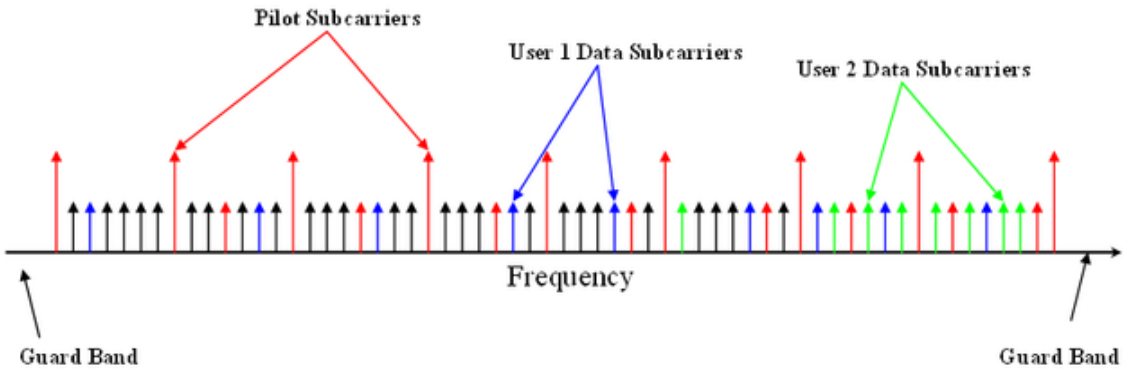

Figure 5. OFDMA subcarriers in the frequency domain. From [10].

OFDMA also allows for a different allocation of sub-carriers to users over time, allowing the network to allocate more sub-carriers dynamically to the users that require them. This feature allows for greater flexibility and efficiency in the utilization of the available frequency bandwidth.

3. SC-FDMA

As mentioned previously, one of the main weaknesses of OFDM (and OFDMA) is the high PAPR. To accommodate the high dynamic range required, a more complex and higher power transmitter is usually used. However, due to the size and power limitations of modern cell phones, a simpler, lower power transmitter is preferred, leading SC-FDMA to be used in the uplink for LTE instead of OFDMA [11].

Despite its name, SC-FDMA also uses multiple sub-carriers to transmit data. However, instead of grouping a number of bits together to form the signal for one sub-carrier, an additional processing block in SC-FDMA spreads the information of each bit over all the sub-carriers. This processing is done by first grouping a number of bits together (e.g., four bits in a 16-PSK modulation). In OFDM, these groups of bits would be the input of the IFFT; but in SC-FDMA, these bits are first put into a FFT function. The output of the FFT process is then put into the IFFT for the creation of the sub-

carriers, similar to OFDM [11]. The reverse is then performed on the receiver side (i.e., FFT followed by an additional IFFT). The result of the IFFT is a time-domain signal, which is fed to a single detector block to recreate the original bits. Therefore, unlike OFDM where the bits are detected on many different sub-carriers, only a single detector is used on the single-carrier output of the IFFT. The resulting difference in the frequency domain representations of OFDMA and SC-FDMA is shown in Figure 6, where each color represents a different set of data.

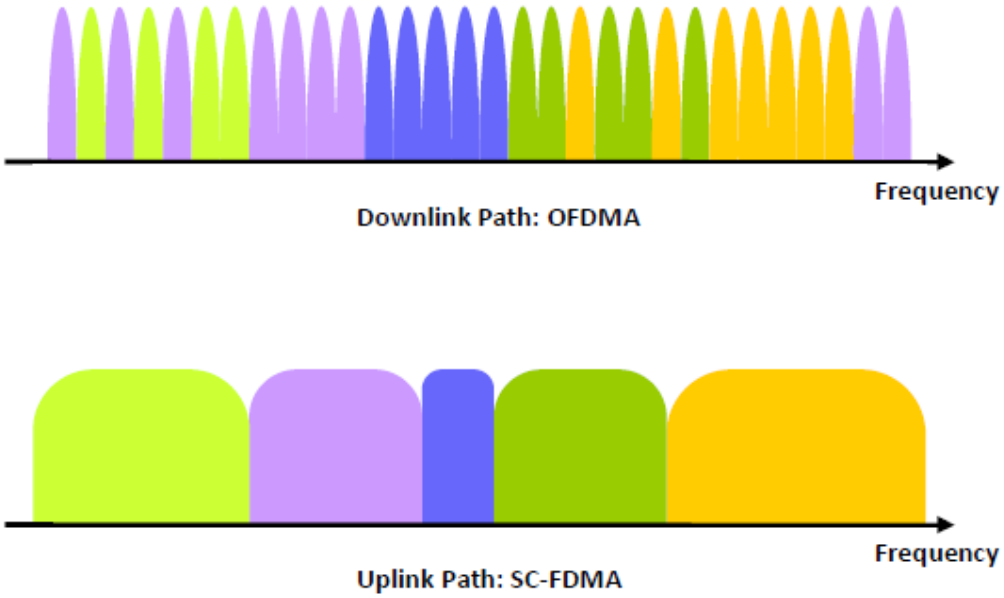

Figure 6. Frequency domain representation of OFDMA and SC-FDMA. From [12].

4. MIMO

In addition to OFDMA and SC-FDMA, MIMO is one of the primary techniques used to achieve the target throughput requirement of the LTE system. As its name implies, MIMO makes use of multiple antennas to transmit and receive data. LTE accommodates up to 4x4 MIMO (four transmitting antennas and four receiving antennas), which allows for up to four parallel streams of data to be transmitted simultaneously. The improved performance is achieved without additional bandwidth or an increase in transmission power. This performance improvement is made possible by dividing the same total transmission power over the multiple antennas to achieve an array

gain that improves the spectral efficiency (more bits per second per hertz of bandwidth) or to achieve a diversity gain that improves the link reliability [13].

MIMO can be used in two different modes, namely spatial multiplexing and diversity coding (or transmit diversity). In LTE, the MIMO mode is selected adaptively depending on the equipment (both eNB and UE) configuration and channel condition.

Spatial multiplexing allows for the transmission of multiple, parallel data streams simultaneously on the same downlink resource block [9] by transmitting and receiving each stream over a separate pair of antennas. In LTE, when all the data streams are allocated to a single user, it allows the user's peak data rate to be increased up to four times. Alternatively, the data streams can also be allocated to different users; this method increases the overall user capacity of a single eNB. However, because each antenna transmits a different stream of data, the channel conditions have to be relatively good.

When the channel conditions deteriorate, diversity coding can be used to increase the robustness of the data transmission instead. Diversity coding does this by transmitting the same data stream over the multiple antennas, allowing the signals to combine coherently. This process requires that multiple data streams (at least two) be allocated to the same user. As the antennas are physically separated, different channel impulse responses reduce the impact of fading that occurs on each of the antenna's signals, resulting in a greater SNR at the receiver.

A model of a MIMO channel is illustrated in Figure 7. In the spatial multiplexing mode, each of the transmitting antennas sends a different data stream (i.e., the three blue data streams, h_{11}, h_{21} and h_{31}, are different from the six other data streams). However, in diversity coding mode, the data sent on all nine streams is the same.

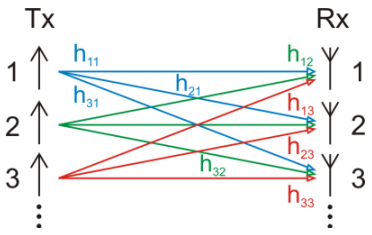

Figure 7. MIMO channel model. From [13].

C. PHYSICAL LAYER

1. Major Parameters

For the access scheme, LTE uses OFDMA for the downlink and SC-FDMA for the uplink. The major parameters for LTE are shown in Table 2.

Table 2. Major parameters for LTE. After [12].

Access Scheme	Uplink	DFTS-OFDM (SC-FDMA)
	Downlink	OFDMA
Bandwidth		1.4, 3, 5, 10, 15, 20 MHz
Sampling Frequency		1.92, 3.84, 7.68, 15.36, 23.04, 30.72 MHz
Frame Duration		10 ms
Sub-frame Duration		1 ms
Sub-carrier Spacing		15 kHz
Cyclic prefix (CP) length	Short	5.2 μs (first symbol), 4.7 μs (following 6 symbols)
	Long	16.7 μs
OFDM Symbols per Sub-frame	Short CP	7
	Long CP	6
Modulation		QPSK, 16QAM, 64QAM
Spatial multiplexing		Single layer for Uplink per UE Up to 4 layers for downlink per UE Multi-User MIMO supported for uplink and downlink

As can be seen from Table 2, the LTE physical layer specifications are flexible so as to enable deployments around the world and support as many regulatory requirements as possible.

2. Frame Structure

The LTE frame structure accommodates its two modes of operation: frequency-division duplexing (FDD) and time division duplexing (TDD). Each mode has its own frame structure defining the timing and symbol requirements that apply for both uplink and downlink transmissions.

The FDD mode uses the type 1 frame structure, which is shown in Figure 8. Each frame is 10 ms in duration and consists of 10 equal sub-frames, which are further divided into two slots of 0.5 ms duration each.

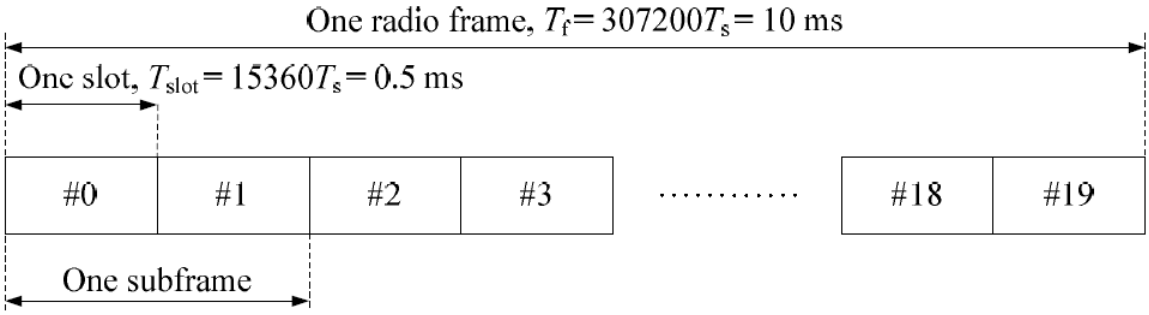

Figure 8. LTE type 1 frame structure. From [14].

The type 2 frame structure is used in the TDD mode and is shown in Figure 9. Similar to the type 1 frames, each type 2 frame is 10 ms in duration, divided into two half-frames. Each half-frame consists of five sub-frames, one of which may be required to be a special sub-frame depending on the downlink-to-uplink switch-point periodicity. The special sub-frame (if required) is made up of three fields: Downlink Pilot Timeslot (DwPTS), Guard Period (GP) and Uplink Pilot Timeslot (UpPTS).

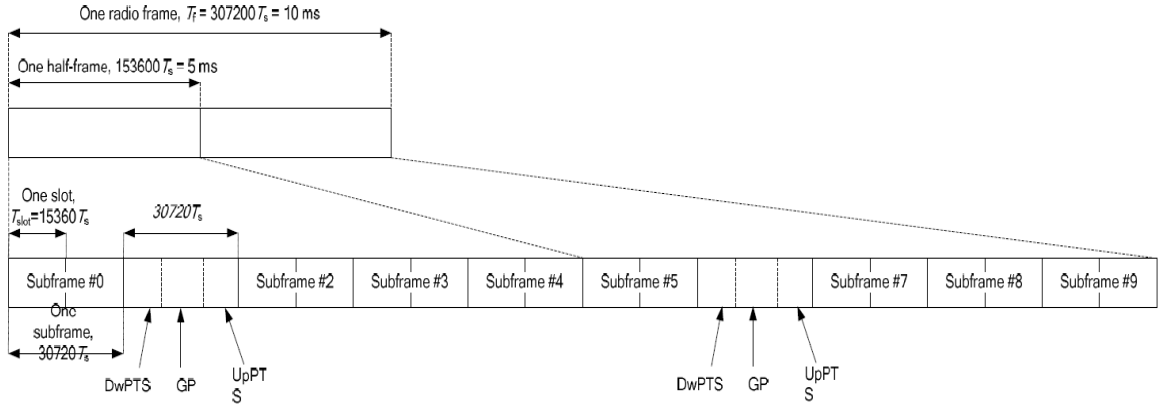

Figure 9. LTE frame structure type 2 (5-ms switch point periodicity). From [14].

The type 2 frame structure has seven different sub-frame format configurations. However, sub-frames 0, 5 and DwPTS are always reserved for downlink transmission, while the sub-frame after the special sub-frame and UpPTS are always assigned to uplink transmission. The various uplink-downlink configurations are shown in Table 3, where 'D' denotes a sub-frame reserved for downlink transmission, 'U' denotes a sub-frame reserved for uplink transmission, and 'S' denotes a special sub-frame.

Table 3. Uplink-downlink configuration for LTE frame structure type 2. From [14].

Uplink-downlink configuration	Downlink-to-Uplink Switch-point periodicity	Subframe number									
		0	1	2	3	4	5	6	7	8	9
0	5 ms	D	S	U	U	U	D	S	U	U	U
1	5 ms	D	S	U	U	D	D	S	U	U	D
2	5 ms	D	S	U	D	D	D	S	U	D	D
3	10 ms	D	S	U	U	U	D	D	D	D	D
4	10 ms	D	S	U	U	D	D	D	D	D	D
5	10 ms	D	S	U	D	D	D	D	D	D	D
6	5 ms	D	S	U	U	U	D	S	U	U	D

3. Frequency Bands

LTE uses all the frequency bands allocated for UMTS and extends the list to include newly allocated frequencies as shown in Table 4. Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) is the air interface of LTE. Each E-UTRAN operating band has a corresponding uplink operating band, downlink operating band and duplex mode.

Table 4. LTE operating bands. From [15].

