2012-09

Exploring weakness in Long Term Evolution (LTE) wireless standards

Tien, Too Huseh

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EXPLORING WEAKNESSES IN LONG TERM EVOLUTION (LTE) WIRELESS STANDARDS

by

Too Huseh Tien

September 2012

Thesis Co-Advisors: Weilian Su
Tri T. Ha

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2012	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Exploring Weakness in Long Term Evolution (LTE) Wireless Standards	5. FUNDING NUMBERS
6. AUTHOR(S) Too Huseh Tien	
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 provider and end users and made security of the network even more indispensable. In this thesis, the LTE specifications are examined, and several security vulnerabilities of LTE mechanisms, in particular those that exist within the Layer 2 protocol of the LTE network, are identified. Among these mechanisms, the power control mechanism for LTE is further explored. The unprotected power control signal together with the Cell Radio Network Temporary Identifier (CRNTI) can be exploited to trick the victim User Equipment (UE) to transmit at a much higher than required power, which introduces significant inter-cell interference to adjacent base stations, evolved NodeB (eNodeB). The ways that an attacker can maliciously manipulate the control field of the power control mechanism are demonstrated. The effectiveness of such attack is evaluated with respect to the victim UEs and the adjacent eNodeBs. The impacts include reduction of battery lifespan of victim UE to 33% of the original battery lifetime and reduction in reverse channel signal-to-interference ratio (SIR) of adjacent eNodeB by 3.4 dB causing a decrease in throughput of 37%.

14. SUBJECT TERMS Long Term Evolution (LTE), Security, Power control, Vulnerabilities	15. NUMBER OF PAGES 103
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	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

EXPLORING WEAKNESSES IN LONG TERM EVOLUTION (LTE) WIRELESS STANDARDS

Too Huseh Tien
Defence Science & Technologies Agency
B.Eng (Electrical Engineering), Nanyang Technological University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2012

Author: Too Huseh Tien

Approved by: Weilian Su
Thesis Co-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 provider and end users and made security of the network even more indispensable. In this thesis, the LTE specifications are examined, and several security vulnerabilities of LTE mechanisms, in particular those that exist within the Layer 2 protocol of the LTE network, are identified. Among these mechanisms, the power control mechanism for LTE is further explored. The unprotected power control signal together with the Cell Radio Network Temporary Identifier (CRNTI) can be exploited to trick the victim User Equipment (UE) to transmit at a much higher than required power, which introduces significant inter-cell interference to adjacent base stations, evolved NodeB (eNodeB). The ways that an attacker can maliciously manipulate the control field of the power control mechanism are demonstrated. The effectiveness of such attack is evaluated with respect to the victim UEs and the adjacent eNodeBs. The impacts include reduction of battery lifespan of victim UE to 33% of the original battery lifetime and reduction in reverse channel signal-to-interference ratio (SIR) of adjacent eNodeB by 3.4 dB causing a decrease in throughput of 37%.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

3GPP	Third Generation Partnership Program
4G	Fourth Generation
AKA	Authentication and Key Agreement
AM	Acknowledged Mode
AS	Access Stratum
BCCH	Broadcast Control Channel
BCH	Broadcast Channel
BPSK	Binary Phase Shift Keying
CCCH	Common Control Channel
CCE	Control Channel Element
CCI	Co-channel Interference
CFO	Carrier Frequency Offset
CN	Core Network
CP	Cyclic Prefix
CRNTI	Cell Radio Network Temporary Identifier
CRC	Cyclic Redundancy Check
CSG	Closed Subscriber Group
DCCH	Dedicated Control Channel
DCI	Downlink Control Message
DL-SCH	Downlink Shared Channel
DoS	Denial of Service
DRX	Discontinuous Reception
DTCH	Dedicated Traffic Channel
DwPTS	Downlink Pilot Timeslot
EAKA	Enhanced EPS-AKA
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
E-UTRA	Evolved Universal Terrestrial Radio Access
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EDGE	Enhanced Data rates for Global Evolution
eNodeB	Evolved NodeB (The base station in LTE system)

EPC	Evolved Packet Core
EPS	Evolved Packet System
ESIM	Enhanced Subscriber Identity Module
FDD	Frequency-Division Duplexing
FFT	Fast Fourier Transform
GP	Guard Period
GSA	Global mobile Suppliers Association
HARQ	Hybrid Automatic Repeat Request
HPSA	High Speed Packet Access
HSS	Home Subscriber Server
IFFT	Inverse Fast Fourier Transformation
ICI	Inter-Carrier interference
IMT	International Mobile Telecommunications
IP	Internet Protocol
IPSec	Internet Protocol Security
ISI	Inter-Symbol-Interference
LEAP	Lightweight Extensible Authentication Protocol
LTE	Long Term Evolution
LTE/SAE	Long Term Evolution/System Architecture Evolution
MAC	Medium Access Control
MCH	Multicast Channel
MBMS	Multimedia Broadcast Multicast Services
MBSFN	Multicast-Broadcast Single Frequency Network
MCCH	Multicast Control Channel
MCS	Modulation and Coding Scheme
MME	Mobility Management Entity
ME	Mobile Equipment
MIMO	Multiple-Input Multiple-Output
MITM	Man-In-The-Middle attack
MTCH	Multicast Traffic Channel
NAS	Non-Access Stratum
OFDM	Orthogonal Frequency-Division Multiplexing

OFDMA	Orthogonal Frequency-Division Multiple-Access
P-GW	Packet Data Network Gateway
PAP	Password Authentication Protocol
PAPR	Peak-to-Average Power Ratio
PBCH	Physical Broadcast Channel
PCFICH	Physical Control Format Indicator Channel
PCCH	Paging Control Channel
PCH	Paging Channel
PDCCH	Physical Downlink Common Control Channel
PDSCH	Physical Downlink Shared Channel
PDCP	Packet Data Convergence
PDU	Protocol Data Unit
PHICH	Physical Hybrid-ARQ Indicator Channel
PRACH	Physical Random Access Channel
PRB	Physical Resource Block
PUCCH	Physical 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
RAR	Random Access Response
REs	Resource Elements
REGs	Resource Element Groups
RF	Radio Frequency
RLC	Radio Link Control
RNTI	Radio Network Temporary Identifier
ROHC	Robust Header Compression
RRC	Radio Resource Control
S-GW	Serving Gateway
SAE	System Architecture Evolution
SC-FDMA	Single-Carrier FDMA

SDU	Service Data Units
SIR	Signal-to-Interference Ratio
SINR	Signal-to-Interference and Noise Ratio
SNR	Signal-to-Noise Ratio
SKC	Session Keys Context
TDD	Time Division Duplexing
TDMA	Time-Division Multiple-Access
TPC	Transmit Power Control
UE	User Equipment
UEID	UE Identification
UL-SCH	Uplink Shared Channel
UMTS	Universal Mobile Telecommunications System
UpPTS	Uplink Pilot Timeslot
W-CDMA	Wideband Code-Division Multiple Access
WIMAX	Worldwide Interoperability for Microwave Access

EXECUTIVE SUMMARY

The rapid increase in data usage in mobile communication systems has led to the development of the fourth generation (4G) Long Term Evolution (LTE) standard. LTE is the current generation wireless data communications standard that is poised to dominate mobile data connectivity in both the commercial and military arenas because of its very high data rate capabilities. The increasingly important role of LTE has increased security concerns among the service provider and end users and made security of the network even more indispensable.

The literature related to the LTE network, in particular, that which is related to the security issues, is reviewed and the security vulnerabilities identified in the available literatures are discussed briefly. In this thesis, the LTE specifications are examined and several security vulnerabilities of LTE mechanisms, in particular those that exist within the Layer 2 protocol of the LTE network, are identified. The identified potential weaknesses include malicious modification of the control protocol data unit (PDU) type reserve field, prioritized retransmission of traffic data, and malicious modification of the power control mechanism.

In this thesis, the focus is on exploring the power control mechanism for LTE. The objectives of power control are to improve the system capacity, coverage and user experience, while at the same time reduce the power consumption of the User Equipment (UE). Fundamentally, uplink power control for LTE is a combination of an open-loop mechanism, where the UE transmit power depends on estimates of the downlink path loss, and a closed loop mechanism, where the network directly controls the UE transmit power by means of explicit transmitter power-control (TPC) commands transmitted in the downlink. This closed loop mechanism is computed dynamically and updated from sub-frame to sub-frame. An adversary can inject false power-control commands to control the UE transmit power, as shown in Figure 1.

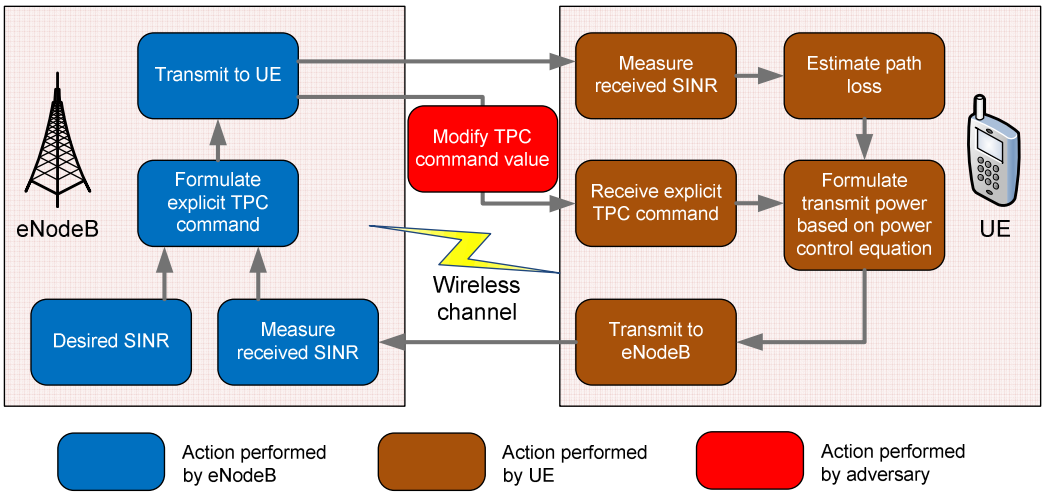

Figure 1. Modified power control mechanism.