E-UTRAN Operating Band	Uplink (UL) operating band BS receive UE transmit	Downlink (DL) operating band BS transmit UE receive	Duplex Mode
	$F_{UL\ low}$ -$F_{UL\ high}$	$F_{DL\ low}$ -$F_{DL\ high}$	
1	1920 MHz – 1980 MHz	2110 MHz – 2170 MHz	FDD
2	1850 MHz – 1910 MHz	1930 MHz – 1990 MHz	FDD
3	1710 MHz – 1785 MHz	1805 MHz – 1880 MHz	FDD
4	1710 MHz – 1755 MHz	2110 MHz – 2155 MHz	FDD
5	824 MHz – 849 MHz	869 MHz – 894MHz	FDD
6[1]	830 MHz – 840 MHz	875 MHz – 885 MHz	FDD

7	2500 MHz – 2570 MHz	2620 MHz – 2690 MHz	FDD
8	880 MHz – 915 MHz	925 MHz – 960 MHz	FDD
9	1749.9 MHz – 1784.9 MHz	1844.9 MHz – 1879.9 MHz	FDD
10	1710 MHz – 1770 MHz	2110 MHz – 2170 MHz	FDD
11	1427.9 MHz – 1447.9 MHz	1475.9 MHz – 1495.9 MHz	FDD
12	699 MHz – 716 MHz	729 MHz – 746 MHz	FDD
13	777 MHz – 787 MHz	746 MHz – 756 MHz	FDD
14	788 MHz – 798 MHz	758 MHz – 768 MHz	FDD
15	Reserved	Reserved	FDD
16	Reserved	Reserved	FDD
17	704 MHz – 716 MHz	734 MHz – 746 MHz	FDD
18	815 MHz – 830 MHz	860 MHz – 875 MHz	FDD
19	830 MHz – 845 MHz	875 MHz – 890 MHz	FDD
20	832 MHz – 862 MHz	791 MHz – 821 MHz	FDD
21	1447.9 MHz – 1462.9 MHz	1495.9 MHz – 1510.9 MHz	FDD
22	3410 MHz – 3490 MHz	3510 MHz – 3590 MHz	FDD
23	2000 MHz – 2020 MHz	2180 MHz – 2200 MHz	FDD
24	1626.5 MHz – 1660.5 MHz	1525 MHz – 1559 MHz	FDD
25	1850 MHz – 1915 MHz	1930 MHz – 1995 MHz	FDD
26	814 MHz – 849 MHz	859 MHz – 894 MHz	FDD
27	807 MHz – 824 MHz	852 MHz – 869 MHz	FDD
28	703 MHz – 748 MHz	758 MHz – 803 MHz	FDD
29	N/A	717 MHz – 728 MHz	FDD[2]
…			
33	1900 MHz – 1920 MHz	1900 MHz – 1920 MHz	TDD
34	2010 MHz – 2025 MHz	2010 MHz – 2025 MHz	TDD
35	1850 MHz – 1910 MHz	1850 MHz – 1910 MHz	TDD
36	1930 MHz – 1990 MHz	1930 MHz – 1990 MHz	TDD
37	1910 MHz – 1930 MHz	1910 MHz – 1930 MHz	TDD
38	2570 MHz – 2620 MHz	2570 MHz – 2620 MHz	TDD
39	1880 MHz – 1920 MHz	1880 MHz – 1920 MHz	TDD
40	2300 MHz – 2400 MHz	2300 MHz – 2400 MHz	TDD
41	2496 MHz – 2690 MHz	2496 MHz – 2690 MHz	TDD
42	3400 MHz – 3600 MHz	3400 MHz – 3600 MHz	TDD
43	3600 MHz – 3800 MHz	3600 MHz – 3800 MHz	TDD
44	703 MHz – 803 MHz	703 MHz – 803 MHz	TDD

NOTE 1: Band 6 is not applicable.
NOTE 2: Restricted to E-UTRA operation when carrier aggregation is configured. The downlink operating band is paired with the uplink operating band (external) of the carrier aggregation configuration that is supporting the configured Pcell.

4. Physical Resource Block and Resource Elements

A Physical Resource Block (PRB) is the smallest element of resource allocation assigned by the base station scheduler [14] and consists of 72 or 84 resource elements depending on the Cyclic Prefix (CP) mode, where each resource element corresponds to an OFDM symbol sub-carrier pair. Each PRB consists of 12 consecutive sub-carriers of constant spacing of 15 kHz each, occupying a total bandwidth of 180 kHz. A downlink slot consists of seven OFDM symbols when normal CP is employed or six OFDM symbols when long CP is employed. Hence, a PRB for a downlink slot using normal CP has seven columns of OFDM symbols and 12 rows of sub-carriers, resulting in 84 resource elements, as shown in Figure 10.

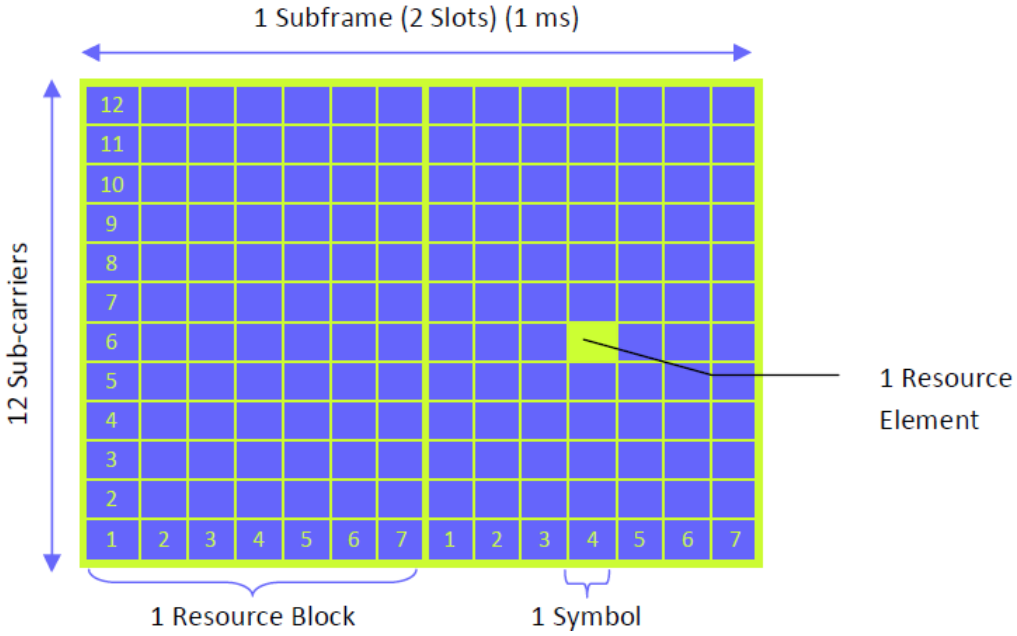

Figure 10. Illustration of a resource block and resource element. From [12].

To allow for variable bandwidths, the LTE specifications also define six sets of supportable bandwidths from 1.4 MHz to 20 MHz with corresponding sampling frequency, FFT size and number of PRBs required as shown in Table 5.

Table 5. LTE Parameters for different bandwidths. From [16].

Transmission Bandwidth	1.4 MHz	3 MHz	5 MHz	10 MHz	15 MHz	20 MHz
Sampling Frequency	1.92 MHz	3.84 MHz	7.68 MHz	15.36 MHz	23.04 MHz	30.72 MHz
FFT Size	128	256	512	1024	1536	2048
#RBs (12 subcarrier)	6	15	25	50	75	100 (110)

5. Synchronization Signals

As the LTE signal is broken down into frames, resource blocks and elements, there is a need for the UE and eNB to be synchronized to ensure that the data can be received correctly. In LTE, synchronization is achieved by the use of two synchronization signals transmitted at regular intervals in the downlink signal, namely the Primary Synchronization Signal (PSS) and the Secondary Synchronization Signal (SSS) [14].

a. PSS

When a UE wishes to connect to an eNB, it first searches for the PSS in the downlink signal to determine the timing of the slots and the cell identity. The PSS is based on a frequency-domain Zadoff-Chu sequence [17], which are codes that have zero cyclic autocorrelation at non-zero lags. This makes it ideal for use as a synchronization code as correlation between the received sequence and the set sequence is maximum at zero lag and zero otherwise. The PSS consists of 62 symbols mapped to the first 31 subcarriers on either side of the DC subcarrier. In the FDD frame format, the PSS is mapped to the last OFDM symbol of slots 0 and 10, while in the TDD frame format, it is mapped to the third OFDM symbol of sub-frames 1 and 6.

b. SSS

The SSS in the downlink signal is used by the UE to obtain the cell identity group, the cell identity within the group, the duplexing method used and the cyclic prefix length. The SSS is based on maximum length sequences [18], which are pseudo-random codes created by cycling through every possible state of a shift register of length x resulting in a sequence of length 2^x-1. Three such codes, each with 31 bits, are

then used to generate the SSS. The SSS is mapped to the same subcarriers and sub-frames as the PSS but transmitted one OFDM symbol earlier.

6. UE Uplink Power Control

Uplink power control determines the average power over a SC-FDMA symbol that the UE transmits over the physical channel [19]. The transmit power of the Physical Uplink Shared Channel (PUSCH) and Physical Uplink Control Channel (PUCCH) can be controlled independently. The objective of uplink transmit power control is to maintain the connection yet reduce the power consumption at the UE.

The power transmitted by the UE is controlled by a closed loop procedure between the eNB and the UE. This procedure is done for every sub-frame. The eNB signals the UE if there is a need to adjust its uplink transmit power by the use of the Transmit Power Control (TPC) command in the PDCCH [19]. The UE then determines the correct transmit power based on the procedure outlined in the following sub-sections.

a. Power control of PUSCH

The power control calculation in the PUSCH is done sub-frame by sub-frame and determined using three possible equations depending on the conditions in which the sub-frame is transmitted.

The first equation is used when the UE transmits a sub-frame with PUSCH but without PUCCH for the serving cell *c*. In such a case, the UE transmit power $P_{PUSCH,c}(i)$ for the PUSCH transmission in sub-frame *i* for the serving cell *c* is given by

$$P_{PUSCH,c}(i) = \min\left\{\begin{array}{c} P_{CMAX,c}(i), \\ 10\log_{10}(M_{PUSCH,c}(i)) + P_{O\_PUSCH,c}(j) + \alpha_c(j)\cdot \mathrm{PL}_c + \Delta_{TF,c}(i) + f_c(i) \end{array}\right\}[\mathrm{dBm}], \quad (2.1)$$

where

- $P_{CMAX,c}(i)$ is the maximum configured UE transmit power in sub-frame *i* for serving cell *c* in dBm,
- $M_{PUSCH,c}(i)$ is the bandwidth of the PUSCH resource assignment expressed in number of resource blocks valid for sub-frame *i* and serving cell *c*,

- $P_{O\_PUSCH,c}(j)$ and $\Delta_{TF,c}(i)$ are parameters determined by higher layers for the serving cell c for j=0 and 1,
- PL_c is the downlink path loss estimate calculated in the UE for serving cell c in dB,
- for j=0 or 1, $\alpha_c \in \{0, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1\}$ and is selected by higher layers for serving cell c , for j=2, $\alpha_c(j) = 1$, and
- $f_c(i)$ is the current PUSCH power control adjustment state for serving cell c. The value of $f_c(i)$ is determined by the TPC command and if accumulation is enabled by higher layers.

  If accumulation is enabled,

$$f_c(i) = f_c(i-1) + \delta_{PUSCH,c}(i - K_{PUSCH}), \tag{2.2}$$

  else

$$f_c(i) = \delta_{PUSCH,c}(i - K_{PUSCH}), \tag{2.3}$$

  where

  - $K_{PUSCH} \in \{4,5,6,7\}$ depending upon the duplexing mode, and
  - $\delta_{PUSCH,c}$ depends on the TPC command and the Downlink Control Information (DCI) format according to Tables 6 and 7.

Table 6. Mapping of TPC command field in DCI format 0/3/4 to accumulated and absolute $\delta_{PUSCH,c}$ values. From [19].

TPC Command in DCI format 0/3/4	**Accumulated $\delta_{PUSCH,c}$ [dB]**	**Absolute $\delta_{PUSCH,c}$ [dB] only DCI format 0/4**
0	-1	-4
1	0	-1
2	1	1
3	3	4

Table 7. Mapping of TPC command field in DCI format 3A to accumulated $\delta_{PUSCH,c}$ values. From [19].

TPC Command in DCI format 3A	**Accumulated $\delta_{PUSCH,c}$ [dB]**
0	-1
1	1

The second case occurs if the UE transmits PUCCH simultaneously with the PUSCH in the sub-frame *i* for the serving cell *c*. Then the transmit power $P_{PUSCH,c}(i)$ for the PUSCH is given by

$$P_{PUSCH,c}(i) = \min\begin{Bmatrix} 10\log_{10}(\hat{P}_{CMAX,c}(i) - \hat{P}_{PUCCH}(i)), \\ 10\log_{10}(M_{PUSCH,c}(i)) + P_{O\_PUSCH,c}(j) + \alpha_c(j)\cdot \mathrm{PL}_c + \Delta_{TF,c}(i) + f_c(i) \end{Bmatrix}[\mathrm{dBm}], \quad (2.4)$$

where $\hat{P}_{CMAX,c}(i)$ is the linear value of $P_{CMAX,c}(i)$, and $\hat{P}_{PUCCH}(i)$ is the linear value of $P_{PUCCH}(i)$ defined in sub-section C-6-b.

Lastly, if the UE is not transmitting PUSCH in the sub-frame *i* for the serving cell *c*, then the UE transmit power $P_{PUSCH,c}(i)$ is computed using

$$P_{PUSCH,c}(i) = \min\begin{Bmatrix} P_{CMAX,c}(i), \\ 10\log_{10}(P_{O\_PUSCH,c}(j) + \alpha_c(j)\cdot \mathrm{PL}_c + f_c(i)) \end{Bmatrix}[\mathrm{dBm}]. \quad (2.5)$$

b. Power control in PUCCH

Similar to the PUSCH, the transmit power control calculation for the PUCCH is done on a sub-frame basis. There are two possible values for the transmit power value depending on the situation.

The first equation is used if the serving cell *c* is the primary cell. For this scenario, the UE transmit power $P_{PUCCH}(i)$ for the PUCCH transmission in sub-frame *i* is calculated using

$$P_{PUCCH}(i) = \min\begin{Bmatrix} P_{CMAX,c}(i), \\ P_{0\_PUCCH} + PL_c + h(n_{CQI}, n_{HARQ}, n_{SR}) + \Delta_{F\_PUCCH}(F') + \Delta_{TxD}(F') + g(i) \end{Bmatrix}[\mathrm{dBm}], \quad (2.6)$$

where

- $P_{CMAX,c}(i)$ is the maximum configured UE transmit power in sub-frame *i* for serving cell *c* in dBm,
- the parameters P_{0_PUCCH}, $\Delta_{\mathrm{F\_PUCCH}}(F)$ and $\Delta_{TxD}(F')$ are provided by higher layers,
- $h(n_{CQI}, n_{HARQ}, n_{SR})$ depends on the PUCCH format,

- PL_c is the downlink path loss estimate calculated in the UE for serving cell c in dB, and
- $g(i) = g(i-1) + \sum_{m=0}^{M-1} \delta_{PUCCH}(i - k_m)$ and is the current PUCCH power control adjustment state for serving cell c (the values of M and k_m depend on the duplexing method used and δ_{PUCCH} values depend on the TPC command according to Tables 8 and 9).

Table 8. Mapping of TPC command field in DCI format 1A/1B/1D/1/2A/2B/2C/2D/2/3 to δ_{PUCCH} values. From [19].

TPC Command Field in DCI format 1A/1B/1D/1/2A/2B/2C/2D/2/3	δ_{PUCCH} **[dB]**
0	-1
1	0
2	1
3	3

Table 9. Mapping of TPC Command Field in DCI format 3A to δ_{PUCCH} values. From [19].

TPC Command Field in DCI format 3A	δ_{PUCCH} **[dB]**
0	-1
1	1

If c is not the primary cell and the accumulation of the TPC command is received with DCI format 3/3A, then the UE transmit power $P_{PUCCH}(i)$ for the PUCCH transmission in sub-frame i is given by

$$P_{PUCCH}(i) = \min\left\{ \begin{array}{c} P_{CMAX,c}(i), \\ P_{0\_PUCCH} + PL_c + g(i) \end{array} \right\} [\text{dBm}]. \qquad (2.7)$$

D. NETWORK ARCHITECTURE AND PROTOCOLS

1. Network Architecture

The LTE architecture comprises three main building blocks, namely the UE, access network and the Evolved Packet Core (EPC). This is shown in Figure 11. The UE represents the user's mobile device that is used to access network services, and the access network is simply a network of base stations (eNBs) resulting in a flat architecture.

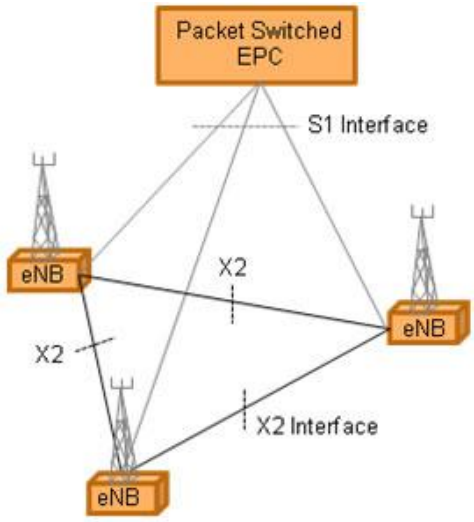

Figure 11. LTE network architecture. From [4].

The EPC is the core network in the LTE/SAE system. The EPC is composed of logical nodes, namely the Packet Data Network Gateway (P-GW), Serving Gateway (S-GW) and Mobility Management Entity (MME). The S-GW acts as a local mobility anchor, forwarding and receiving packets to and from the eNB serving the UE. The P-GW interfaces with external Packet Data Networks (PDN) such as the Internet.

The MME is a signaling only entity, which means that IP data packets do not go through the MME. The MME is mainly responsible for overall access control of the UE, S-GW/P-GW selection and management of the bearers.

In LTE, all the network interfaces are based on IP. The eNBs are interconnected by means of an X2 interface and to the EPC by means of an S1 interface. The functional split between the eNB (E-UTRAN) and the EPC is shown in Figure 12.

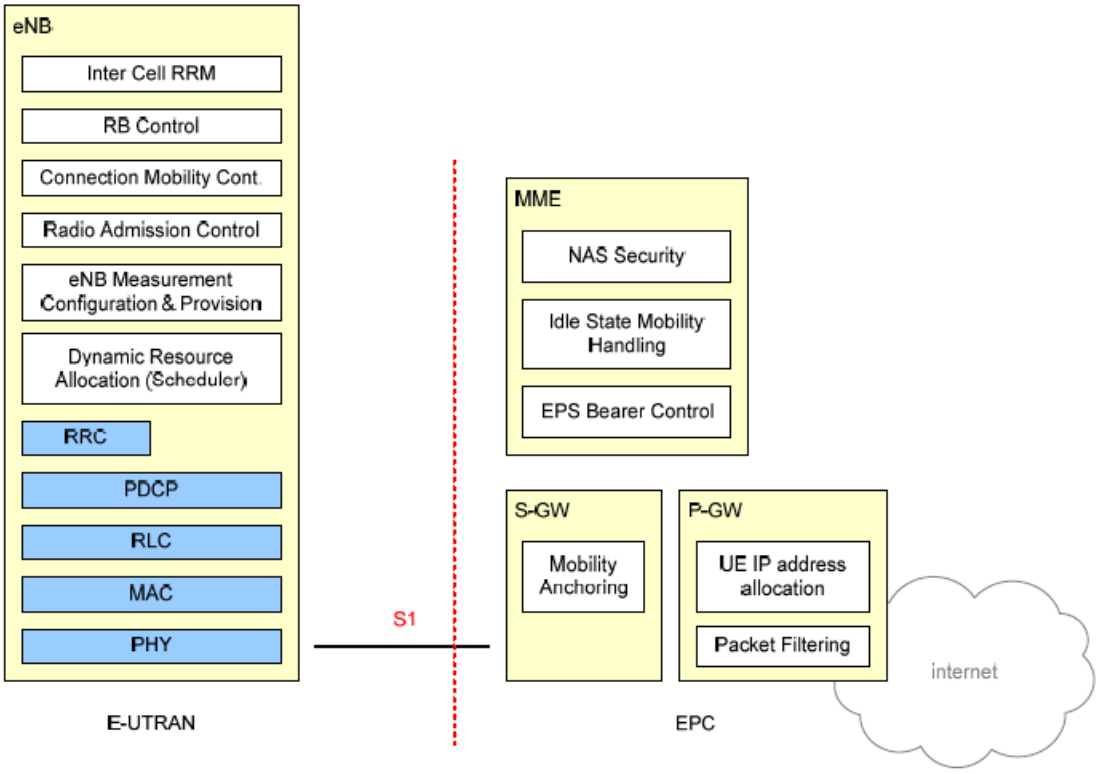

Figure 12. Functional split between eNB and EPC. From [20].

The eNB implements traditional Node-B functions as well as protocols previously implemented in the Radio Network Controller (RNC), removing the need for a centralized controller. The main reason for distributing the intelligence amongst the eNBs is to speed up the connection set-up and reduce the time required for a handover. The time for a handover is essential for real-time services where end-users tend to experience dropped calls or simply hang-up if the handover takes too long [4].

2. Layer 2 Protocols

Layer 2 of LTE consists of three sub-layers, namely Packet Data Convergence Protocol (PDCP), Radio Link Control (RLC) and Medium Access Control (MAC). The relationships and data flow among the three sub-layers, the upper IP layer and lower physical layer are shown in Figure 13.

The PDCP sub-layer performs functions such as header compression and decompression, ciphering and in-sequence delivery and duplicate detection at handover

for RLC. The RLC sub-layer functions include segmentation, in-sequence delivery and duplicate detection, while the MAC sub-layer performs multiplexing of logical channels on to the transport channels and de-multiplexing MAC data units between the physical and RLC sub-layer. As the main concentration of this thesis is on the physical layer, only the functions of the lower two sub-layers (RLC and MAC) are further elaborated.

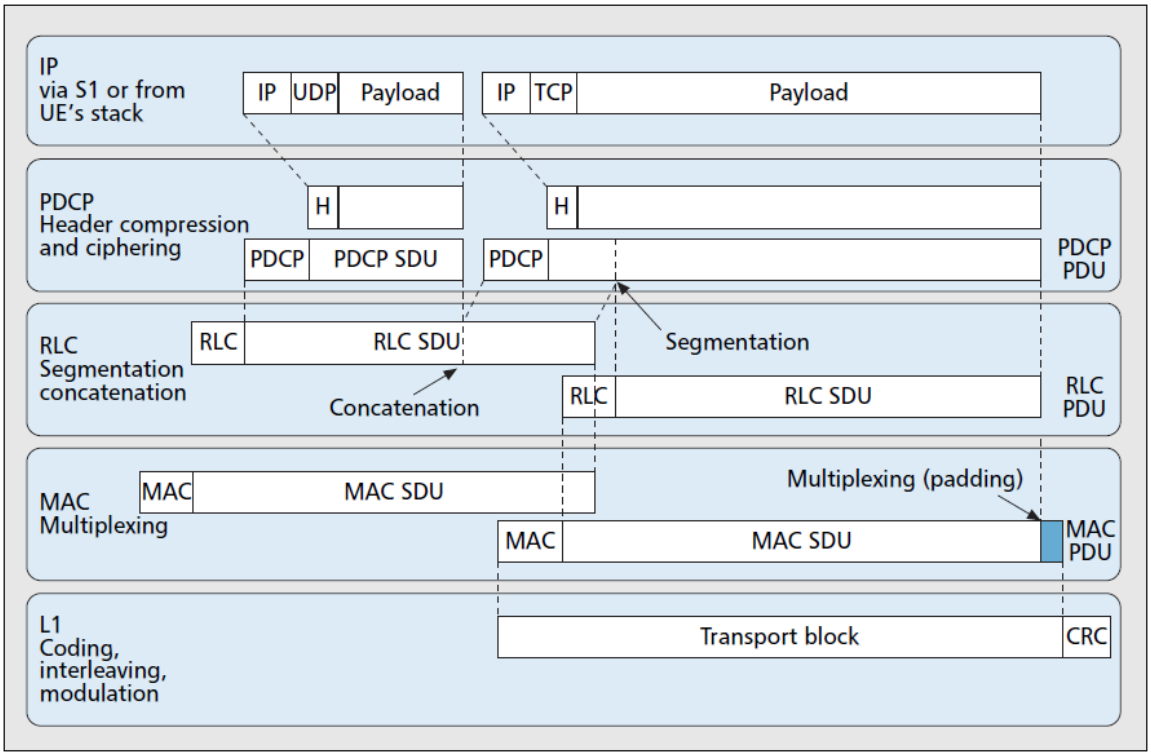

Figure 13. Illustration of data flow through layer 2 protocol stack. From [21].

a. RLC sub-layer

The RLC layer does protocol error detection and recovery and functions as the interface between the PDCP layer and the MAC layer. An overview of the RLC sub-layer is shown in Figure 14.

The RLC layer can be configured in three different modes for data transfer: Acknowledged (AM), Unacknowledged (UM) and Transparent (TM). The RLC performs a number of functions depending on the mode it is in. Under UM, it does concatenation, segmentation and reassembly of RLC SDUs, reordering of RLC data

PDUs, duplicate detection and RLC SDU discard. AM differs from UM in that it requires the receiver to acknowledge the receipt of the RLC PDU. This acknowledgement is done using a type of control PDU called the STATUS PDU. This allows AM to have all the functions under UM plus error correction through ARQ and re-segmentation of RLC data PDUs. AM also prioritizes the retransmission of data over new data.

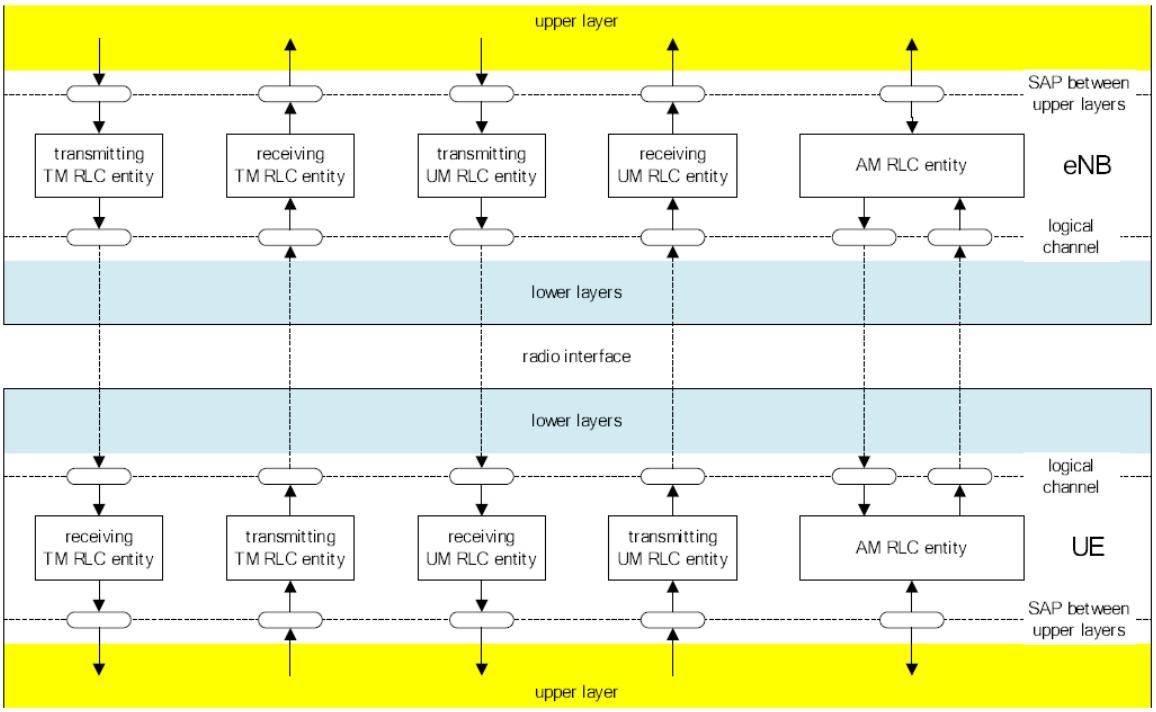

Figure 14. Overview model of RLC sub-layer. From [22].

In the TM, there is no segmentation and reassembly of RLC SDUs, no RLC headers added and no guarantee of delivery.

b. MAC sub-layer

The MAC layer is mainly responsible for the mapping of logical channels to the appropriate transport channels and the multiplexing and de-multiplexing MAC Service Data Units (SDU) between the physical and RLC layer. This mapping is done for both the uplink and downlink.

The relationship between the downlink logical, transport and physical channels is shown in Figure 15. A logical channel is defined by the type of information it carries–either control or traffic.

In the downlink there are five logical control channels and two logical traffic channels. The five logical control channels are Paging Control Channel (PCCH), Broadcast Control Channel (BCCH), Common Control Channel (CCCH), Dedicated Control Channel (DCCH) and Multicast Control Channel (MCCH).

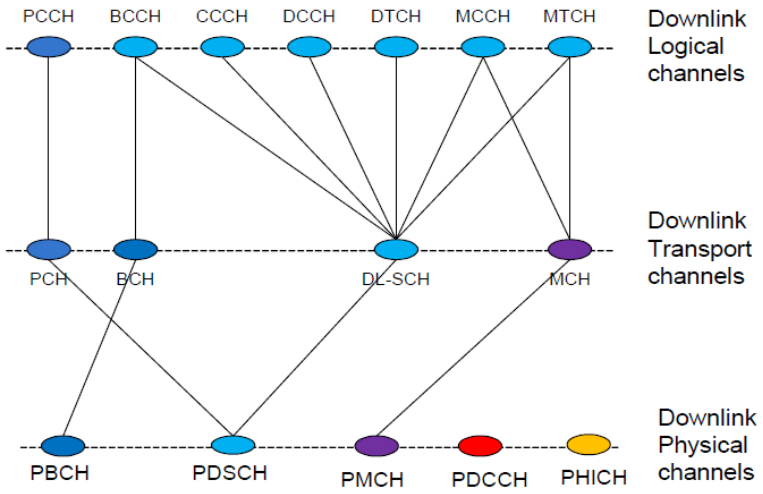

Figure 15. Downlink logical, transport and physical channels mapping. From [23].

As their names suggest, the PCCH is used for paging information transfer when searching for a UE, and the BCCH is used for broadcasting system control information. The CCCH and DCCH are both used for transmitting control information between the UEs and the network. However, the CCCH is used when the UEs have no Radio Resource Control (RRC) connection with the network, while the DCCH is a point-to-point channel used when the UEs have RRC connection with the network. The MCCH is a point-to-multipoint channel used for transmitting Multimedia Broadcast Multicast Services (MBMS) information needed for multicast reception.

The two logical traffic channels are the Dedicated Traffic Channel (DTCH) and Multicast Traffic Channel (MTCH). Both are used for transmitting user traffic, but the DTCH is a point-to-point channel dedicated to a single UE, while the

MTCH is a point-to-multipoint channel used for transmission of user traffic to UEs receiving MBMS.

The seven logical channels are then mapped to one or more of the four downlink transport channels—Paging Channel (PCH), Broadcast Channel (BCH), Multicast Channel (MCH) and Downlink Shared Channel (DL-SCH).

The PCH, BCH and MCH are all broadcast over the entire cell coverage area to support various functions. The PCH supports UE discontinuous reception (DRX) to enable UE power saving, the BCH broadcasts a fixed pre-defined transport format and the MCH supports multicast-broadcast single frequency network (MBSFN) combining of MBMS transmission on multiple cells. The DL-SCH is optionally broadcast in the cell coverage area. It supports adaptive modulation/coding, hybrid automatic repeat request (HARQ), power control, resource allocation, DRX, MBMS and multi-antenna beam-forming technologies.

The four downlink transport channels are further mapped into one of five physical downlink channels—Physical Downlink Shared Channel (PDSCH), Physical Downlink Control Channel (PDCCH), Physical HARQ Indicator Channel (PHICH), Physical Broadcast Channel (PBCH) and Physical Multicast Channel (PMCH).