The unprotected power control signal together with the Cell Radio Network Temporary Identifier (CRNTI) can be exploited to change the intended behavior of the UE. The CRNTI provides unique end User Equipment identification (UEID) at the cell level and is assigned to the associated UE by the network during the initial establishment of uplink synchronization. An adversary can exploit the fact that CRNTI is transmitted in the clear and misuse it for malicious activities.

The ways that an attacker can maliciously manipulate the control field of the power control mechanism are demonstrated in this thesis. The attacker acts as a combination of base station, evolved NodeB (eNodeB), and the UE. Initially, the attacker impersonates a UE and connects to the genuine eNodeB to obtain the cell–specific reference signal. The attacker at a later stage presents itself as a bogus eNodeB and generates false messages to the victim UE. The attacker can perform message injection attack on the victim UE in three stages. Stage 1 involves the extraction of messages between the victim UE and the eNodeB to obtain CRNTI. Stage 2 involves the calculation of the timing advance to synchronize the false message frame to the victim UE. Stage 3 involves the injection of false messages with the TPC field adjusted to the

designated value to change the behaviors of the victim UE. The correlation and graph for the required power of the injected message for varying received false-signal-to-legitimate-signal is also derived.

The effectiveness of such an attack with respect to the victim UEs and adjacent eNodeBs are evaluated. The impacts include reduction of battery lifespan of victim UE and reduction in reverse channel signal-to-interference ratio (SIR) of adjacent eNodeB.

The interference generated by the victim UE in a 120-degree sectoring cell is examined. A combination of these interferences creates a cascading effect on adjacent eNodeBs, and the received SIR at the eNodeB is derived. From the derivation, it is observed that SIR is dependent on the power transmitted by the UEs, and Matlab simulation is performed to generate the average SIR. It is indicated in the simulation results that the received SIR at the eNodeB decreases from a nominal value of 11.7 dB to 8.3dB when the interfering sources are transmitting at maximum power.

In general, a modulation and coding scheme (MCS) with a higher throughput requires a higher SIR to operate in. The decrease in SIR leads to the adoption of an MCS type with a lower throughput. The MCS is lowered from MCS-10, with a corresponding maximum throughput of 3.2 bits per second per hertz, to MCS-8, with a corresponding maximum throughput of 2.0 bits per second per hertz. The maximum throughput of the legitimate UE is reduced by 37.5%.

.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank 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, Kim Hong, my family, and friends for their continuous support during my study in Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

"LTE is the next step in user experience, enhancing more demanding application such as interactive TV, mobile video blogging, advanced gaming, and professional services. Data rates are significantly higher. LTE supports a full [internet protocol] IP-based network and harmonization with other radio access technologies." [1]

The rapid increase in data usage in mobile communication systems has led to the development of fourth generation (4G) wireless technologies, which includes Long Term Evolution (LTE) and Worldwide Interoperability for Microwave Access (WiMAX). LTE is a standard developed by the Third Generation Partnership Program (3GPP) Long Term Evolution/System Architecture Evolution (LTE/SAE), a consortium of telecommunications associations formed in order to define communication standards, and is specified in the 3GPP's Release 8 document series, with minor enhancements described in Release 9.

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

The first release of 3G provided by 3GPP in 2000 is known as "Release 99". This defines the wideband code-division multiple access (W-CDMA) and UMTS standards. In 2001, a new feature, "all-IP core network", was added to Release 99, and it evolved to Release 4. HPSA includes Release 5 and Release 6. Release 5 introduced the high speed downlink packet access (HSDPA) in 2002 and Release 6 introduced the high speed uplink packet access (HSUPA) and included more features like multimedia broadcast multicast services (MBMS) and integration with wireless local area network (LAN) in 2005. Release 7 introduced HSPA+ in 2007 and primarily deals with the development of specification like latency and quality of service (QoS) improvement and real time applications.

Although the HSPA systems offer significant improvement in performance over previous UMTS systems, their designs were limited by compatibility requirement in the UMTS specification. In addition, with the emergence of packet-based mobile broadband system like WiMAX, it is imperative for 3GPP to develop new standards and mobile technologies to ensure competitiveness for the next decade and beyond in order to meet the increasing demand of the network services, in terms of higher data rates, reduced latency, improved system capacity and coverage. LTE/SAE proposes to fulfill these requirements by using an IP converged architecture system which is able to work across multiple access networks. Thus, LTE was first introduced in Release 8 in 2008, while Release 9 is the LTE release with SAEs enhancement and the interoperability of LTE and WiMAX.

The overall high level objective of LTE is to provide an extremely high performance radio-access technology that provides full vehicular speed mobility and can coexist with HSPA and other previous networks. With the scalable bandwidth functionality of LTE, operators are able to migrate their networks and users from HSPA to LTE over time with ease.

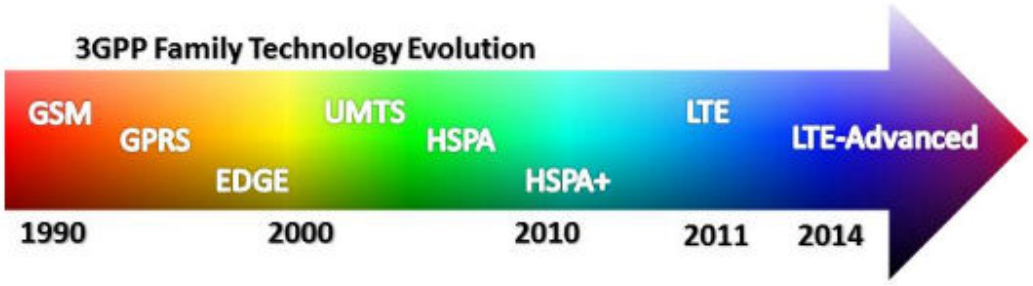

Figure 1. 3GPP family technology evolution. From [2].

LTE is able to provide unprecedented performance in terms of peak data rates, delay, and spectrum efficiency to the network when compared with its predecessors. LTE can provide up to 100 Mbps downlink data rate and up to 50 Mbps uplink data; this is four times faster than previous HSPA+ data rates. The comparison of peak data rates and other parameters between LTE and its predecessors are shown in Table 1.

Table 1. Comparison of parameters between LTE and its predecessors. From [3].

	WCDMA (UMTS)	HSPA (HSDPA/HSUPA)	HSPA+	LTE
Maximum downlink speed (bps)	384 k	14 M	28 M	100 M
Maximum uplink speed (bps)	128 k	5.7 M	11 M	50 M
Latency round trip time (approximate)	150 ms	100 ms	50ms (Max)	~10 ms
3GPP releases	Rel 99/4	Rel 5/6	Rel 7	Rel 8
Approximate years of initial roll out	2003/4	2005/6 HSDPA 2007/8 HSUPA	2008/9	
Access methodology	CDMA	CDMA	CDMA	OFDMA/SC-FDMA

A LTE evolution update report researched and published by Global mobile Suppliers Association (GSA) dated January 5, 2012, [4] confirms that 49 LTE operators have already launched commercial services. These 49 LTE operators have launched LTE networks services in 29 countries, which include Armenia, Australia, Austria, Bahrain, Belarus, Brazil, Canada, Denmark, Estonia, Finland, Germany, Hong Kong, Hungary, Japan, Kuwait, Latvia, Lithuania, Norway, Philippines, Poland, Puerto Rico, Saudi Arabia, Singapore, South Korea, Sweden, UAE, Uruguay, USA, and Uzbekistan. The countries with deployed LTE services are shaded in red in Figure 2.

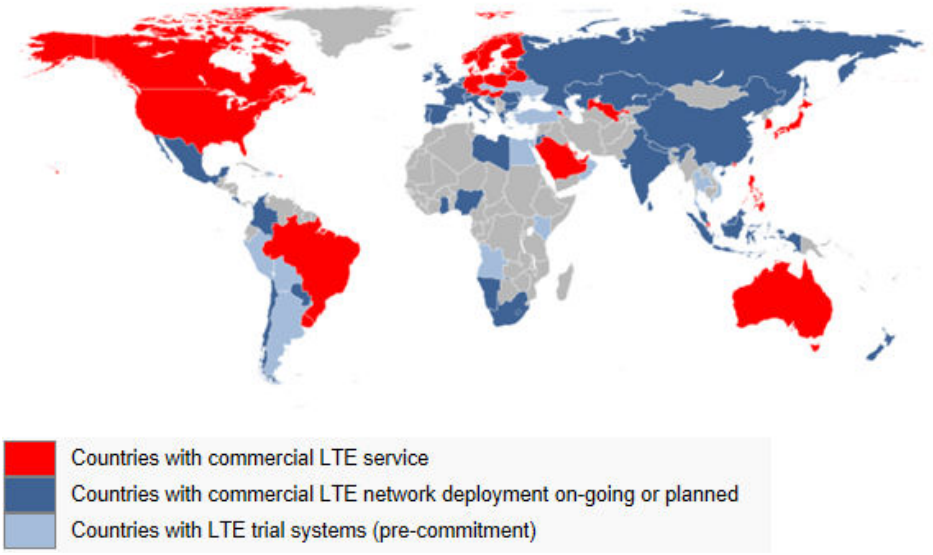

Figure 2. 3GPP LTE evolution country map. From [5].

The GSA report also confirms that 285 operators in 93 countries have committed to commercial LTE network deployments or are engaged in trials, technology testing or studies. This includes the 49 commercial LTE network that are already launched, 117 deployments that are in progress or planned in 76 countries, and another 59 operators in 17 other countries that are engaged in LTE technology trials, tests or studies.

This report suggests that the operators around the world have strengthened their commitment and investment in the LTE technology, and GSA forecast that there will be 119 commercial LTE networks in more than 50 countries by the end 2012.

The motivations for the growth of interest in LTE are as follows: continued competitiveness of the 3G system, user demand for higher data rates and QoS, packet switch 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 [6].

There are several key features of LTE discussed in [7]. These features are access scheme, data rate, latency, mobility, spectrum allocation, frequency bands, scalable bandwidth, cell size, supported users, internetworking with legacy network, packet switched radio interface and support or Multicast-Broadcast Single Frequency Network (MBSFN).

For the access scheme feature, LTE uses orthogonal frequency-division multiple access (OFDMA) for the downlink and single carrier frequency-division multiple access (SC-FDMA) for the uplink. The major parameters for LTE are shown in Table 2.

For the date rate feature, the peak download rates can support up to 299.6 Mbit/s and upload rates up to 75.4 Mbit/s, depending on the User Equipment (UE) category. Five different terminal classes have been defined from a voice centric class up to a high-end terminal that supports peak data rates. The download and upload rates for respective UE Categories are shown in Table 3.

For the latency feature, in optimal conditions, the data transfer latency is low at sub-5 ms for small IP packets. This is lower for handover and connection set-up time than with previous radio access technologies.

For mobility features, there is also an improved support for mobility, exemplified by support for terminals moving at up to 350 km/h or 500 km/h depending on the frequency band [8].

For the spectrum allocation feature, the LTE supports frequency-division duplexing (FDD) and time-division duplexing (TDD) communication systems as well as half-duplex FDD with the same radio access technology.

For the frequency bands feature, LTE supports all frequency bands currently used by International Mobile Telecommunications (IMT) systems. For the scalable bandwidth feature, LTE includes increased spectrum flexibility, with 1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz and 20 MHz wide cells standardized.

For the cell size feature, LTE supports cell sizes from tens of meters radius (femto and picocells) up to 100 km radius macrocells. In the lower frequency bands to be used in rural areas, 5 km is the optimal cell size, 30 km having reasonable performance, and up to 100 km cell sizes supported with acceptable performance. In city and urban areas, higher frequency bands (such as 2.6 GHz in the EU) are used to support high speed mobile broadband. In this case, cell sizes may be 1 km or even less.

For the supported user feature, LTE supports at least 200 active clients in every 5 MHz cell [9]. For internetworking with legacy network, LTE supports the inter-operation and co-existence with legacy standards.

For the MBSFN feature, LTE can deliver services such as Mobile TV using the LTE infrastructure and is a competitor for DVB-H-based TV broadcast.

Several key enablers are required to achieve the aggressive performance targets of the LTE. The identified key enablers for the LTE are orthogonal frequency-division multiplexing (ofdm), multiple-input multiple-output (MIMO), and system architecture evolution (SAE). [10]

The OFDM technology is an enabler in LTE because of its capability to transmit at high data bandwidth efficiently while providing resilience to reflection and interference. OFDMA is used in the downlink to achieve high peak data rates in high

spectrum bandwidth and SC-FDMA is used in the uplink because its small peak-to-average power ratio; the more constant power enables high RF power amplifier efficiency in mobile handsets, which is an important factor for battery power equipment.

Table 2. Major parameter for LTE Release 8. After [6].

Access Scheme	Uplink	DFTS-OFDM
	Downlink	OFDMA
Bandwidth		1.4, 3, 5, 10, 15, 20 MHz
Minimum TTI		1 ms
Sub-carrier spacing		15 kHz
Cyclic prefix length	Short	4.7 μs
	Long	16.7 μs
Modulation		QPSK, 16QAM, 64QAM
Spatial multiplexing		Single layer for Uplink per UE Up to 4 layers for downlink per UE MU-MIMO supported for uplink and downlink

Table 3. User equipment categories for LTE Release 8. After [6].

Category		**1**	**2**	**3**	**4**	**5**
Peak rate (Mbps)	Downlink	10	50	100	150	300
	Uplink	5	25	50	50	75
Capability for physical functionalities						
RF bandwidth		20MHz				
Modulation	Downlink		QPSK, 16QAM, 64 QAM			
	Uplink		QPSK, 16QAM			
Multi-antenna						
2 RX diversity		Assumed in performance requirements				
2x2 MIMO		Not supported	Mandatory			
4x4 MIMO		Not supported				Mandatory

The MIMO technique is an enabler because one of the main problems encountered by previous telecommunications systems was that multiple signals arose from the many reflections that are encountered along the path. These signals would reach the destination at different times and result in a disrupted waveform signal. With the

usage of MIMO, these additional signal paths can be used as an advantage to increase the throughput. MIMO antenna technology enables ten times as many users per cell as 3GPP's original WCDMA access technology [6].

Lastly, the SAE enables the system architecture to evolve in order to handle the very high data rate and low latency requirements for 3G LTE. One of the significant changes to the system architecture is that a number of the functions previously handled by the core network have been transferred out to the periphery. This leads to a "flatter" form of network architecture and allows direct routing of the data to the destination, which in turn reduces the latency times.

With the superior features that LTE can provide, LTE is the next generation wireless data communications standard that is poised to dominate mobile data connectivity in both the commercial and military. In the commercial sector, a disruption in service due to security reasons can jeopardize the reputation and reduce the revenue of the service provider. In the military sector, the integrity and the timely transmission of data are of upmost importance. Any compromise may result in failure of the mission.

Security is indispensable for secured communication between users and mobile networks. The increasingly important role of LTE has brought about a number of security concerns among the service provider and end users. The aim of this thesis is to provide a comprehensive analysis on the potential weakness of the LTE protocol.

B. PROJECT OBJECTIVE

Security within the LTE system has become extremely important to ensure secured communication of the user terminals accessing network services. The security and robustness of the LTE standard, especially those of its control channels in Layer 2, namely, Radio Link Control (RLC), Medium Access Control (MAC) and Packet Data Convergence (PDCP), need to be further examined.

C. SCOPE OF THESIS

The scope of the thesis includes the review of the LTE protocol standards and the assessment of existing threats to LTE system, followed by an exploration of methods of

hacking into and manipulating the control channel without the other party's knowledge. This thesis research can serve as a starting point to protect, as well as to exploit, protocol weaknesses in LTE and, thus, open exploitation space.

D. APPROACH/STRUCTURE

The literature related to the LTE network is briefly discussed in Chapter II. In particular, available literature related to security issues is reviewed and security vulnerabilities are identified. The LTE specifications are examined, and several other potential security weaknesses of the features and mechanisms, especially those related to the control channels within the LTE network's Layer 2 protocol, are identified.

In Chapter III, some of the important technical aspects of 3GPP are discussed. Some basic technologies and methods employed in LTE, which include OFDM, OFDMA, SC-FDMA and MIMO, are explored. A general overview of LTE architecture, the different protocol layers and their interaction within the LTE network, followed by the threat model and LTE's security architecture are presented in Chapter III. Finally, the details of sub-layer protocols, namely, RLC, MAC and PDCP within the LTE network's Layer 2 protocol, are elaborated on.

In Chapter IV, LTE's power control mechanisms are explored and the unprotected power control signal is exploited to conduct attacks on UEs and degrade their intended services. The ways that an adversary can maliciously manipulate the power control mechanism's control field in order to sabotage the victim UE are demonstrated. This chapter concludes by evaluating the impacts of the attack.

In Chapter V, the results of the thesis are summarized and the potential research issues related to the security of LTE are discussed.

II. LITERATURE REVIEW

A. OVERVIEW

The majority of research related to LTE began in 2008, after the release of the first LTE standard by 3 GPP. As the objective of the thesis is to examine the security and robustness of the LTE standard, the literature review is related to materials discussing the security aspect of LTE. A relatively small amount of research has been done on the security of LTE, and only a limited number of security exploitations in LTE have been discussed extensively in the published literature. There is, however, literature that serves to provide a background and presents a tutorial overview of proposed security mechanisms in Evolved Packet System (EPS), which lists some open security issues and key threats in LTE at that time.

The threats discussed in [11] are the illegal access and usage of user's and mobile equipment's (ME')s identities, the tracking of user based on UE's identity and signaling messages, the illegal access and usage of keys used in security procedures, the malicious modification of UE parameters to deny UE of normal services, the tampering with the system information broadcasted to the Evolved Universal Terrestrial Radio Access Network (E-UTRAN), the denial-of-service (DoS) to the UE, and the replaying attacks which affect the integrity of data. These threats to the LTE network were not further elaborated in [11].

B. AUTHENTICATION PROTOCOL AND KEY MANAGEMENT ENHANCEMENT IN LTE

Several researchers have done work to enhance the robustness of the security protocol and mechanism in LTE.

The authors in [12] describe the LTE security architecture and mobility procedures related to key management techniques in order to minimize the effects of a possible key compromise in the access points. They go on to compare in detail LTE's key management security properties with the session keys context (SKC) concept. The

authors conclude that LTE could benefit from the SKC type of key management since SKC concept is simpler and allows higher key distributor scalability, while the security properties are quite similar.

The authors in [13] survey and compare three authentication protocols candidates: Password Authentication Protocol (PAP), Lightweight Extensible Authentication Protocol (LEAP) and Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) for LTE network. The conclusion is that PAP and LEAP are vulnerable to dictionary attacks. EAP-TLS can provide reliable security performance, but has considerable overhead.