Each physical channel serves a specific function and is modulated depending on the configuration of the upper layers. The PDSCH carries the DL-SCH and PCH and is modulated using QPSK, 16-QAM and 64-QAM. The PDCCH carries resource allocation information of PCH and DL-SCH, HARQ information and uplink scheduling grant to the UE using QPSK modulation. The PHICH carries HARQ acknowledgments (ACK) or negative acknowledgments (NACK) and is modulated using QPSK. The PBCH carries the BCH information in a fixed format of four sub-frames within a 40 ms interval. Each sub-frame is independently self-decodable and is modulated using QPSK. Lastly, the PMCH carries the MCH information and is modulated using QPSK, 16-QAM and 64-QAM.

The method by which the six downlink physical channels are then mapped onto the downlink physical resource block before being transmitted over the air is described in Chapter IV.

The MAC layer also multiplexes the uplink logical to transport channels in a similar manner. The relationship between the uplink logical, transport and physical channels is shown in Figure 16.

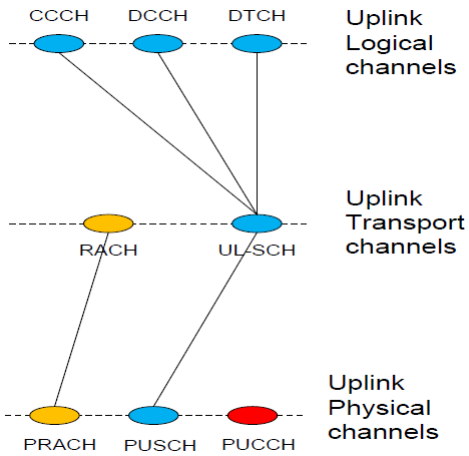

Figure 16. Uplink logical, transport and physical channels mapping. From [23].

There are two logical control channels and one logical transport channel in the uplink, namely the Common Control Channel (CCCH), the Dedicated Control Channel (DCCH) and the Dedicated Traffic Channel (DTCH). Similar to the downlink, the CCCH and DCCH are both used for transmitting control information between the UEs and the network. However, the CCCH is used when the UE has no RRC connection, while the DCCH is a point-to-point channel used when the UEs have RRC connection with the network. The DTCH is the only logical transport channel and is a point-to-point channel used for the transfer of user data for one UE.

The three logical channels are then mapped to one of the two uplink transport channels—the Random Access Channel (RACH) and the Uplink Shared Channel (UL-SCH). The RACH used for limited transmission of control information from UE with the possibility of collisions in the channel. This channel is used when a UE

first joins a network and has not acquired the settings to transmit on the UL-SCH. The UL-SCH is used for information on adaptive modulation/coding, HARQ, power control and resource allocation after the UE is synchronized with the network.

The two transport channels are further mapped into one of three physical uplink channels—the Physical Radio Access Channel (PRACH), the PUSCH and PUCCH. The PRACH and the PUSCH are the physical channels used to carry the RACH and the UL-SCH, respectively. The PUCCH, on the other hand, is used to carry downlink channel quality indication (CQI) reports, scheduling requests (SR) and HARQ ACK/NACKs for downlink transmissions.

3. Radio Resource Control

The RRC layer [24] is part of the LTE air interface control plane. This layer is responsible for the broadcast of system information related to both the Non-Access-Stratum (NAS) and Access Stratum (AS). It performs RRC control such as paging, establishment, modification and release of RRC connection, radio configuration and QoS control. Other functions performed by the RRC layer are inter-radio access technologies mobility, measurement configuration and reporting, generic protocol error handling and support of self-configuration and self-optimization.

E. LTE SECURITY

The LTE/SAE security architecture [25] is designed to provide secure communications for control signaling and the user data between the different entities of the LTE. An overview of the security architecture is shown in Figure 17.

Similar to the 3G security architecture, five security feature groups (or levels I, II, III, IV and V) are defined. Each of these levels aims to meet certain threats and accomplishes certain security objectives. Level I is network access security and provides UEs with secure access to the network, protecting it against attacks on the radio link. Level II is network domain security used to protect against attacks on the wired portion of the network and enables nodes to exchange signalling and user data in a secure manner. The next level (level III) represents user domain security and secures access to

mobile stations, while level IV, application domain security, enables applications in the UEs and the provider domain to securely exchange messages. Lastly, level V, visibility and configurability of security, enables the UE to inform the user whether a security feature is in operation and whether the use and provision of services should depend on the security feature.

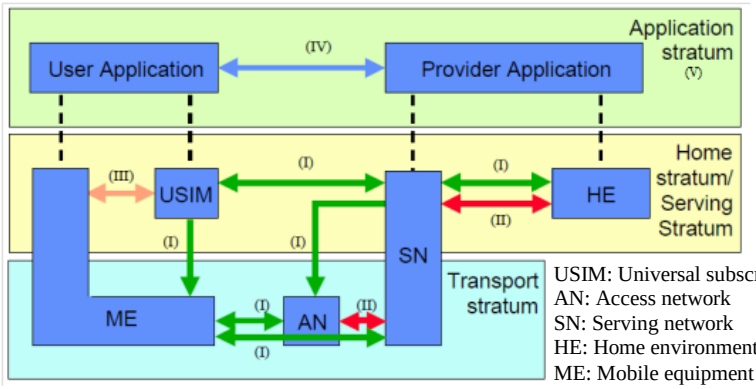

Figure 17. Overview of the LTE security architecture. From [25].

The LTE trust model is presented in Figure 18. As can be seen from the figure, the area around the eNB and the air interface from the eNB to the UE are considered non-trusted areas. Hence, the LTE network can be seen as a secure core network with a radio access network and connecting interfaces that are vulnerable to attack.

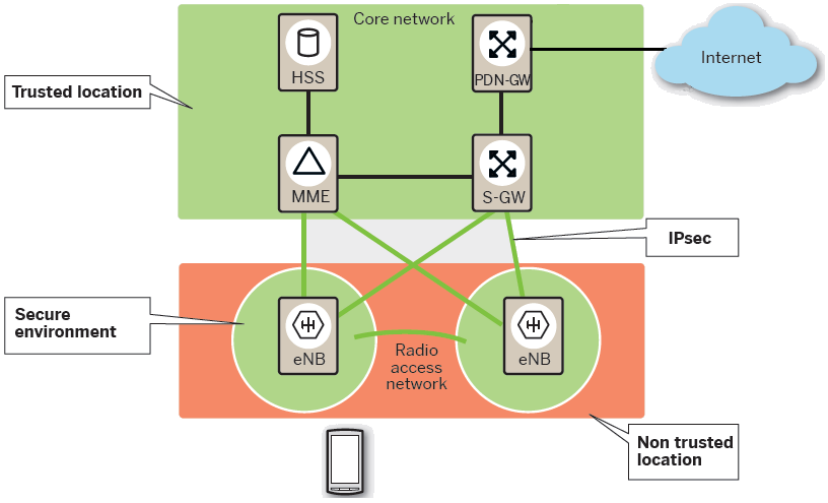

Figure 18. LTE trust model. From [26].

As the focus of this thesis is on the LTE air interface signal, only the network access security feature group is discussed in greater detail. The network access security can be broken down into six aspects: cellular security, handover security, IP Multimedia Subsystem (IMS) security, Home eNB (HeNB) security, Machine Type Communication (MTC) security and air interface security.

1. Cellular Security

LTE requires mutual authentication between the UE and the MME in the EPC. This authentication is achieved using the Evolved Packet System (EPS) Authentication and Key Agreement (AKA) procedure. Under EPS AKA, the Home Subscriber Server (HSS) generates a root key from which a key hierarchy is derived using cryptographic functions. The keys in this hierarchy are used to protect signaling and user data traffic between the UE and network.

Keys derived from the root key cannot be used to deduce the root key or sibling keys and are bound to where, how and for which purpose they are used. This feature prevents an attacker from compromising an entire network if he manages to obtain one of the derived keys or from using a key from one network to compromise another. Furthermore, the key hierarchy and bindings allow for the routine changing of keys for a certain use (e.g., securing communications between the UE and eNB) without impacting other services (e.g., communications between the UE and the EPC) or having to change the root key.

Once the UE and EPC are mutually authenticated, control and user data traffic between the parties are protected by use of Internet Key Exchange/IP Security (IKE/IPSec) or other integrity, replay protection and encryption mechanisms.

2. Handover Security

When a UE moves between two eNBs, a handover of security parameters occurs between the source eNB to the destination eNB. In addition, there may be a need to reestablish security should the source eNB be compromised (forward security) or maintain security should the destination eNB be compromised (backward security). This

process is shown in Figure 19, where the source eNB is eNB1 and destination eNB is eNB2.

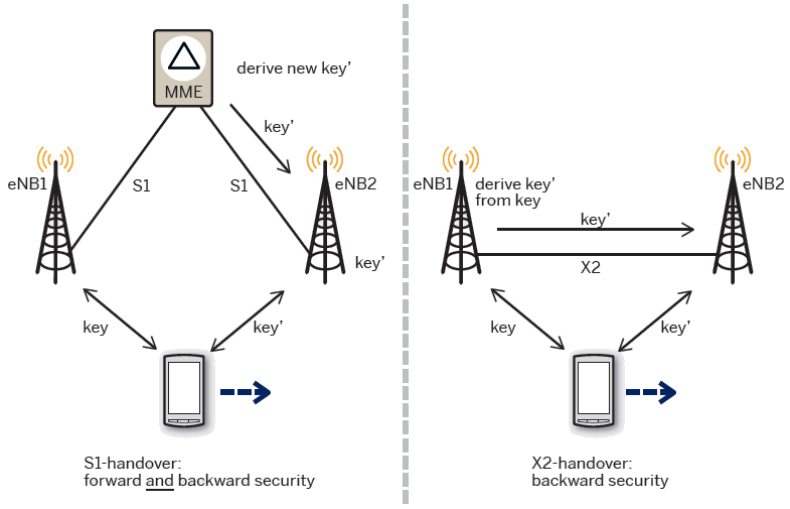

Figure 19. Handover security process. From [26].

Handovers between LTE and legacy 3GPP systems or LTE and non-3GPP systems are also protected in a similar way. If the destination network is trusted, the security context may be transferred over from the source LTE network to reduce the number of times the UE is required to be authenticated and to reduce the handover time.

However, if the destination network is not trusted or the security context cannot be transferred, then a re-authentication of the UE and network occurs. The exact authentication process differs depending on the scenario and types of networks involved.

3. IMS Security

IMS is an overlay architecture that provides LTE networks with multimedia services. The IMS authentication keys and processes are stored in the IMS Subscriber Identity Module (ISIM) in the UE.

For a user to access multimedia services, the UE has to be authenticated at both the LTE network and IMS layers. The main entities in the IMS are the Session Initiation Protocol (SIP) proxies and the Call Service Control Functions (CSCF). The CSCF consists of Proxies-CSCF (P-CSCF), Interrogating-CSCF (I-CSCF) and Serving-CSCF (S-CSCF).

Upon receiving a request from an UE, the P-CSCF redirects and forwards the SIP message to the I-CSCF within the UE's home network. The I-CSCF contacts the HSS for an appropriate S-CSCF to send the registration request to. The selected S-CSCF then replies the HSS with a request to obtain the user's authentication data to authenticate the UE and provide the session control of the multimedia services.

4. HeNB Security

The HeNB is a low cost, low power femtocell that can be installed by a subscriber to increase indoor coverage for the LTE signal. The HeNB connects to the EPC through a HeNB gateway over the Internet via the broadband backhaul. Similar to the eNB, the HeNB supports network access security and UE access security.

5. MTC Security

MTC is the communication between the entities within the LTE network without human interaction. The MTC devices can communicate with the MTC servers or with other MTC devices directly via the LTE networks. There are three security areas for the MTC security architecture: security between the MTC device and the network; security between the network and the MTC server, user or application; and security between the MTC server, user or application and the MTC device. In an LTE network, the MME represents the network to carry out mutual authentications with the MTC device via the EPS AKA procedure.

6. Air Interface Security

Under LTE the physical layer air interface between the UE and eNB does not inherently perform any security measures in terms of encryption or authentication. These functions are left to the higher layers to manage. However, the air interface does employ encoding and scrambling using Radio Network Temporary Identifier (RNTI) [14]. While this feature helps to conceal the information, it is still possible to decode and unscramble the signal to obtain the information within.

III. LTE SYSTEM SECURITY VULNERABILITES

A. OVERVIEW

Research for the development of LTE began in 2004; however, the majority of research into the LTE protocols came only after the release of the first version LTE standard by 3GPP in 2008. This literature review concentrates on materials discussing possible vulnerabilities in the LTE system. To date a number of public research papers have been released on the security of LTE; however, as LTE is relatively new, only a limited number of security exploitations have been discussed extensively in the published literature.

An overview of the network access security vulnerabilities is presented in Section B followed by further elaboration on the LTE air interface security vulnerabilities in Section C.

B. NETWORK ACCESS SECURITY VULNERABILITIES

A comprehensive summary of threats against LTE/LTE-A is provided in [27]. These threats target vulnerabilities in the LTE system architecture, access procedure, handover procedure, the IMS security mechanism, the HeNB security mechanism and the MTC security architecture. The vulnerabilities are discussed in further detail in the following paragraphs.

1. System Architecture Vulnerabilities

The IP-based architecture of the LTE system and the use of Voice over IP (VoIP) expose LTE to security risks that affect all IP-based networks (e.g., address spoofing, packet monitoring and injection, Denial-of-Service (DoS) attacks) that would be less likely in previous 3GPP networks that were not based on IP [28]. The flat nature of the architecture also makes the base stations more susceptible to attacks as a single MME station serves multiple base stations, while in the traditional UTMS architecture, the serving network only manages two base stations [27].

The introduction of a new small, low-cost base station (HeNB) for coverage of indoor environments exposes the LTE system to additional security risks. Due to the size and cost of HeNB, it can be easily obtained by attackers who can then use it to conduct possible Man-in-the-Middle (MiTM) attacks on the network. The use of HeNBs also requires the network to implement separate handover authentication procedures for HeNB to eNB mobility scenarios, which adds additional complexity and exposes the network to more threats [27].

2. Access Procedure Vulnerabilities

The LTE system uses EPS AKA to provide access security. While this process is an improvement over the AKA mechanism, there are still some instances where private information is sent in the clear. An example is the sending of the International Mobile Subscriber Identity (IMSI) in plaintext by the UE when the UE registers to a network for the first time or when there is some error during the follow up processes [29].

The EPS AKA scheme is also unable to prevent DoS attacks that can possibly overwhelm the network. For example, an attacker could impersonate a UE to send fake IMSIs repeatedly to overwhelm the HSS. It has also been highlighted in [29] that the EPS AKA scheme has a number of security issues like the lack of perfect forward security, lack of sequence number synchronization and susceptibility to MiTM attacks.

3. Handover Procedure Vulnerabilities

There are three possible vulnerabilities in the handover procedure. The first is the possible lack of backward security. Since a key hierarchy is used, the source eNB may choose to derive new keys for multiple destination eNBs from the current key. Hence, if the current eNB is compromised and the current key is obtained, then further derived keys are no longer secure [27].

The second possibility is the vulnerability to service disrupting replay attacks [27]. If the attacker can intercept an encrypted handover request message from a UE, then when the UE wants to move out of the current eNB, the attacker can replay the collected message to the destination eNBs. The destination eNB decodes the message and replies

with a Next-hop Chaining Counter (NCC) value corresponding to the replayed message. Upon receiving this value, the UE's NCC check fails as it does not correspond to the correct NCC value. The UE then initiates a new handover procedure, delaying the transition and possibly disrupting services to the user.

The last possibility is to force a handover. As the UE decides which eNB to connect to based on the signal power it receives from each candidate eNB, it is possible to force a handover of the UEs in a target area to switch to a compromised eNB by broadcasting a more powerful signal than that of the legitimate eNBs [30].

4. IMS Vulnerabilities

To provide the multimedia services, the IMS is connected to the Internet directly. This connection exposes it to a number of attacks despite the use of the IMS AKA procedure.

The IMS security mechanism is vulnerable to several types of signaling attacks [31]. As described in Chapter II, for the UE to be authenticated on the IMS system, the P-CSCF/MME sends a request to the I-CSCF/S-CSCF/HSS with the UE's IMSI. An attacker can possibly flood the I-CSCF/S-CSCF/HSS by impersonating the P-CSCF/MME and sending correct packets with invalid IMSI.

The requirement for the UE to authenticate using both EPS and IMS AKAs means additional complexity and energy consumption for the UE [32]. The IMS AKA also lacks key security features like sequence number (SQN) synchronization required to prevent MiTM attacks.

5. HeNB Security Vulnerabilities

As the purpose of the HeNB is for users to be able to enhance indoor coverage in homes or small offices, ease of set-up is the main concern. Hence, the physical and cyber security measures are comparatively less demanding than a standard eNB. This poses a number of security threats to the HeNB, the UEs and the network.

Due to the reduced physical security around the HeNB, the HeNB cannot be considered a trusted party. Together with the lack of a vigorous mutual authentication

procedure between the UE and the HeNB, the current HeNB security architecture cannot prevent various attacks including eavesdropping attacks, MiTM and masquerading attacks [33]. Also, because the interfaces to the core network are usually via the Internet, the HeNB is vulnerable to Internet-based attacks.

The next vulnerability is the links between the UE and the HeNB and the backhaul between the HeNB and the EPC. These are susceptible to many kinds of attacks because they can be insecure wireless links, making the data and conversations vulnerable to interception and eavesdropping [34].

6. MTC Security Vulnerabilities

The MTC lacks security schemes for the communication between the MTC applications and the MTC devices and the MTC applications and the network.

MTC devices tend to be small and have relatively low computational power. This makes them susceptible to several attacks such as physical attacks, compromise of credentials and protocol attacks. In addition, it is possible to create high signaling overhead between the HSS and the MME by simulating simultaneous authentication of a large number of MTC devices [27], possibly overwhelming the entities or the network.

C. AIR INTERFACE SECURITY VULNERABILITIES

The air interface describes the wireless connection between the UE and eNB or HeNB in the network. Security in the air interface is of particular concern because there is no way to prevent attackers from monitoring, intercepting or jamming the wireless signal between the entities since it is transmitted over public space.

Attacks on the air interface can be classified into two categories: passive or active. Passive attacks occur when the attacker only eavesdrops on the communications between the mobile device and the base station, without interfering or transmitting any data. Active attacks occur when the attacker not only listens in on the communication but jams the signal, modifies the data or injects a new message.

1. Passive Air Interface Attacks

Despite efforts to secure the air interface using encryption, passive attacks, such as traffic analysis and user tracking, may still be possible. LTE requires the use of random temporary identifiers, such as the RNTI and Temporary Mobile Subscriber Identity (TMSI), to protect the identity of individual UEs over the air interface. However, because TMSIs are usually not changed in a given tracking area, which may be composed of up to a hundred cells, an attacker may be able to track the movements of a UE over a number of cells. The deployment of HeNBs exacerbates this vulnerability as the range of the HeNB is typically in the range of 10 meters, allowing for a high level of accuracy in tracking the movements of a UE [35].

2. Active Air Interface Attacks

Although modifying user data in the air interface is difficult due to cryptographic measures taken by the higher layers, it may still be possible to modify or disrupt physical layer services.

a. Jamming

The first possible attack is the jamming of the air interface [36]. While jamming an entire eNB signal (i.e., barrage jamming) would be difficult and power consuming, an attacker can possibly jam select key control or synchronization signals to achieve the same effect. By jamming only the center 62 subcarriers of the LTE downlink (instead of all 128 to 2048 sub-carriers), the attacker would be able to prevent the UE from detecting the PSS and SSS signals, effectively denying the UE from accessing the eNB in that cell. Similarly, an attacker could choose to jam only the PUCCH, which is essential for the synchronizing of uplink requests and transmit power adjustments, thus causing service disruption for multiple UEs.

Alternatively, as presented in [37], an attacker can exploit the correlation between non-orthogonal carriers in carrier aggregated or bonded channels to cause a service disruption.

b. Insertion of false PSS

As the PSS is required for the UE to synchronize with the downlink signal, there is no way to protect it cryptographically. Hence, it is possible to cause UEs to synchronize to a wrong timing by broadcasting a false PSS signal [36]. If the attack is successful, the UEs misses the correct slot timing of the eNB, which results in the UEs being unable to connect to the legitimate network, and the UEs decode the attackers false downlink signal instead. The exploitation of this vulnerability is explored in the next chapter.

c. Modification of Layer 2 control signals

Although most data is encrypted on the downlink and uplink signals, there are some control signals that remain in the clear. This opens up the possibility that the control signals can be maliciously modified. Some possibilities are highlighted in [38], namely, the modification of the control PDU type field and the false request to retransmit data.

The control PDU of the RLC has a 3-bit type field. Currently, only type 000 (STATUS PDU) is defined, while the remaining combinations (001–111) are reserved. An attacker could cause a legitimate STATUS PDU to be dropped by the recipient if he could modify the type field to anything other than 000. Since the STATUS PDU is used to acknowledge receipt of data PDUs, an RLC transmitter would assume that the receiver did not receive the data PDUs and would wrongly retransmit them.

The RLC layer operating in AM prioritizes retransmissions over sending of new data. An attacker could also exploit this by sending false negative acknowledgement in the STATUS PDU, resulting in the transmitter wrongly retransmitting already received data PDUs.

d. Monitoring and modification of RRC messages

The RRC has a number of messages that are sent in plaintext before and after the UE is authenticated. A list of 22 RRC messages that are sent unencrypted and unauthenticated is shown in Table 10.

Table 10. List of unauthenticated plaintext RRC messages. From [24].

No.	Message	Purpose	Direction
1	CSFBParametersRequestCDMA2000	To obtain the CDMA2000 1xRTT Parameters from the network to generate the registration message to join the network	UE to network
2	CSFBParametersResponseCDMA2000	To provide the CDMA2000 1xRTT Parameters to the UE so the UE can register with the network	Network to UE
3	DLInformationTransfer	For the downlink transfer of NAS or non-3GPP dedicated information	Network to UE
4	MasterInformationBlock	System information transmitted on BCH	Network to UE
5	MBMSCountingRequest	To count the UEs that are receiving or interested in receiving specific MBMS services	Network to UE
6	MBMSInterestIndication	To inform network that the UE is receiving/ interested in receiving or no longer receiving/ interested in receiving MBMS via an MRB	UE to network
7	MBSFNAreaConfiguration	Contains the MBMS control information applicable to an MBSFN area	Network to UE
8	MeasurementReport	For the indication of measurement results	UE to network
9	Paging	For the notification of one or more UEs	UE to network
10	RRCConnectionReconfiguration	Command to modify an RRC connection	Network to UE
11	RRCConnectionReconfigurationComplete	To confirm the successful completion of an RRC connection reconfiguration	UE to network
12	RRCConnectionReject	To reject the RRC connection establishment	Network to UE
13	RRCConnectionRelease	To command the release of an RRC connection	Network to UE
14	RRCConnectionRequest	To request the establishment of an RRC connection	UE to network
15	RRCConnectionSetup	To establish SRB1	Network to UE
16	RRCConnectionSetupComplete	To confirm the successful completion of an RRC connection establishment	UE to network
17	SecurityModeCommand	To command the activation of AS security	Network to UE
18	SystemInformation	To convey one or more System Information Blocks.	Network to UE
19	SystemInformationBlockType1	Contains information relevant when evaluating if a UE is allowed to access a cell and defines the scheduling of other system information	Network to UE
20	UECapabilityEnquiry	To request the transfer of UE radio access capabilities for network as well as for other RATs	Network to UE
21	UECapabilityInformation	To transfer of UE radio access capabilities requested by the network	UE to network
22	ULInformationTransfer	For the uplink transfer of NAS or non-3GPP dedicated information	UE to network

As the RRC is an essential control channel for the LTE system, if an attacker can manipulate the information in the messages, he can easily disrupt the communications between the UE and the network. A possible example is an attacker injecting a false RRCConnectionRelease message into the link, causing the UE to unknowingly drop its RRC connection with the network and causing a service disruption.

e. Modification of physical layer control signals

Under LTE, the physical layer also performs a number of procedures to maintain the stability of the radio link. One of these procedures is the UE TPC mechanism. The TPC in LTE consists of an explicit 2-bit control field in the DCI that requires the UE to increase or reduce its transmit power. Therefore, an attacker could modify the TPC field to falsely require the UE to increase or decrease its transmit power [38]. This modification would result in either the UE wasting unnecessary energy transmitting at a higher power than required or in losing uplink with the eNB if the transmit power is reduced below the threshold required for maintaining the link. The exploitation of this TPC vulnerability is further elaborated on and explored in the next chapter.

IV. BREAKING DOWN THE LTE SIGNAL

A. OVERVIEW

The LTE physical layer air interface is made up of procedures and channels that are used by the network and the UE to transmit user data and control information. The physical layer design is greatly influenced by the requirements of 4G networks for high peak transmission rates, spectral efficiency and multiple channel bandwidths.

This chapter delves deeper into the physical layer procedures of the LTE system, specifically the PDCCH, explains how this is simulated in MATLAB and explores how the information within the downlink signal can possibly be exploited. The proposed attack methodology is detailed in Section B. This is followed in Section C by an explanation of how the DCI and RNTI are encoded and decoded and how an attacker can use this scheme to extract information. The decoding process of the PDCCH is elaborated on in Section D, while an explanation of how an attacker can generate a false PDCCH signal is provided in Section E. Lastly, details on the simulation results and an evaluation of the feasibility of such an attack are presented in Section F.

B. PROPOSED ATTACK METHODOLOGY

The attack proposed in [38] is expanded upon and its feasibility investigated in this chapter. It is suggested that the attacker perform the message injection attack on the victim UE in four stages.

1. Stage 1: Obtaining Cell Parameters

As LTE operates on a synchronized uplink and downlink, any attacker must pose as a valid UE to obtain the cell synchronization timing via the PSS and SSS. This enables the attacker to obtain cell specific parameters like the Cell-Identity (Cell-ID), Master Information Block (MIB) and System Information Block 1 and 2 (SIB1 and SIB2).

This information allows the attacker to further access the network to obtain uplink power control protocol-related information like the Cell RNTI (C-RNTI), TPC-PUSCH-RNTI and TPC-PUCCH-RNTI. The C-RNTI is assigned by the eNB to each UE to allow

the UE to decode control information addressed to it. Hence, by obtaining a C-RNTI value, the attacker can use it to guess the C-RNTI of other legitimate UE as the eNB may issue the C-RNTI in a sequential manner.

2. Stage 2: Obtaining C-RNTI of Other UEs

After obtaining synchronization with the network, the attacker can then begin to monitor the network to obtain other legitimate UE's C-RNTI. This can be done in two ways—namely, monitoring the cell for handover commands or using a sequential search. A C-RNTI is assigned to a UE during a cell handover; hence, an attacker could monitor the network to obtain a C-RNTI of a new UE to the cell. However, this involves the attacker waiting for an unknown period of time till a new UE joins the cell.

Alternatively, the attacker can carry out a sequential search brute force attack. By utilizing the C-RNTI obtained in stage 1, the attacker can potentially reduce the search region to a few thousand values. Details on how the attacker can decode the legitimate signal are expanded in Section C and D of this chapter.

3. Stage 3: Calculating the Signal Delay

For the attacker to utilize the minimum power to overcome the legitimate eNB signal, he/she has to ensure that the false signal arrives at the UE synchronized with the legitimate eNB signal [38]. This reduces the amount of destructive interference between the two signals. To do so, the attacker needs to estimate the distance of the user from himself/herself. As each symbol takes up 1/14 ms in time, the attacker needs to be able to synchronize within this small time window.

To mitigate the need for this estimation, the attacker could position himself/herself close to the eNB such that the time difference of signal arrivals would be minimal. Alternatively, as described in Chapter III, the attacker could generate a false downlink signal containing the PSS and SSS of the legitimate signal, forcing all UEs within a certain range to synchronize with the attacker instead. However, both these mitigation methods require the attacker to broadcast at higher power levels as the false signal needs to overcome the eNB signal.

4. Stage 4: Injection of False Messages

Using the information obtained in stages 1 and 2, the attacker can now create a false downlink signal with a malicious DCI message. Once the attacker has identified a victim UE and (if required) determined the appropriate delay, he/she can begin to broadcast the false downlink signal using a HeNB to trick a victim UE (using a Format 0 DCI message encoded with its C-RNTI) or a group of UEs (using a Format 3/3A DCI message encoded with the TPC-PUSCH-RNTI or TPC-PUCCH-RNTI) into changing the uplink transmit power. The victim UE then synchronizes to the new signal and decodes the malicious DCI information, causing it to either increase its transmit power as suggested in [38] or reduce its transmit power causing service disruption. Details on the creation of the false message are explained in Sections C and E of this chapter.

C. DCI AND RNTI

1. DCI

The DCI is the information encoded within the PDCCH and serves to allow the eNB to send control information to the UE. The various DCI formats, respective purposes and RNTI used to scramble the CRC are shown in Table 11.

Table 11. DCI formats, purposes and RNTI used to scramble CRC. From [39].

DCI Format	Purpose	RNTI used
Format 0	For transmission of uplink scheduling (UL-SCH) assignments	C-RNTI
Format 1	For transmission of downlink scheduling (DL-SCH) assignments for single antenna operation	C-RNTI
Format 1A	For the compact transmission of DL-SCH assignments for single antenna operation	C-RNTI, RA-RNTI, P-RNTI, SI-RNTI
Format 1B	Support closed-loop single-rank transmission with possibly contiguous resource allocation	C-RNTI
Format 1C	For downlink transmission paging, RACH response and dynamic BCCH scheduling	C-RNTI
Format 1D	For the compact transmission of DL-SCH assignments with pre-coding and power offset information.	C-RNTI
Format 2/2A/2B/2C	For the transmission of DL-SCH assignments MIMO operation	C-RNTI
Format 3	For the transmission of TPC commands for PUSCH and PUCCH with 2 bit power adjustments	TPC-PUSCH-RNTI, TPC-PUCCH-RNTI
Format 3A	For the transmission of TPC commands for PUSCH and PUCCH with 1 bit power adjustments	TPC-PUSCH-RNTI, TPC-PUCCH-RNTI

The selection of DCI format is done by the higher layers, depending on the type of information required to be sent. The DCI message generated is then affixed with a Cyclic Redundancy Code (CRC) that is scrambled by the required RNTI.

Several processing steps are taken to encode the DCI message into a PDCCH channel. A flowchart of these steps is shown in Figure 20.

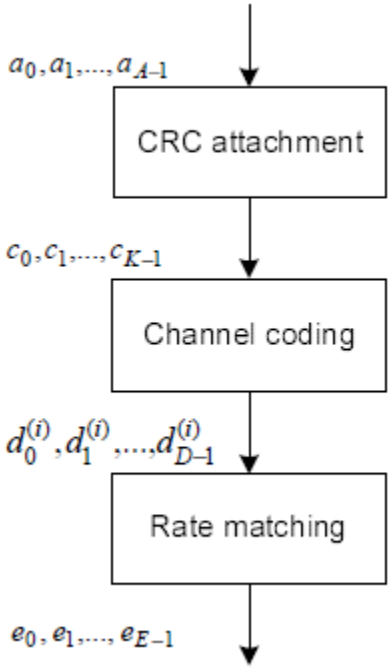

Figure 20. Processing for one DCI. From [39].