The research in [14] examines the weaknesses and strength of the Authentication and Key Agreement protocol (EPS-AKA) and identifies the protocol's potential weaknesses. A new authentication protocol, Enhanced EPS-AKA (EAKA), is proposed which provides full (online) mutual entity authentication between ESIM (Enhanced Subscriber Identity Module) and Home Subscriber Server (HSS) and removes the need for delegated authentication.

C. WEAKNESS OF IP CONVERGED LTE NETWORK

A survey of security threats conducted in [15] shows that the reason for the unexpected service disruption and disclosure of information is the inherent weakness of the converged Internet Protocol (IP) architecture of the LTE. The IP network is susceptible to conventional attacks like IP address spoofing, user ID theft, theft of service and DoS and intrusion attacks; these attacks are extended to the LTE network. In addition, as mentioned in [16], the network is vulnerable to the known computer network attack techniques such as man-in-the-middle (MITM), eavesdropping, Trojan, virus and malware. Security vulnerabilities in the IP can jeopardize the entire IP converged LTE network.

D. VULNERABILITIES OF NON-ACCESS-STRATUM (NAS) OF E-UTRAN

The authors in [40] study the vulnerabilities of the Non-Access Stratum (NAS) of E-UTRAN and illustrate attacks that exploit these vulnerabilities. The transmission of the unprotected Radio Resource Control (RRC) messages and the transmission of

International Mobile Subscriber Identity (IMSI) in plain text without confidentiality and integrity protection are discussed in the article. In addition, the CRNTI information in Layer 1 provides attackers the opportunities to track an UE across cells. The exploitation of these vulnerabilities allows the attackers to launch efficient and effective DoS attacks on the eNodeB.

E. THREATS EXPLOITING LAYER 2 INFORMATION

To the best of our knowledge, [17] is the only available reference that deals with identifying threats and attacks by manipulating the information in MAC and RRC signaling messages. The focus of [17] is on the security and privacy threats in radio interface between eNodeB and the UE. There are two identified threats; the first threat is the tracking of UE location based on the unique CRNTI, cell level measurement reports or packet sequence numbers, and the second threat is the message insertion attack in UE's long discontinuous reception (DRX) period.

The long DRX period allows the UE to periodically switch off the processing elements to save on the limited battery power and improves on power consumption's efficiency. However, this introduces extended delays when the UE needs to transmit or receive data and may pose a security loophole for the system while the UE is "inactive" during the long DRX period. The UE is vulnerable to attacks during this period; these attacks includes false buffer status report attack which either steal bandwidth by changing the packet scheduling behavior or changes the behavior of load balancing /admission control algorithms in the eNodeB.

F. INVESTIGATION OF LTE SPECIFICATION

Investigation of the LTE specifications revealed that there are vulnerabilities within the LTE's Layer 2 protocol. In this thesis, these vulnerabilities are identified and the working principles are discussed briefly. The focus is on exploring LTE's power control mechanism. The ways to exploit the unprotected fields of the power control message and attacks to the victim UE are detailed in Chapter IV.

Some of the potential vulnerabilities include the malicious modification of control PDU type reserve field, the prioritized retransmission of traffic data, and the malicious modification of power control mechanism. These are discussed in the following sections.

1. Malicious Modification of Control PDU Type Reserve Field

The STATUS PDU is sent by the receiver to feedback on the status of the received PDU. The control PDU type field is 3 bits and the STATUS PDU is indicated by 000, while 001-111 are reserved. PDUs with this reserved coding will be discarded by the receiving entity for this release of the protocol (Release 10). The adversary can maliciously adjust the control PDU type field to the reserved value and the recipient will not be able to recognize and subsequently discard the STATUS PDU.

2. Prioritized Retransmission of Traffic Data

The Radio Link Control (RLC) priority ruling [29] states that "the transmitting side of an Acknowledged mode (AM) RLC entity shall prioritize retransmission of RLC data Protocol Data Unit (PDUs) over transmission of new AM PDUs." This implies that when the transmitter receive a negative acknowledge on the previously PDU, it will retransmit the missing PDU, instead of transmission of new data. This creates an opportunity for the adversary to manipulate status update of the victim UE to negative acknowledgement. This tricks the transmitter into continuously prioritizing and allocating resource for the retransmission and reduces the chance of transmitting the legitimate data.

3. Malicious Modification of Power Control Mechanism

The power control mechanism for LTE involves transmission of explicit TPC control command to increase or decrease the transmission power of the UE. The adversary can exploit the unprotected power control signal to conduct attacks on the UEs and degrade their intended services**.** The impacts include depleting the limited battery power of the UE at a faster rate, increasing interference to the neighboring cells.

III. TECHNICAL BACKGROUND

Some of the important technical aspects of 3GPP LTE are discussed in this chapter. The basic technologies and methods employed in LTE, which include OFDM, OFDMA, SC-FDMA, and MIMO, are discussed in the following sections. In addition, an overview of LTE architecture and the details of Layer 1 and Layer 2 protocols followed by the LTE security and proposed threat model are presented. This aim of this chapter is to provide the reader a preliminary background on LTE and aids him/her in understanding the problem to be discussed in Chapter IV.

A. LTE TECHNOLOGY BASICS

The LTE physical layer employs several advanced technologies to convey both control and data information between the eNodeB and the UE. These techniques include OFDM and MIMO data transmission.

1. OFDM

Most cellular systems prior to LTE used single-carrier modulation schemes. Although LTE uses OFDM instead of single-carrier modulation, it is imperative to understand how the previous single-carrier systems dealt with multipath-induced channel distortion and contrast that with OFDM systems. Graphical representations of single-carrier transmission and OFDM in the frequency domain are shown and contrasted in Figure 3.

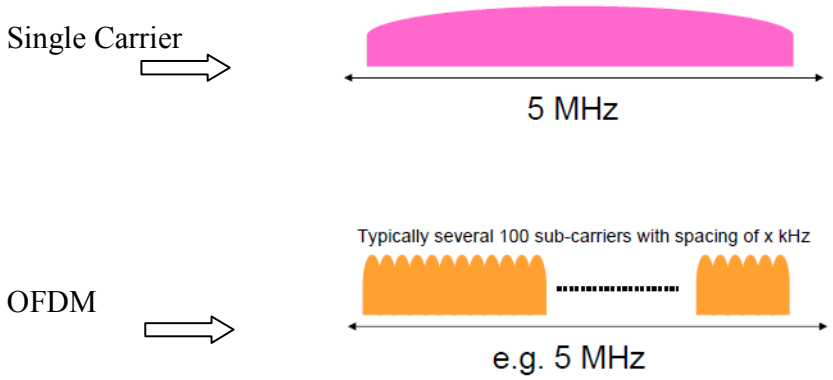

Figure 3. Representation of single-carrier transmission and OFDM in the frequency domain. From [18].

In a communication system, delay spread refers to the amount of time delay at the receiver from a signal travelling from the transmitter along different paths [19]. The delay caused by multipath transmission can result in a received symbol from a delayed path to "bleed" into a subsequence symbol that arrived at the receiver via the direct path. This effect is known as inter-symbol interference (ISI) and is shown in Figure 4. In general, the single-carrier system symbol time decreases as data rate increases, and it is possible for ISI to spill into a second or third subsequent symbol at very high data rate.

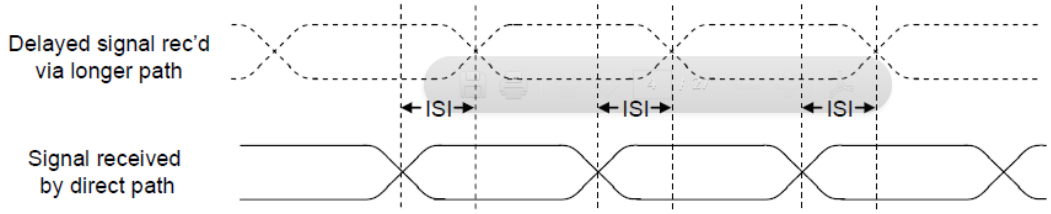

Figure 4. Multipath-induced time delays result in ISI. From [19].

Single-carrier systems usually compensate for channel distortion via time domain equalization using either channel inversion or equalizers [19].

In channel inversion, a known sequence is transmitted over the channel prior to sending actual information. As the original signal is known at the receiver, a channel equalizer is able to determine the channel response and multiply the subsequent data-bearing signal by the inverse of the channel response to reverse the effects of multipath.

CDMA systems can employ equalizers to resolve the individual paths and then combine digital copies of the received signal shifted in time to enhance the receiver signal-to-noise ratio (SNR).

The implementation of channel equalizers is more complex as data rates increase. The symbol times are shorter, and ISI is much more severe. The data rates of LTE is up to 100 Mbps and delay spreads are about 17 μs [19]; thus, the approach of channel equalization is unfeasible. Hence, OFDM is introduced, which eliminates ISI and greatly simplifies the task of channel compensation.

LTE system employs OFDM as the downlink transmission scheme due to its robustness against frequency selective-fading and narrowband interference. In OFDM,

the available bandwidth is spilt into multiple, narrow bandwidth sub-carriers and the data is transmitted in parallel steams. Each sub-carrier is then independently modulated using conventional modulation schemes such as quadrature phase-shift keying (QPSK), 16 quadrature amplitude modulation (QAM) or 64QAM and transmitted over the closely spaced, orthogonal sub-carriers. A representation of the OFDM signal in the frequency and time domain is shown in Figure 5. The problem of ISI is more severe as the data transmission rate increases, and this problem occurs because the channel delay spread is greater than the symbol period when the data is transmitted as a serial stream.