First, a CRC is calculated for the DCI message (bits $a_0, a_1,\ldots,a_{A-1}$). The entire DCI message is used to calculate the parity bits for the CRC. The parity bits are 16 bits in length and calculated using the generator polynomial, $g_{\mathrm{CRC16}}(D) = [D^{16} + D^{12} + D^5 + 1]$ where D^x is the value of the bit a_x.

The generated parity bits are then appended to the back of the DCI message creating bits $c_0, c_1,\ldots, c_{K-1}$ before it is channel coded. The DCI is encoded by means of a tail-biting convolutional encoder, the design of which is shown in Figure 21.

The encoder is constraint length seven and code rate 1/3. To accomplish the tail-biting concept, the six shift registers are initialized to the last six bits of the input stream so that the initial and final states of the shift registers are the same.

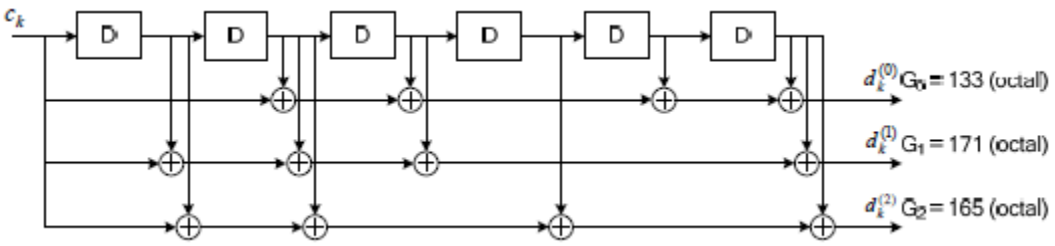

Figure 21. Design of tail-biting convolutional encoder for DCI. From [39].

Next, each of the outputs from the encoder ($d_k^{(0)}$, $d_k^{(1)}$ and $d_k^{(2)}$) is separately fed through a sub-block interleaver before the bits are interleaved and rate matched. The rate matching is necessary because the PDCCH also has a number of formats, which determine the number of resource elements per PRB used to transmit the PDCCH. The design of the interleaving and rate matching process is shown in Figure 22.

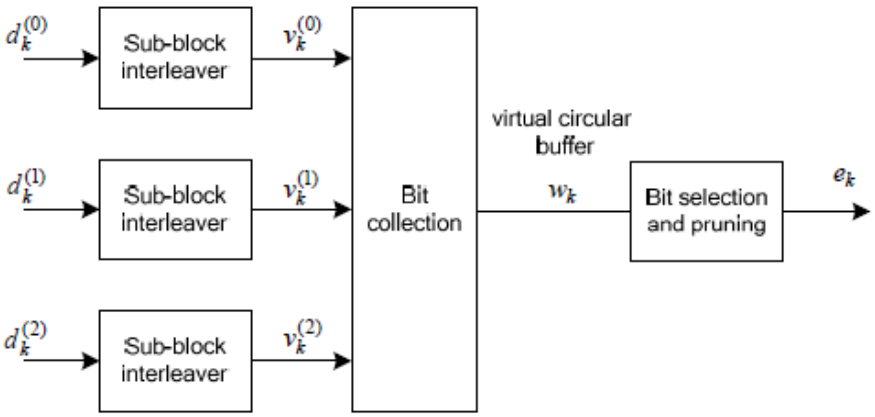

Figure 22. DCI interleaving and rate matching process. From [39].

Each sub-block interleaver carries out a permutation on the incoming bit-stream by first converting it into a 32-column matrix and then permutating it using the fixed pattern shown in Table 12.

Table 12. Inter-column permutation pattern for sub-block interleaver. From [39].

Number of columns $C_{subblock}^{CC}$	**Inter-column permutation pattern** $< P(0), P(1), ..., P(C_{subblock}^{CC} - 1) >$
32	< 1, 17, 9, 25, 5, 21, 13, 29, 3, 19, 11, 27, 7, 23, 15, 31, 0, 16, 8, 24, 4, 20, 12, 28, 2, 18, 10, 26, 6, 22, 14, 30>

An example of how the sub-block interleaver permutates the columns in the 32-column matrix is shown in Figure 23. Note that the values within each column do not change as the entire column is shifted.

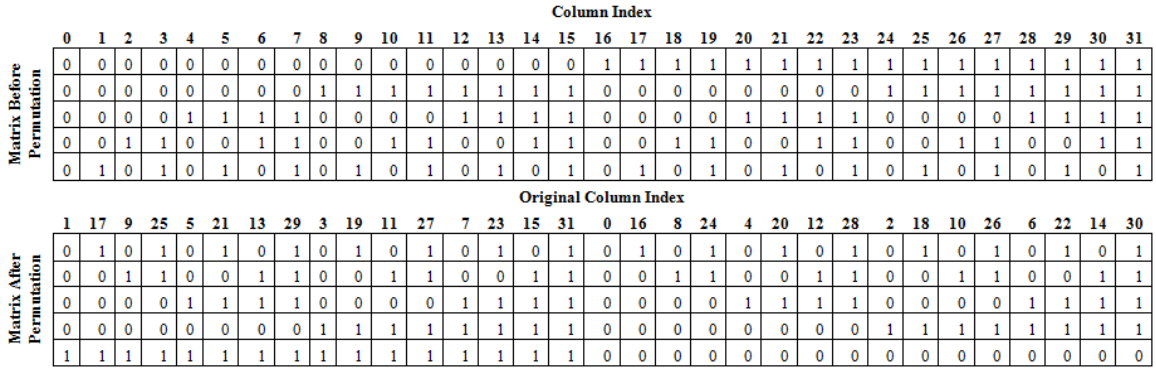

Figure 23. Example of a matrix before and after permutation.

The output from the sub-block interleavers is then collected in a circular buffer, which basically collects each of the outputs and sequentially adds them to the buffer. The bits are then selected and pruned from the circular buffer to create an output sequence length that meets the required code rate determined by the PDCCH format.

2. RNTI

The RNTI is assigned by the network to identify one specific radio channel/user from other radio channels/users. There are different types of RNTI, and each is used for a different purpose. Each type of RNTI and its respective purpose is listed in Table 13.

Table 13. Types of RNTI and their usage. From [40]

RNTI	Meaning	Usage
P-RNTI	Paging RNTI	Paging and system information change notification
SI-RNTI	System Information RNTI	Broadcast of system information
M-RNTI	MCCH RNTI	MCCH information change notification
RA-RNTI	Random Access RNTI	Random access response
C-RNTI	Cell RNTI	Dynamically scheduled unicast transmission
T C-RNTI	Temporary C-RNTI	Contention resolution and Msg3 transmission when no C-RNTI is assigned
SPS C-RNTI	Semi-Persistent Scheduling C-RNTI	Semi-persistently scheduled unicast transmission (activation, reactivation, deactivation and retransmission)
TPC-PUCCH-RNTI	Transmit Power Control PUCCH RNTI	PUCCH uplink power control
TPC-PUSCH-RNTI	Transmit Power Control PUSCH RNTI	PUSCH uplink power control

In addition, each RNTI has a range of possible values that the network can assign to the UE. This may be done sequentially or randomly depending on the network configuration. The list of possible values for each type of RNTI is shown in Table 14.

Table 14. Possible values for RNTI. From [40].

Value (hexadecimal)	RNTI
0000	N/A
0001–003C	RA-RNTI, C-RNTI, SPS C-RNTI, T C-RNTI, TPC-PUCCH-RNTI and TPC-PUSCH-RNTI
003D-FFF3	C-RNTI, SPS C-RNTI, T C-RNTI, TPC-PUCCH-RNTI and TPC-PUSCH-RNTI
FFF4-FFFC	Reserved for future use
FFFD	M-RNTI
FFFE	P-RNTI
FFFF	SI-RNTI

From Tables 13 and 14, it can be seen that an attacker would be interested in obtaining as many different RNTIs as possible by connecting to the eNB, since guessing is not feasible given the large number of values. In particular the C-RNTI, TPC-PUCCH-RNTI and TPC-PUSCH-RNTI would be useful to an attacker to affect the power control loop of the LTE network maliciously. The C-RNTI is a unique identifier of a UE issued by the eNB, while the TPC-PUCCH-RNTI and TPC-PUSCH-RNTI are identifiers issued by the eNB to groups of UEs within the cell. The attacker can, therefore, encode a

malicious DCI format 0 message with a C-RNTI to target a single UE or target multiple UEs by encoding a malicious DCI format 3/3A message with a TPC-PUCCH-RNTI or TPC-PUSCH-RNTI.

D. DECODING THE PDCCH

The PDCCH has multiple formats (listed in Table 15) and the format used by the eNB is unknown to the UE. Therefore, the UE (and the attacker) needs to decode the PDCCH blindly to extract the encoded DCI within.

Table 15. Definition of PDCCH formats. From [14].

PDCCH format	Number of CCEs	Number of REGs	Number of PDCCH bits
0	1	9	72
1	2	18	144
2	4	36	288
3	8	72	576

A UE is only informed of the number of OFDM symbols within the control region of a sub-frame but is not provided with the location of its corresponding PDCCH. The UE finds the PDCCH addressed to it by monitoring a set of PDCCH candidates in every sub-frame. The UE does this by unscrambling each candidate's CRC using its assigned RNTI; the RNTI used depends on the search space. If no CRC error is detected, the UE considers it as a successful decoding attempt and reads the control information within the successful candidate.

Depending on the purpose of the DCI within the PDCCH, the eNB scrambles the CRC with different RNTIs. With the multiple possible combinations of RNTIs, PDCCH candidates, DCI and PDCCH formats, a significant number of attempts are required to decode the PDCCH successfully if no specific algorithm is followed.

To overcome this in LTE, the UE tries to decode PDCCHs in the common search space first before trying in UE-specific search space. The common search space carries the DCIs for system information (scrambled using the SI-RNTI), paging (P-RNTI), PRACH responses (RA-RNTI) or uplink TPC commands (TPC-PUCCH-RNTI/TPC-

PUSCH-RNTI). However, it also may carry control information for specific UEs (scrambled using the C-RNTI). When searching the common search space, it iterates for only two aggregation levels (4 and 8) and tries to decode all PDDCH candidates for all possible common space DCI formats. The aggregation level is the number of Control Channel Elements (CCE) in a PDCCH.

The UE-specific search space can carry DCIs for UE-specific allocations using the UE's assigned C-RNTI, semi-persistent scheduling (SPS C-RNTI) or initial allocation (temporary C-RNTI). The UE-specific search space is scanned for all four possible aggregation levels (1, 2, 4 and 8).

The starting location is fixed for common search space and is assigned by higher layers for the UE-specific search space. An illustration of the difference between the common and UE-specific search spaces is shown in Figure 23.

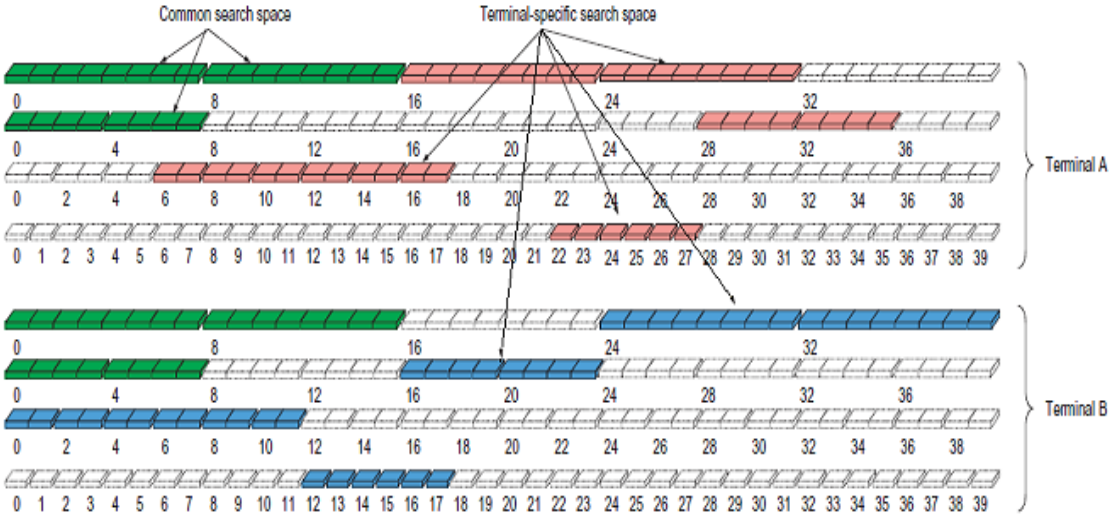

Figure 24. Common and UE-specific search spaces in control region. From [41].

In the case of the attacker, the desire is to obtain a C-RNTI of another legitimate UE. Hence, the attacker has to conduct a brute force search of the entire search space (common and UE), trying all the respective aggregation levels and C-RNTI values until no CRC error is detected.

E. ENCODING THE PDCCH

The PDCCH carries scheduling assignments and other control information from the eNB to the UE. The key control information carried in the PDCCH is the DCI. A flowchart illustrating how the DCI is encoded and decoded from the PDCCH is shown in Figure 25.

Several PDCCH channels are multiplexed together to form the final signal that is to be transmitted out of the cell. This signal is then scrambled based on the Cell-ID before being modulated using QPSK (i.e., 4-bits per symbol).

If MIMO is used, the modulated symbols are then mapped to the respective antenna ports depending on whether it is spatial multiplexing or transmit diversity. After mapping to the antenna ports, the symbols are then interleaved using a pre-defined permutation matrix.

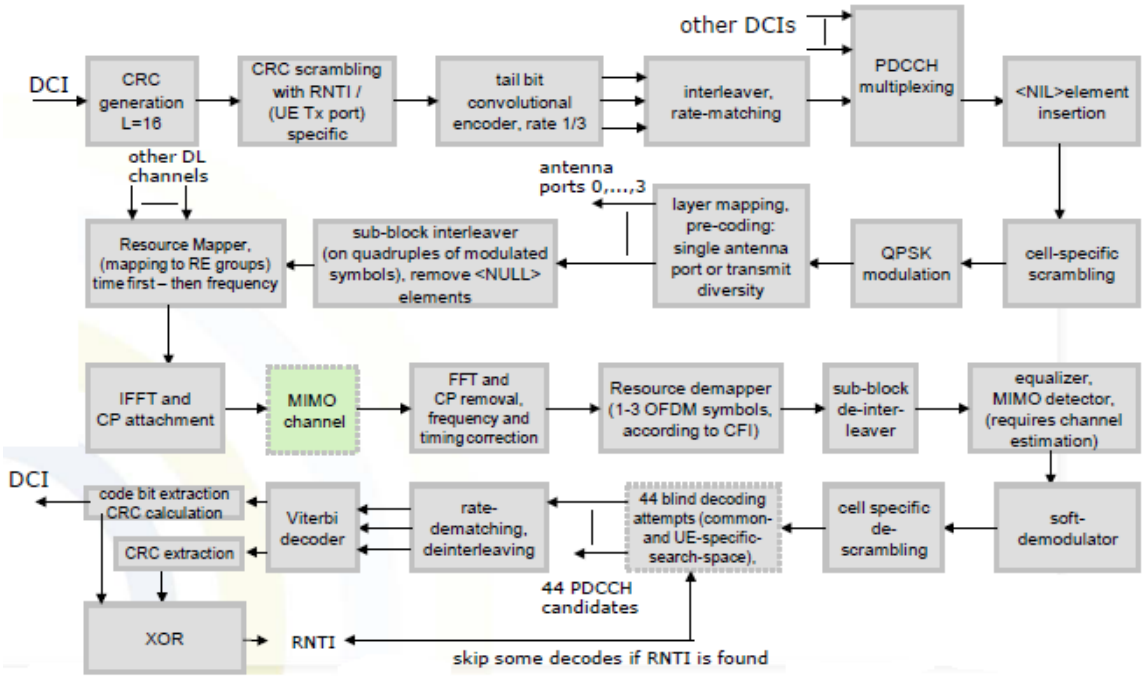

Figure 25. Process of encoding and decoding the DCI in the PDCCH. From [16].