In OFDM, this problem is avoided by converting the data stream into multiple, parallel sub-carriers. This conversion creates an OFDM symbol that is generally much longer than the symbol on single-carrier systems and, thus, greater than the channel delay spread. In Figure 5, the guard interval, which is the cyclic prefix (CP), is inserted prior to the OFDM symbol in the time domain to eliminate ISI due to channel delay spread. The use of narrow-band sub-carriers combined with the CP makes the transmission of OFDM symbols inherently robust to the time dispersion on the channel and eliminates the need for complex channel equalization on the receiver end. This property greatly simplifies the processing required for the UE, which in turn reduces the terminal cost and the power consumption.

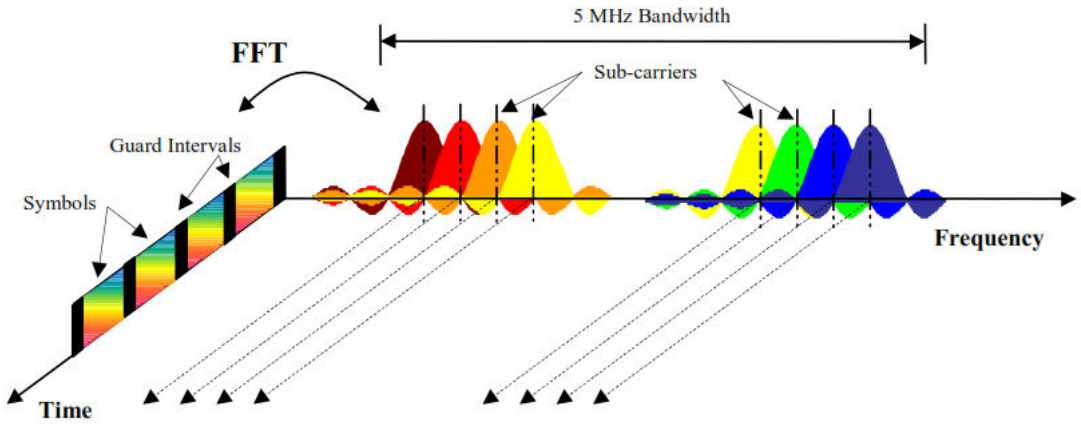

Figure 5. Frequency-time representation of an OFDM signal. From [20].

The generation of the OFDM signal is based on the inverse fast Fourier transforms (IFFT), as illustrated in Figure 6. As shown in Figure 6, the IFFT converts *N* frequency domain symbol streams to *N* complex time domain samples. These time domain samples are then serialized to create the time domain signal.

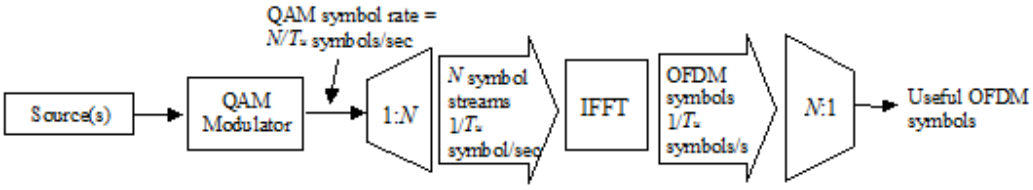

Figure 6. OFDM signal generation chain. From [20].

The superiority of OFDM to single-carrier systems in term of its ability to eliminate ISI is discussed in previous section. OFDM, however, has two primary weaknesses when compared to the single-carrier systems. OFDM is sensitive to carrier frequency errors and has a large signal peak-to-average power ratio (PAPR).

One of the problems for OFDM is that it is sensitive to carrier frequency errors due either to local oscillator offset or Doppler shifts [19]. Different reference frequencies used in the transmitter and receiver can cause inter carrier interference (ICI) and result in the loss of OFDM orthogonality. Also, the use of a cost effective local oscillator in the UE may cause drifting of frequency and result in carrier frequency offset (CFO), which may be greater than sub-carrier spacing.

Another disadvantage of OFDM is that it has a large signal PAPR. Amplitude variations in the transmitted power of the single OFDM symbol are high because the OFDM symbol is a combination of all of the sub-carriers, and the power these sub-carriers can vary significantly. A high PAPR increases the dynamic range requirement of the analog-to-digital and digital-to-analog converters and also reduces the efficiency of the transmitter's radio frequency (RF) power amplifier. The usage of a more expensive transmitter capable of accommodating these requirements is often the remedy to the large PAPR.

2. OFDMA

In an OFDM transmission scheme, a single user receives all the sub-carriers at one time. On the other hand, in an OFDMA transmission scheme, different users can receive different subsets of sub-carriers simultaneously. Each user is allocated a specific time-frequency resource, where data is transmitted over different sub-carriers over a certain time period. The transmission scheme can be viewed in term of the time and frequency domain. OFDM allocates resources to users in the time domain only, while OFDMA allocates resources to users in both the time and frequency domains. A contrast in the preceding transmission schemes is illustrated in Figure 7.

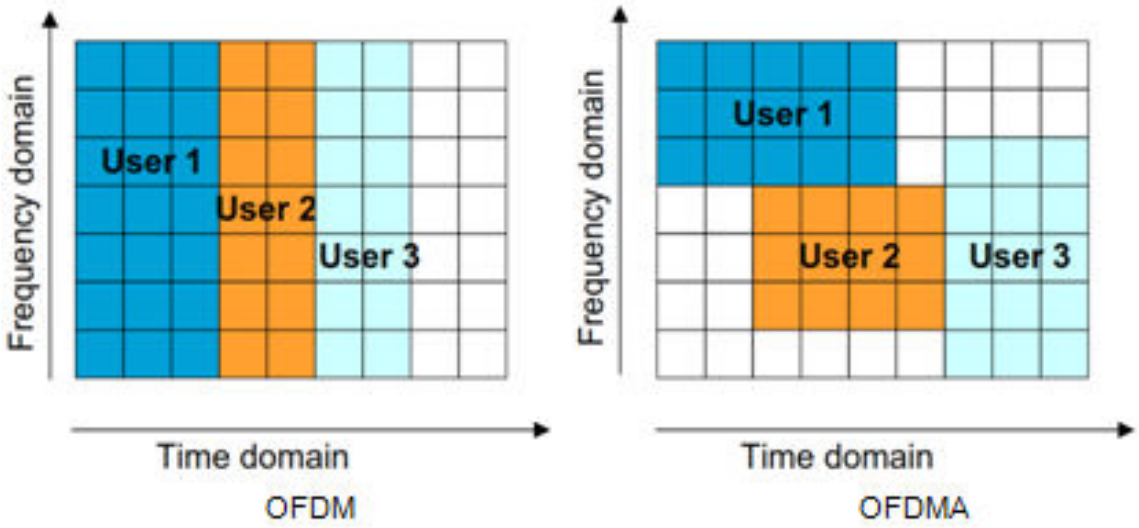

Figure 7. Contrast between transmission schemes of OFDM and OFDMA. From [18].

3. SC-FDMA

OFDMA is able to fulfill LTE's high transmission data rate requirement while eliminating ISI in the downlink as discussed in the previous section. The properties of OFDMA signals, in particular the high PAPR, result in poorer uplink coverage. This property makes it less favorable as an uplink transmission scheme for LTE.

SC-FDMA is selected as the LTE uplink transmission scheme since it can achieve the benefits that OFDM brings to LTE because of similarities in the signal processing

properties of both transmission schemes. At the same time, SC-FDMA has a low PAPR. This low PAPR characteristic is especially important for the design of a cost-effective power amplifier for the UE.

The principle of discrete Fourier transform (DFT)-spread-OFDM is used to generate the SC-FDMA signal as illustrated in Figure 8. The process is that an *N*-point DFT is first input to a block of modulation data symbols in order to transform these modulation symbols into frequency domain. The output of the transformed signal is then mapped to the available sub-carriers, which then pass through an *M*-point IFFT operation block. This is followed by parallel-to-serial conversion and the addition of CP. There are two main schemes to implement the sub-carrier mapping, namely localized and distributed. In a localized scheme, each user uses a set of adjacent sub-carriers to transmit data. In a distributed scheme, each user uses sub-carriers that are spread across the entire bandwidth.

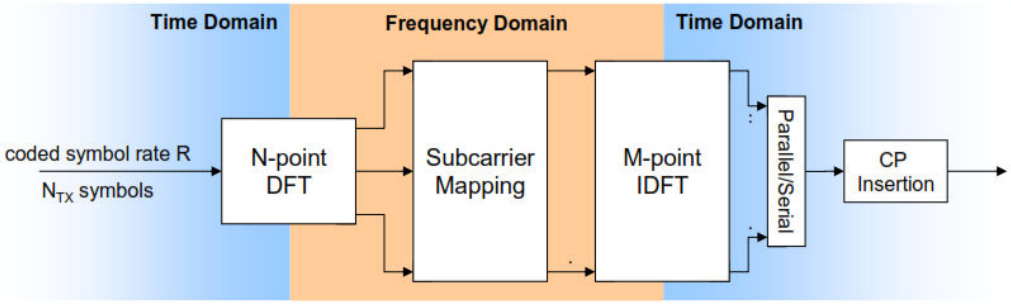

Figure 8. SC-FDMA signal generation chain. From [18].

In OFDM, each data symbol is modulated to each sub-carrier individually at a given instant, and the digital modulation represents the amplitude of the respective sub-carrier. Each sub-carrier of an OFDM signal carries information related to one specific symbol. In contrast, in SC-FDMA, a linear combination of all the transmitted data symbols at a given instant is modulated to a given sub-carrier, and all the transmitted sub-carriers of the SC-FDMA signal carry a component of respective modulated data symbols. Thus, each sub-carrier of the SC-FDMA signal carries information of all the transmitted symbols. The representation of OFDMA and SC-FDMA signals are shown in Figure 9.

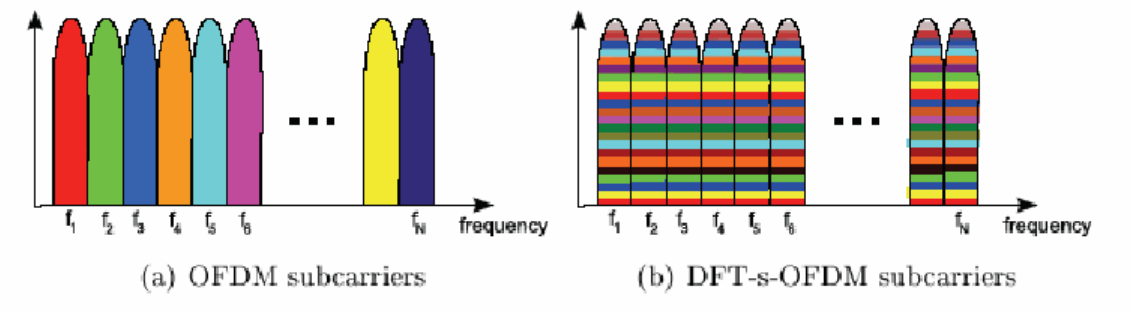

Figure 9. Representation of OFDM and SC-FDMA signals. From [18].

4. MIMO Concept

MIMO technology is one of the key enablers for LTE to achieve the ambitious requirement for high throughput and spectral efficiency through the use of multi-antenna techniques at both the transmitter and receiver in the network. The improved performance is achieved without additional bandwidth or increased transmission power. This 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 [19].

On a high level, LTE multi-antenna transmission can be divided into two modes, namely spatial multiplexing and transmit diversity. Spatial multiplexing uses non-orthogonal MIMO codes to increase the bandwidth, while transmit diversity uses orthogonal MIMO cods to increase power while preserving bandwidth. The use of one MIMO mode or another depends on the radio channel condition.

Spatial multiplexing is a technique that allows transmission of multiple, different data streams simultaneously on the same downlink resource block and is only possible if the channel allows it [20]. These data streams can belong to a single user, which significantly increases the peak rate of one user. These data streams can also belong to different users, which increase the overall capacity. The principle of spatial multiplexing is illustrated in Figure 10. As shown in Figure 10, spatial multiplexing exploits the channel's spatial dimension. The transmitted data stream go through a channel, which

consists of all N_tN_r paths between the N_t transmit antennas at the transmitter and the N_r receive antennas at the receiver. This channel can be represented by the channel matrix $\boldsymbol{H}$, where h_{ij} represents the complex gain of the channel between the jth transmitter and the ith receiver, as shown in Figure 11.

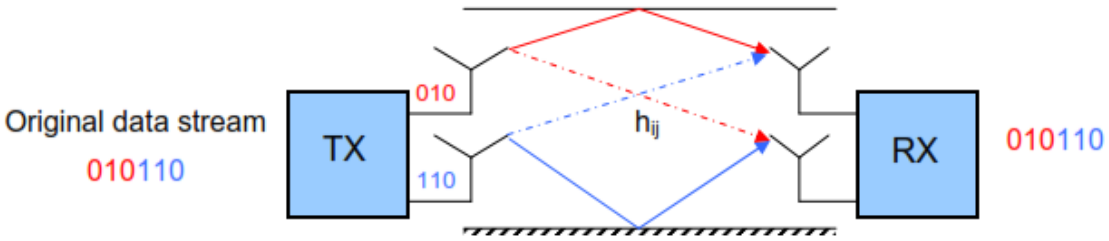

Figure 10. Principle of spatial multiplexing. From [20].

$$H = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1Nt} \\ h_{21} & h_{22} & & h_{2Nt} \\ \vdots & \vdots & \ddots & \vdots \\ h_{Nr1} & h_{Nr2} & \cdots & h_{NrNt} \end{bmatrix}$$

Figure 11. Channel matrix $\boldsymbol{H}$. From [21].

On the other hand, transmit diversity can be used to increase the robustness of the data transmission instead of increasing the data rate. Transmit diversity is a technique for coherently adding the signals received from two transmit antennas. As the antennas are physically separated, different channel impulse responses reduce the impact of deep fading that occurs on each of the antenna, respectively, thereby enhancing the link reliability.

5. Generic Frame Structure

LTE physical layer transmission is deployable in two modes: frequency-division duplexing (FDD) and time-division duplexing (TDD), each of which has its own frame structure. The frame structure defines the frame slot and symbol in the time domain. Although the uplink and downlink data transmission schemes are different, they share a common frame structure.

Frame structure type 1 is defined for FDD mode, and the structure is as shown in Figure 12. The LTE data transmission is segmented into frames which are 10 ms in duration. Each frame consists of 10 sub-frames, and each sub-frame is further divided into two slots period of 0.5 ms duration each.

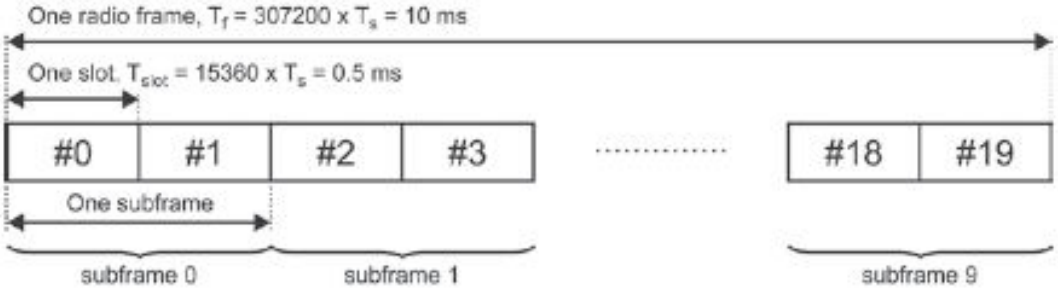

Figure 12. LTE frame structure type 1. From [22].

Frame structure type 2 is defined for TDD mode and is shown in Figure 13. The LTE data transmission is also segmented into frames which are 10 ms in duration. Each frame consists of two half frames. The half frame is further divided into four sub-frames and a special sub-frame, or five sub-frames depending on the downlink to uplink switch point periodicity. The special sub-frames consist of three fields: Downlink Pilot Timeslot (DwPTS), Guard Period (GP) and Uplink Pilot Timeslot (UpPTS).

The frame structure of TDD can exist in seven different sub-frame format configurations, with sub-frames 0 and 5 and DwPTS always reserved for downlink transmission. The sub-frame that follows after the special sub-frame and UpPTS is assigned to uplink transmission. The various uplink-downlink configurations are shown

in Table 4, where D denotes a sub-frame reserved for downlink transmission, U denotes a sub-frame reserved for uplink transmission, and S denotes the special sub-frame.

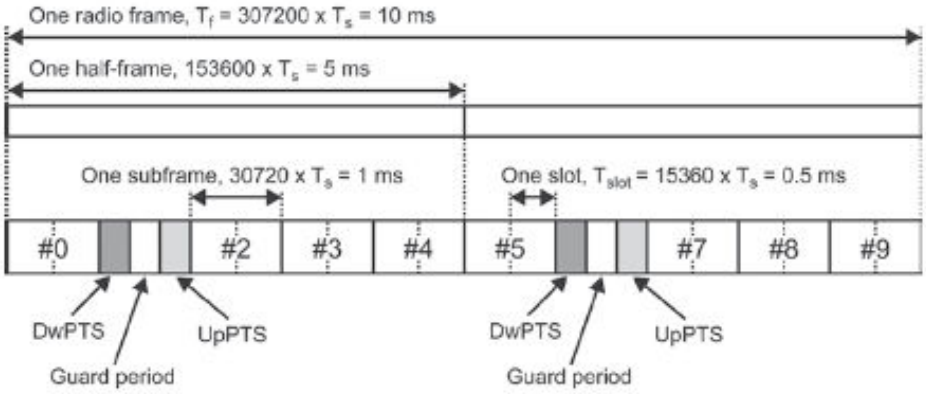

Figure 13. LTE frame structure type 2 (5 ms switch point periodicity). From [22].

Table 4. Uplink-downlink configuration for LTE frame structure type 2 [22].

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

6. Physical Resource Block

A physical resource block (PRB) is the smallest element of resource allocation assigned by the base station scheduler [23]. LTE is a system with scalable bandwidth. The current LTE specification defines six sets of supportable bandwidth from 1.4 MHz to 20 MHz with the corresponding PRBs required as shown in Table 5. 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. A resource block comprises of seven columns of OFDM symbols and 12 rows of sub-carriers, which constitutes 84 resource elements, as shown in Figure 14.

Table 5. Resource block configuration for different channel bandwidths. From [24].