Lastly, the PDCCH signal is mapped onto the PRB depending on the format. The supported PDCCH formats with their respective consecutive CCEs and Resource

Element Groups (REG) required were shown previously in Table 15. The process of allocation of REGs is explained in detail in the following sub-section. The PRB is then transmitted via the OFDMA downlink signal.

To create the false downlink signal, the attacker basically follows the steps given to encode a malicious DCI message onto a legitimate downlink signal.

1. CCEs and REGs

A PDCCH is transmitted on one or more consecutive CCEs. Each CCE is made up of nine REGs, which in turn are made up of four resource elements. Hence, four PDCCH QPSK symbols are mapped onto each REG. The location of the CCEs within the PRBs is shown in Figure 26.

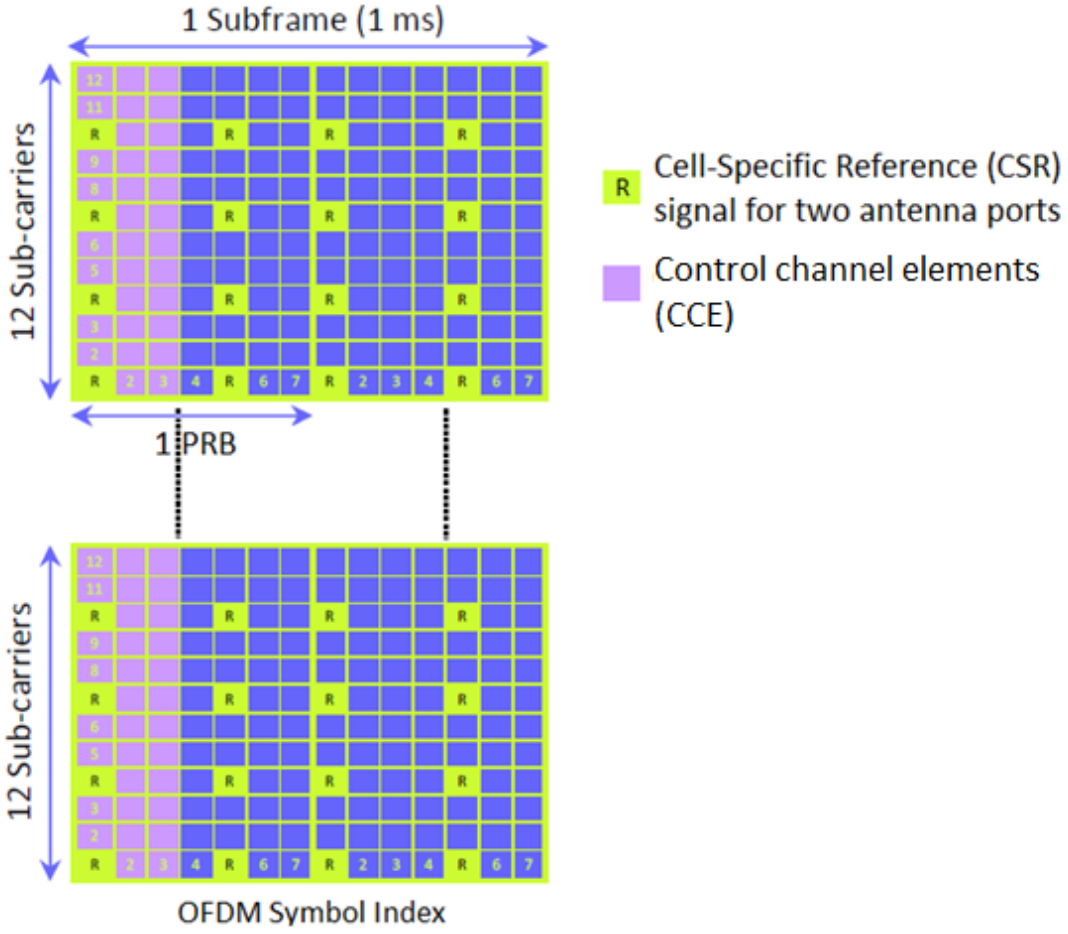

Figure 26. CCEs and UE control region (3 OFDM symbols) in the PRB. From [12].

The number of CCEs available depends on the size of the UE control region, which in turn depends on the number of OFDM symbols allocated to the control channels. This allocation is determined by the network and is transmitted to the UE during the initial connection to the cell.

The encoded PDCCH symbols are allocated to the REGs in sequential order starting from the OFDM symbol number and followed by the sub-carrier number of the first resource element of the REG. An example of this allocation is shown in Figure 27.

Notice in Figure 27 that the REGs need not be allocated to a continuous block of four resource elements. For example, REG3 is split into two sections of two resource elements each since subcarrier 4 is occupied by a cell-specific reference signal (indicated by the 'R').

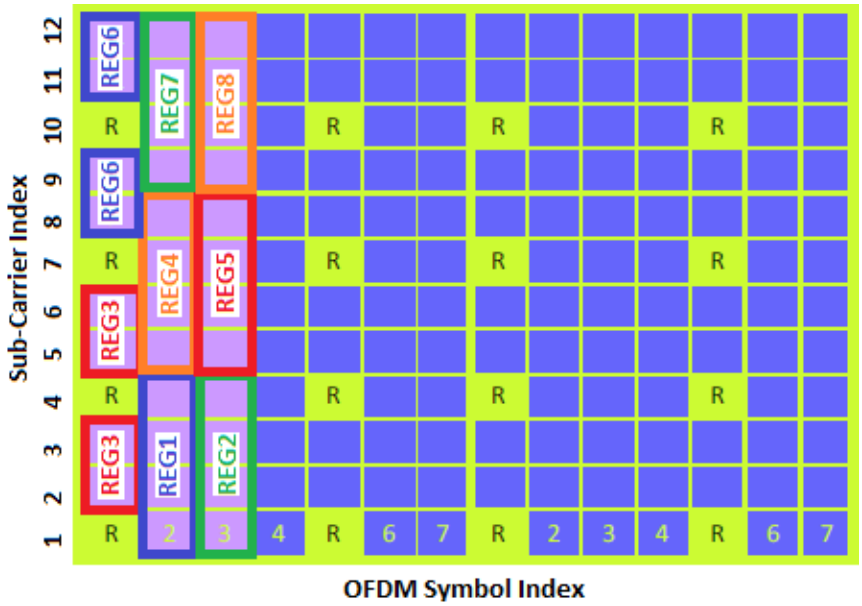

Figure 27. Sequence of allocation of PDCCH symbols to REGs in PRB. After [14].

F. SIMULATION AND RESULTS

The proposed attack was simulated using specifically developed MATLAB tools and the communications toolbox. To simplify the simulation, the following assumptions were made.

Firstly, the eNB had only one UE in the cell, thus, sending out only one PDCCH channel in the downlink signal. Secondly, the attacker was close enough to the eNB such that the false and legitimate signals arrive at the same time at the victim UE.

1. Brute Force Scan for C-RNTI

In stage two of the proposed attack, the attacker is required to decode the PDCCH over the air on the network to obtain the C-RNTI of other UEs. Two scenarios were simulated to compare the difference between the decoding time required. In scenario A, the attacker assumes that the C-RNTI values are assigned in a random manner and conducts a brute force attack scanning all possible values of the C-RNTI. For scenario B, the attacker carries out an attack assuming that the eNB assigns C-RNTI values in sequential order within a range of a few thousand values.

a. Scenario A

The value of the valid C-RNTI can vary from 1 to 65523. Since the value of the C-RNTI affects when the DCI is decoded by the UE, it affects the length of time the simulation takes to run. Hence, different C-RNTI values (10000, 20000, 30000, 40000 and 50000) were used to encode the DCI, and the average of five runs for each value was recorded as shown in Table 16.

Table 16. Time taken for a brute force search of C-RNTI values.

Scrambling C-RNTI value	Average time taken (s)
10000	46889
20000	41558
30000	43966
40000	50754
50000	40936
Overall average time	**44821 (12.45 hours)**

As can be seen from the results, the time taken to do a brute force guess is beyond the effective period of an attack since it is unlikely that a single UE will stay within a single cell for a continuous period of more than 12 hours.

b. Scenario B

If the attacker assumes that the valid C-RNTI values are assigned by the eNB in a sequential manner, the C-RNTI value obtained in stage 1 would be the middle value from which to search. Based on this assumption, seven runs were conducted with increasing C-RNTI search ranges. The time taken to decode the DCI in each run is shown in Table 17.

From run number 4 in Table 17, a search range of up to 10,000 values around the attacker's C-RNTI is still within an acceptable time period of two hours and covers a third of the valid C-RNTI values, making such an attack viable. To further reduce the required scan range, the attacker could repeat stage one of the attack a number of times to discover the pattern and range of valid C-RNTI values allocated by the eNB.

Table 17. Time taken to guess of C-RNTI value for different search ranges.

Run	C-RNTI scan range	Time taken (s)
1	±1000	86
2	±2000	196
3	±5000	2848
4	±10000	7398
5	±15000	11690
6	±20000	23288
7	±25000	40258

Based on the results in Table 17, the graph in Figure 28 was plotted. As expected, it shows that the time taken increases proportionally with the search range. This is because the search is still done sequentially in each case albeit for fewer values.

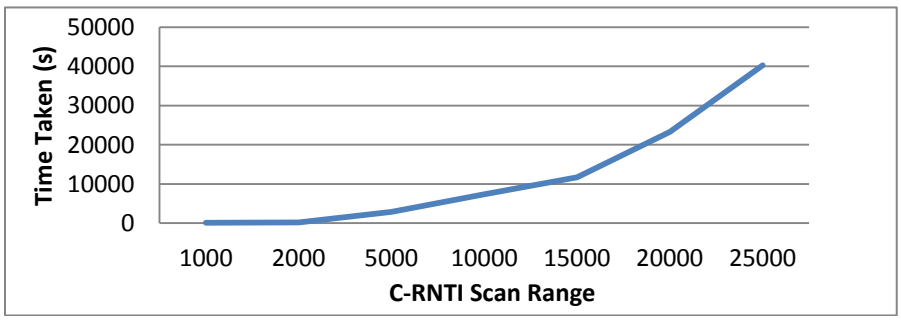

Figure 28. Plot of C-RNTI scan range vs. time taken to decode.

2. Power Ratio Required to Overcome the Legitimate PSS Signal

To avoid calculating the transmission delay from the victim UE, the attacker can choose to broadcast a false PSS signal to force victim UEs to synchronize with the false downlink signal. This is simulated by assuming both signals are received at the UE and by finding the threshold power ratio between the false and legitimate signals required to get the UE to reliably detect the malicious PSS. The simulation is performed using a single-input single-output (SISO) antenna configuration in FDD mode for different timing offset values, where the malicious PSS is either advanced or delayed by a few symbols (i.e., −2, −1, 0, 1 or 2 symbols) with respect to the legitimate PSS. The results are plotted in a graph as shown in Figure 29.

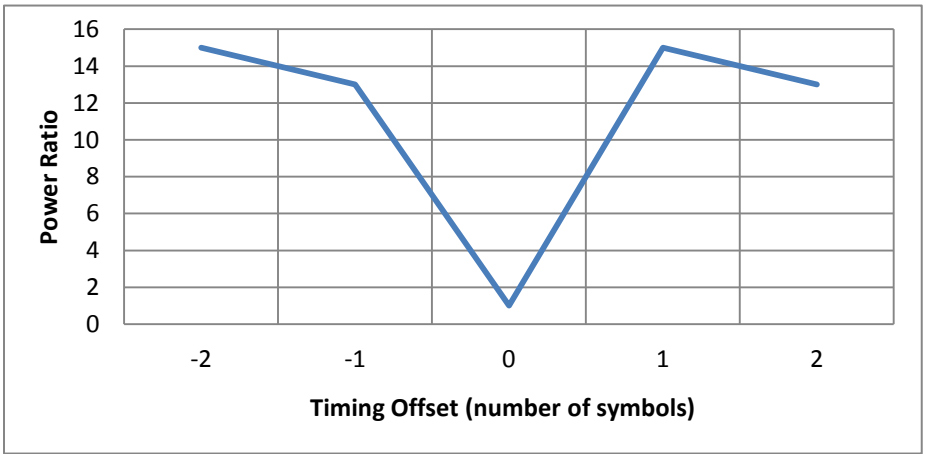

Figure 29. Plot of power ratio vs. offset of malicious PSS.

From Figure 29, we can see that it takes more power to overcome the legitimate PSS when the malicious PSS arrives at the victim UE two symbols before the legitimate signal (2/14 ms early) or one symbol after the legitimate signal (1/14 ms late). This is because the CSR signals are broadcast two symbols before and one symbol after the PSS is broadcast in the PRB as shown in Figure 30. Since the CSRs are also specially coded signals to allow easy detection by the UE, it stands to reason that it would take more power to overcome them as compared with random data bits transmitted in other symbols of the PRB. An attacker should avoid transmitting a PSS with offsets that coincide with the CSRs or other known reference signals like the SSS.

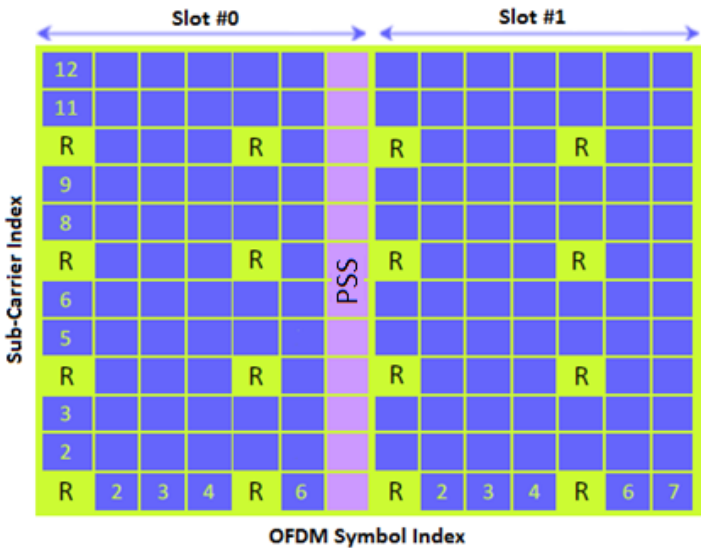

Figure 30. Position of the PSS within slot 0 of a type 1 frame. After [12].

It is also noted that to overcome the legitimate PSS the power ratio required by the attacker has to be at least 13 times greater. This implies that the range of such an attack would be very limited unless the attacker has access to a sufficiently powerful transmitter.

3. Power Ratio Required to Overpower Legitimate TPC Signal

In stage four, the attacker's false signal must be able to overpower the legitimate signal in order for the UE to successfully decode it. This is simulated by assuming both signals are received at the UE and by finding the threshold power ratio between the false and legitimate signals required to get the UE to reliably decode the malicious TPC. The simulation is performed for six values of signal-to-noise ratios (0, 3, 6, 9, 12 and 15 dB) and for both SISO and 2x2 MIMO (two transmitting and two receiving antennas) antenna configurations to replicate various conditions in the real world. 2x2 MIMO in transmit diversity mode was chosen to simulate the worst possible configuration in a cellular network case where the receiver has two received signals to coherently combine since it is unlikely that the maximum of four receiving antennas could be fitted on a cell phone. The average of the values for each case are recorded as shown in Table 18. For example, in SISO case, malicious TPC signal of '01' requires a power ratio of 1.26 to override the eNB TPC signal of '10'.