Channel bandwidth $BW_{Channel}$ [MHz]	**1.4**	**3**	**5**	**10**	**15**	**20**
Transmission bandwidth configuration N_{RB}	6	15	25	50	75	100

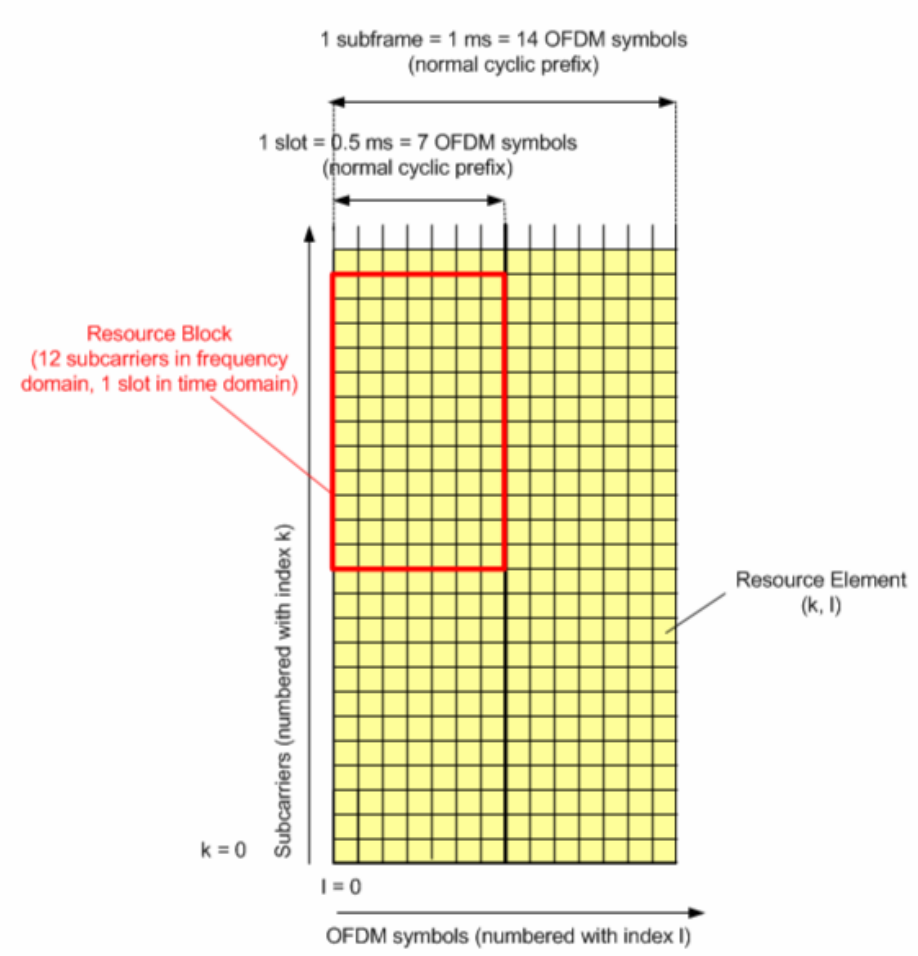

Figure 14. Downlink resource grid. From [24]

7. Supportable Frequency Bands

The LTE specifications inherited the frequency bands defined for UMTS and extended the list as shown in Table 6, where each E-UTRAN operating band with its corresponding uplink and downlink operating band and duplex modes are displayed.

Table 6. LTE operating band. From [24].

E-UTRA 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
...			
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
NOTE 1: Band 6 is not applicable			

B. LTE NETWORK ARCHITECTURE OVERVIEW

The high-level view of the LTE architecture network is shown and the interaction of the various elements and interfaces are illustrated in Figure 15.

The architecture of the LTE is comprises of three main building blocks. They are the UE, E-UTRAN and the Evolved Packet Core (EPC).

The UE is a mobile unit that allows a user to access network services, connecting to the E-UTRAN via the radio interface.

The E-UTRAN consists of eNodeBs, which is another name for base stations, and provides the user-plane (PDCP, RLC, MAC and physical layers) and control-plane

(RRC) protocol terminations towards the UE. The eNodeBs are typically interconnected to each other by the X2 interface, enabling direct communication. The EUTRAN is connected to the EPC by means of the S1 interface, and this connects the eNodeBs to the mobility management entity (MME) and serving gateway (S-GW) elements.

The EPC is the core network in the LTE/System Architecture Evolution (SAE) system and is responsible for overall control of the UE and establishment of the bearers, which are the traffic flows between the UE and the Packet Data Network Gateway (P-GW). The EPC is comprised of logical nodes, namely, P-GW, S-GW and MME.

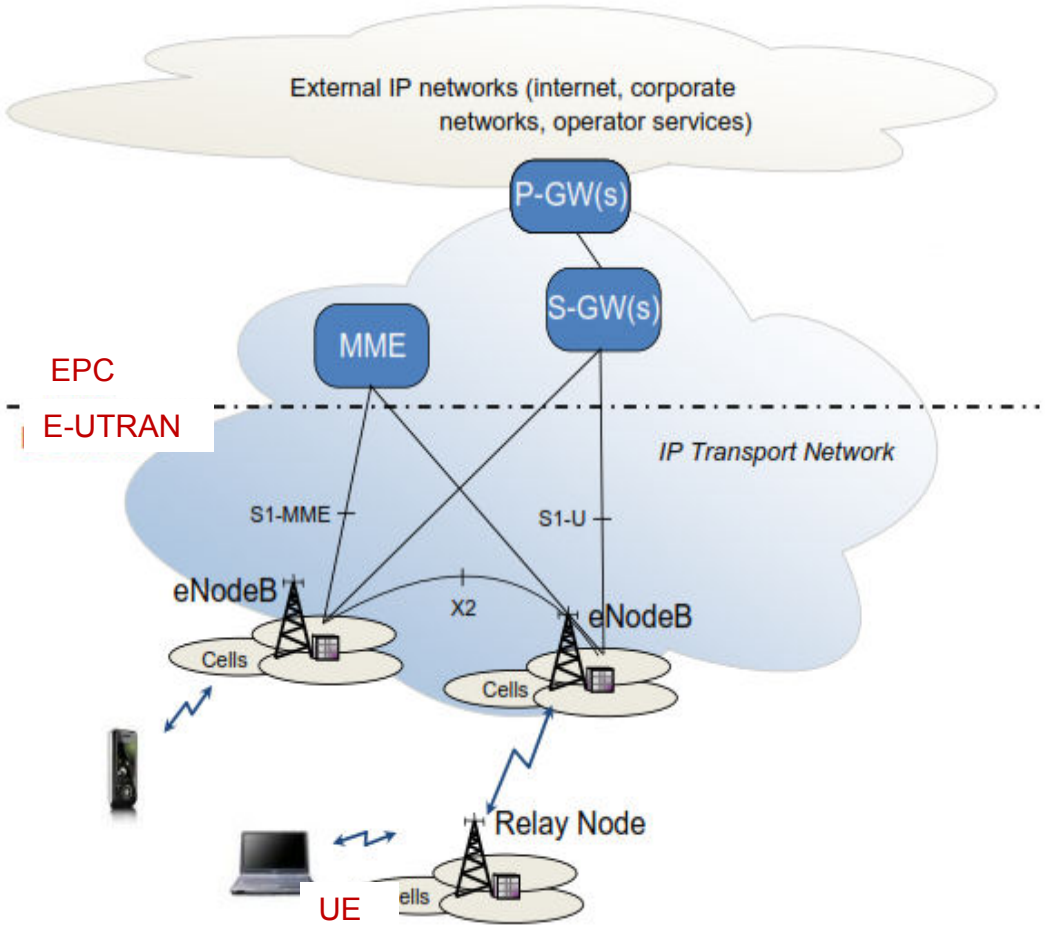

Figure 15. High level architecture of LTE. After [25].

The functional split between the E-UTRAN and EPC is shown in Figure 16. The yellow boxes in Figure 16 represent the logical nodes, white boxes represent the functional entities of the control plane, and the blue boxes represent the radio protocol layers.

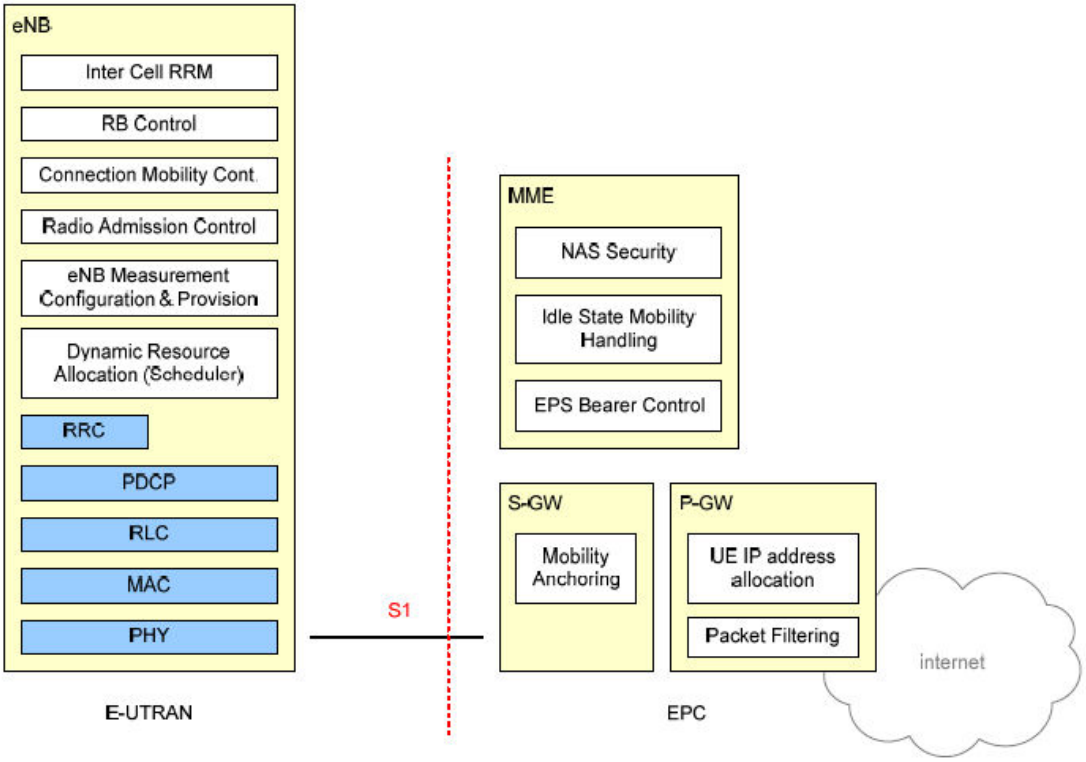

Figure 16. Functional split between the E-UTRAN and EPC. From [26].