Table 18. Power ratio required to overpower eNB TPC signal with malicious TPC signal.

SISO						
	eNB TPC Signal					
Malicious TPC signal		00	01	10	11	Average
	00		1.57	1.53	1.53	1.85
	01	1.01		1.26	1.43	1.48
	10	1.51	1.69		1.41	1.84
	11	1.30	1.73	1.34		1.75
	Average	1.27	1.66	1.38	1.46	
2x2 MIMO						
	eNB TPC Signal					
Malicious TPC signal		00	01	10	11	Average
	00		18.77	6.26	22.15	18.87
	01	2.24		2.64	2.84	3.09
	10	7.70	35.17		2.90	18.31
	11	3.56	6.73	2.40		5.07
	Average	4.50	20.22	3.77	9.30	

On average the malicious signal required 1.73 times (SISO case) and 11.34 times (MIMO case) of the power of the eNB signal to be decoded accurately by the victim UE. It is also observed that the eNB TPC signal requiring the least power to overcome on average is '00' (SISO case) and '10' (MIMO case), and the malicious TPC signal requiring the least power to influence the UE on average is '01'. This trend is obvious when the results are plotted in graphs as shown in Figure 31 and 32 for the SISO and MIMO cases, respectively.

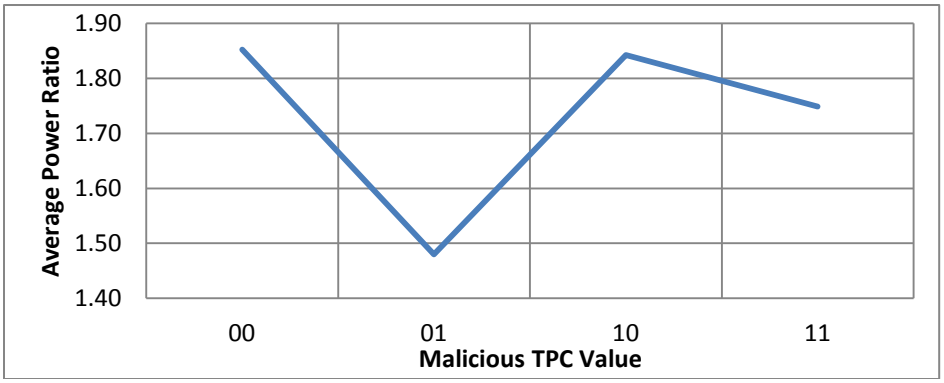

Figure 31. Plot of average power ratio vs. malicious TPC value (SISO).

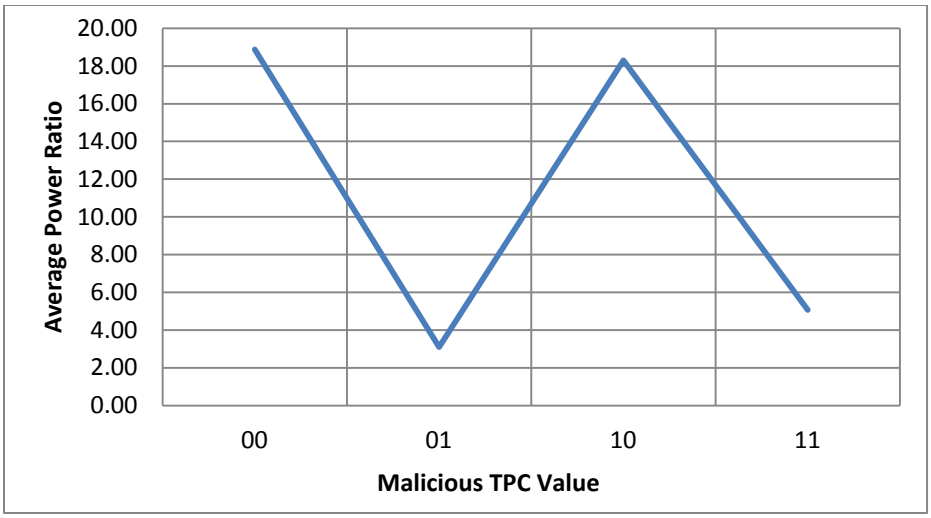

Figure 32. Plot of average power ratio vs. malicious TPC value (MIMO).

From Table 18, we can see that in the SISO environment, to force the TPC value to '01' takes 18% less power than forcing the TPC value to '11'. Similarly, in the MIMO case forcing the TPC value to '01' takes 64% less power than forcing the TPC value to the next lowest TPC value of '11'. This implies that the attacker should transmit a malicious TPC value of '01' (i.e., command the UE to reduce its transmit power by 1 dB), to maximize the chance of a successful attack. Such an attack is feasible since the malicious signal power required by the attacker is only 1.48 times (SISO case) or 3.09 times (MIMO case) of the legitimate signal power reaching the victim UE.

As shown in Figures 31 and 32, different TPC values require different power to override them for a successful attack. The difference in power requirement may be due to the encoding process and OFDM conversion. If other download channels use the same encoding method, they could be exposed to similar bit change attacks.

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

A comprehensive study of the LTE protocols and physical layer specifications and their respective vulnerabilities was provided in this thesis. The LTE physical layer was then simulated using MATLAB tools and manipulated to simulate an attack on the uplink transmit power control procedure without the knowledge of the user.

The results of the simulations show that an attack is feasible as it can be accomplished within a short amount of time (less than two hours) using modest computational power. Additionally, the simulation highlighted that there is a possible weakness in the encoding of the PDCCH that allows the attacker to overpower the legitimate signal with a significantly lower signal power for the TPC value of 01 compared to other values. This weakness could potentially expose other similarly encoded control channels to attacks.

The impacts of the attack on the UE depend on the attacker's broadcasted malicious TPC value. If the malicious TPC value is '10' or '11', the impact is the unnecessary increase in transmit power causing shorter battery life and increased interference with other UEs. Conversely, if the malicious TPC value is '00' or '01', then the attacker causes uplink service disruption by reducing the UE's uplink transmit power below the required value to reach the eNB. In addition, if the attacker chooses not to synchronize his false downlink signal with the legitimate signal and broadcast a malicious PSS instead, he can also cause the UEs within range to lose synchronization with the eNB resulting in both uplink and downlink service disruptions.

B. RECOMMENDEDATIONS FOR FUTURE WORK

The work within this thesis puts forward a number of potential security issues inherent in both the LTE protocol security as well as the physical layer security procedures. These areas can be further explored to understand whether they indeed pose a risk to the LTE system or if the risks can be mitigated by other measures.

1. Unauthorized and Unencrypted Messages in the RRC

As highlighted in Chapter III, there are a number of RRC messages that are passed over the air interface unauthorized and unencrypted. Although these messages are encoded further in the physical layer, with sufficient time and knowledge of the specifications, an attacker can monitor the encoded control information and inject changes into the signals. Hence, this warrants an in-depth study into the various RRC messages to understand how they can be better protected.

2. Injection of Malicious DCI Messages

Since the DCI is used for multiple purposes including scheduling and paging, an investigation can be done on how an attacker can inject false DCI messages into the downlink to overwrite legitimate ones. The malicious DCI message could cause multiple UEs to transmit at the same time (scheduling attack) or cause UEs to perform unnecessary procedures (paging attack).

3. Improving the PDCCH Encoding Scheme

As the results of the simulation show, there is a potential weakness in the encoding for the PDCCH. An exploration of which stage(s) of the encoding is responsible for this weakness and how it can be improved should be conducted.

LIST OF REFERNCES

[1] M. Batistatos *et al.*, "Mobile telemedicine for moving vehicle scenarios: Wireless technology options and challenges," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1140–1150, 2012.

[2] Wikipedia, "4G," June 2013. [Online]. Available: http://en.wikipedia.org/wiki/4G. [Accessed June 2013].

[3] I. Poole, "Radio-Electronics.com 3G LTE Tutorial - 3GPP Long Term Evolution," [Online]. Available: http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/3g-lte-basics.php. [Accessed June 2013].

[4] 3GPP, "LTE," [Online]. Available: http://www.3gpp.org/LTE. [Accessed June 2013].

[5] GSA, "GSA Evolution to LTE report," 10 May 2013. [Online]. Available: http://www.gsacom.com/news/gsa_376. [Accessed June 2013].

[6] NgnGuru Solutions, "LTE Deployment Map," 2013. [Online]. Available: http://ltemaps.org/home/. [Accessed June 2013].

[7] Magna Design Net Inc., "OFDM," 2013. [Online]. Available: http://www.magnadesignnet.com/en/booth/technote/ofdm/page2.php. [Accessed June 2013].

[8] "Orthogonal Frequency-Division Multiplexing," *Wikipedia*, June 2013. [Online]. Available: http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing. [Accessed June 2013].

[9] 3GPP, "Feasibility Study for Orthogonal Frequency Division Multiplexing (OFDM) for UTRAN enhancement," June 2004. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/25892.htm. [Accessed June 2013].

[10] Wikipedia, "Orthogonal Frequency-Division Multiple Access," June 2013. [Online]. Available: http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiple_access. [Accessed June 2013].

[11] M. Sauter, "An Introduction To SC-FDMA Used By LTE In Uplink Direction," May 2007. [Online]. Available: http://mobilesociety.typepad.com/mobile_life /2007/05/an_introduction.html. [Accessed June 2013].

[12] Telesystem Innovations Inc., “LTE in a Nutshell: The Physical Layer,” 2010. [Online]. Available: http://www.tsiwireless.com/docs/whitepapers/LTE %20in%20a%20Nutshell%20-%20Physical%20Layer.pdf. [Accessed June 2013].

[13] “MIMO,” *Wikipedia*, June 2013. [Online]. Available: http://en.wikipedia.org/wiki/MIMO. [Accessed June 2013].

[14] 3GPP, “LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation; 3GPP TS 36.211 V11.2.0,” April 2013. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36211.htm. [Accessed June 2013].

[15] 3GPP, “LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception; 3GPP TS 36.101 V11.4.0,” April 2013. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36101.htm. [Accessed June 2013].

[16] Mulder *et al.*, “LTE Tutorial part 1; LTE Basics,” Presentation in *Femto Forum Plenary*, June 2010.

[17] “Zadoff-Chu Sequences,” *Wikipedia*, May 2013. [Online]. Available: http://en.wikipedia.org/wiki/Zadoff%E2%80%93Chu_sequence. [Accessed June 2013].

[18] Wikipedia, “Maximum length sequence,” June 2013. [Online]. Available: http://en.wikipedia.org/wiki/Maximum_length_sequence. [Accessed June 2013].

[19] 3GPP, “LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Layer Procedures; 3GPP TS 36.213 V11.2.0,” April 2013. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36213.htm. [Accessed June 2013].

[20] 3GPP, “LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2; 3GPP TS 36.300 V11.5.0,” April 2013. [Online]. Available: http://www.3gpp.org/ftp/specs/html-INFO/36300.htm. [Accessed June 2013].

[21] A. Larmo *et al.*, “The LTE Link-Layer Design,” *IEEE Communications Magazine*, pp. 53–59, April 2009.

[22] 3GPP, “LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control protocol Specification; 3GPP TS 36.322 V11.0.0,” October 2012. [Online]. Available: http://www.3gpp.org/ftp/specs/html-INFO/36322.htm. [Accessed June 2013].

[23] EventHelix, "3GPP LTE Channels and MAC Layer," 2009. [Online]. Available: http://www.eventhelix.com/lte/presentations/3gpp-lte-mac.pdf. [Accessed June 2013].

[24] 3GPP, "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification; 3GPP TS 36.331 V11.3.0," April 2013. [Online]. Available: http://www.3gpp.org/ftp/specs/html-INFO/36331.htm. [Accessed June 2013].

[25] 3GPP, "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture; 3GPP TS 33.401 V11.6.0," April 2013. [Online]. Available: http://www.3gpp.org/ftp/specs/html-INFO/33401.htm. [Accessed June 2013].

[26] R. Blom *et al.*, "Security in the Evolved Packet System," *Ericsson Review,* pp. 4–9, Feb 2010.

[27] J. Cao *et al.*, "A survey on Security Aspects for LTE and LTE-A Networks," *IEEE Communications Surveys and Tutorials,* vol. PP, no. 99, pp. 1–20, 2013.

[28] Park *et al.*, "A Survey of Security Threats on 4G Networks," in *IEEE Globecom Workshops, 2007*, pp. 1–6, Washington, DC, November 2007.

[29] H. Mun *et al.*, "3G-WLAN Internetworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA," in *Wireless Telecommunications Symposium, 2009*, pp. 1–8, Prague, April 2009.

[30] Skalvos *et al.*, "LTE/SAE Security Issues on 4G Wireless Networks," *IEEE Security & Privacy,* vol. 11, no. 2, pp. 55–62, 2012.

[31] G. Kambourakis *et al.*, "DoS attacks exploiting signaling in UMTS and IMS," *Computer Communications,* vol. 34, pp. 226–235, 2010.

[32] L. Gu *et al.*, "A Green and Secure Authentication for the 4th Generation Mobile Network," in *Australasian Telecommunication Networks and Applications Conference (ATNAC), 2011*, pp.1, 7, 9–11, Melbourne, VIC, November 2011.

[33] C. K. Han *et al.*, "Building Femtocell More Secure with Improved Proxy Signature," in *IEEE Global Telecommunications Conference*, pp.1–6, Honolulu, HI, November 2009.

[34] 3GPP, " Universal Mobile Telecommunications System (UMTS); LTE; Security of Home Node B (HNB) / Home evolved Node B (HeNB); 3GPP TS 33.320 V11.6.0," November 2012. [Online]. Available: http://www.3gpp.org/ftp/specs/html-INFO/33320.htm. [Accessed June 2013].

[35] I. Bilogrevic *et al.*, "Security Issues in Next Generation Mobile Networks: LTE and Femtocells," in *2nd International Femtocell Workshop*, pp. 1–3, Luton, UK, June 2010.

[36] Lichtman *et al.*, "Comments of Wireless @ Virginia Tech," Virginia Tech, Blacksburg, Virginia, 2012.

[37] S. Anand *et al.*, "Security Vulnerability due to Channel Aggregation/Bonding in LTE and HSPA+ Networks," in *IEEE Global Telecommunications Conference*, pp. 1, 5–9, Huston, TX, December 2011.

[38] H. T. Too, "Exploring Weakness in Long Term Evolution (LTE) Wireless Standards," M.S. Thesis, Dept. Elect and Computer Eng., Naval Postgraduate School, Monterey, CA, 2012.

[39] 3GPP, "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding; 3GPP TS 36.212 V11.2.0," April 2013. [Online]. Available: http://www.3gpp.org/ftp/specs/html-INFO/36212.htm. [Accessed June 2013].

[40] 3GPP, "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification; 3GPP TS 36.321 V11.2.0," April 2013. [Online]. Available: http://www.3gpp.org/ftp/specs/html-INFO/36321.htm. [Accessed June 2013].

[41] National Chung Hsing University, Wireless Communications and Cloud Computing Lab, "PDCCH Processing," [Online]. Available: http://wccclab.cs.nchu.edu.tw/www/images/Wireless_Broadband_Networks/chap% 2013. [Accessed June 2013].

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California