The functions of the logical node eNodeB include radio resource management, IP header compression and encryption of user data stream, the selection of an MME, the routing of user plane data towards S-GW, the scheduling and transmission of paging message, broadcast information and public warning system messages, the measurement and measurement reporting configuration for mobility and scheduling, closed subscriber group (CSG) handling that allows a permitted group of user to access a particular cell, and a transport level packet marking in the uplink. [26]

The functions of the logical node MME are non-access stratum (NAS) signaling (i.e., the signaling between the protocols that operates between UE and the Core Network

(CN)), NAS signaling security, access stratum (AS) security control, and inter-CN node signaling for mobility between 3GPP access networks. [26]

The functions of the logical node S-GW include acting as the local mobility anchor point for inter-eNodeB handover and mobility anchoring for inter-3GPP mobility, E-UTRAN idle-mode downlink packet buffering and initiation of network triggered service request procedure, lawful interception, and packet routing and forwarding.

The functions of the logical node P-GW consist of per-user based packet filtering, lawful interception, UE IP address allocation, transport level packet marking in the uplink and the downlink, and uplink and downlink service level charging, gating and rate enforcement.

A comprehensive list of the functions offered by the logical nodes can be found in 3GPP 36.300. [26]

The user plane protocol stack consists of MAC, RLC and PDCP sub-layers that are terminated at eNodeB as shown in Figure 17. The functions of these sub-layers are discussed in the following sections. The control plane protocol stack is similar to user plane protocol stack, with the exception of additional Radio Resource Control (RRC) sub-layer terminated at eNodeB and NAS protocol terminated at MME, as shown in Figure 18.

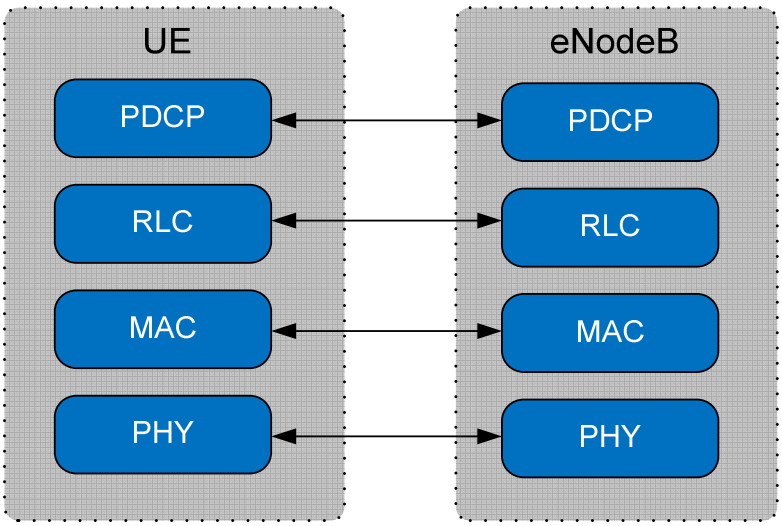

Figure 17. User plane protocol stack. After [26].

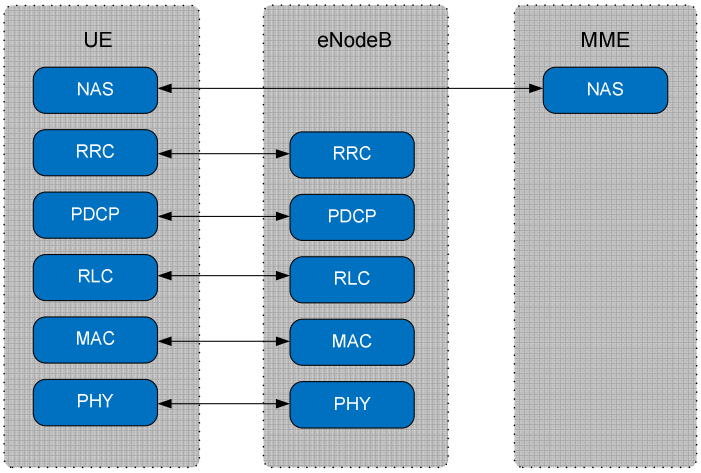

Figure 18. Control plane protocol stack. After [26].

C. NETWORK AND PROTOCOL ARCHITECTURE

The relationships of the IP packet with the Protocol Data Unit (PDU) and Service Data Units (SDU) at the respective layers are illustrated in Figure 19. In a data transmission from the eNodeB to the UE, each protocol layer receives a SDU from higher layer and appends the respective layer header to form and send the PDU to the lower layer. In this study, the main focus is on the Layer 2 protocol. The PDCP, RLC and MAC layers together constitute the Layer 2.

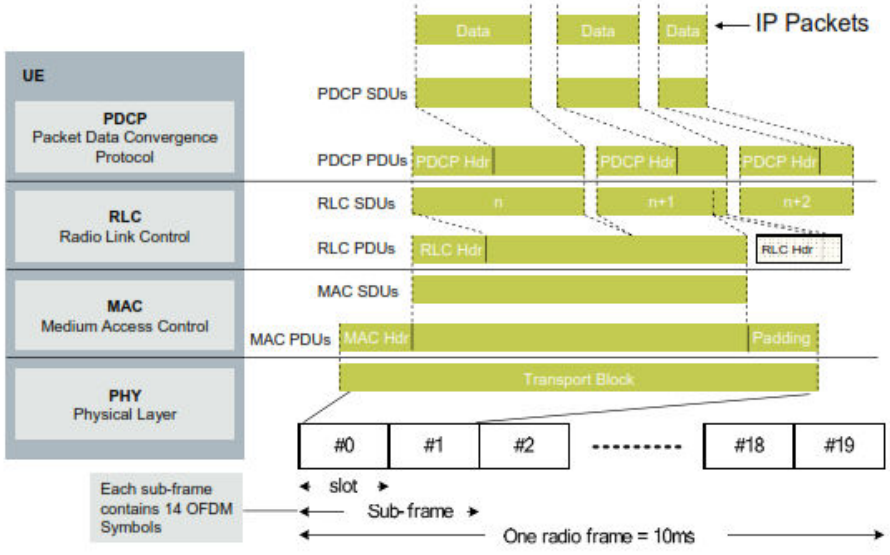

Figure 19. Transmission of data in LTE downlink in time domain. From [27].

1. MAC [28]

The MAC layer is mainly responsible for managing the mapping of logical channels to the appropriate transport channels and the multiplexing and de-multiplexing MAC SDUs between the physical and RLC layer. The various logical and transport channels within LTE standard are illustrated in Figure 20 and Figure 21, respectively. The supported mappings between these logical and transport channels for the downlink are displayed in Figure 22, while those for the uplink are displayed in Figure 23. The main transport channel for the downlink is DL-SCH while that for uplink is UP-SCH, as shown in Figure 22 and 23, respectively. Other functions performed by MAC are the hybrid automatic repeat request (HARQ) for retransmission function, scheduling information reporting, and priority handling between UEs by means of dynamic scheduling, priority handling between logical channels of one UE, logical channel prioritization, and transport format selection.

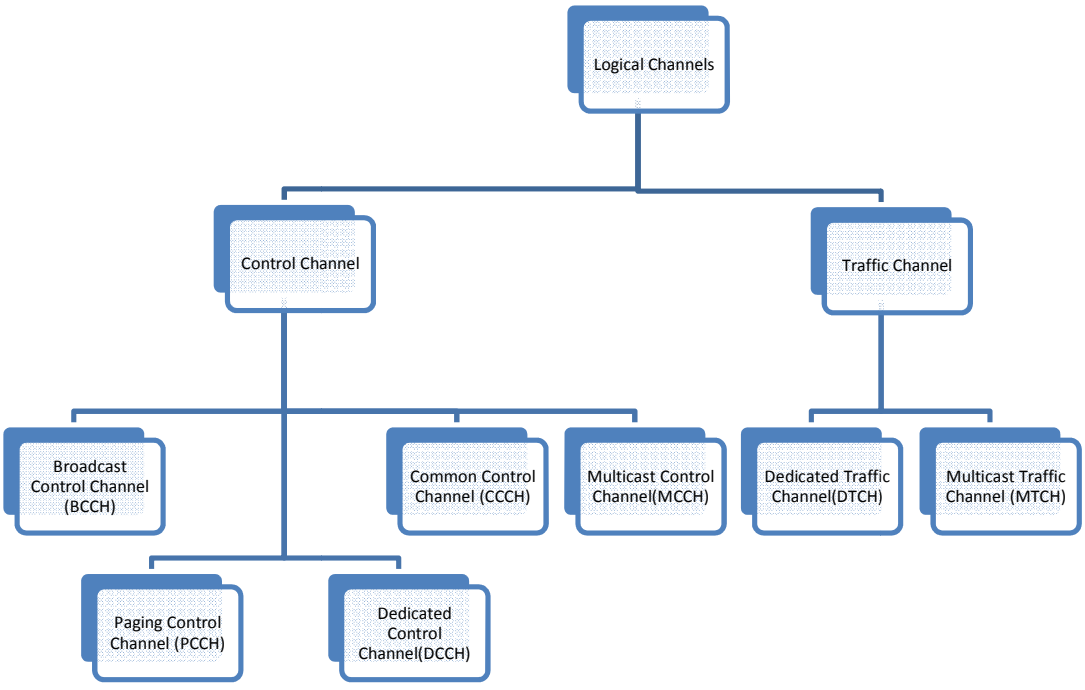

Figure 20. Logical channels in LTE. After [28].

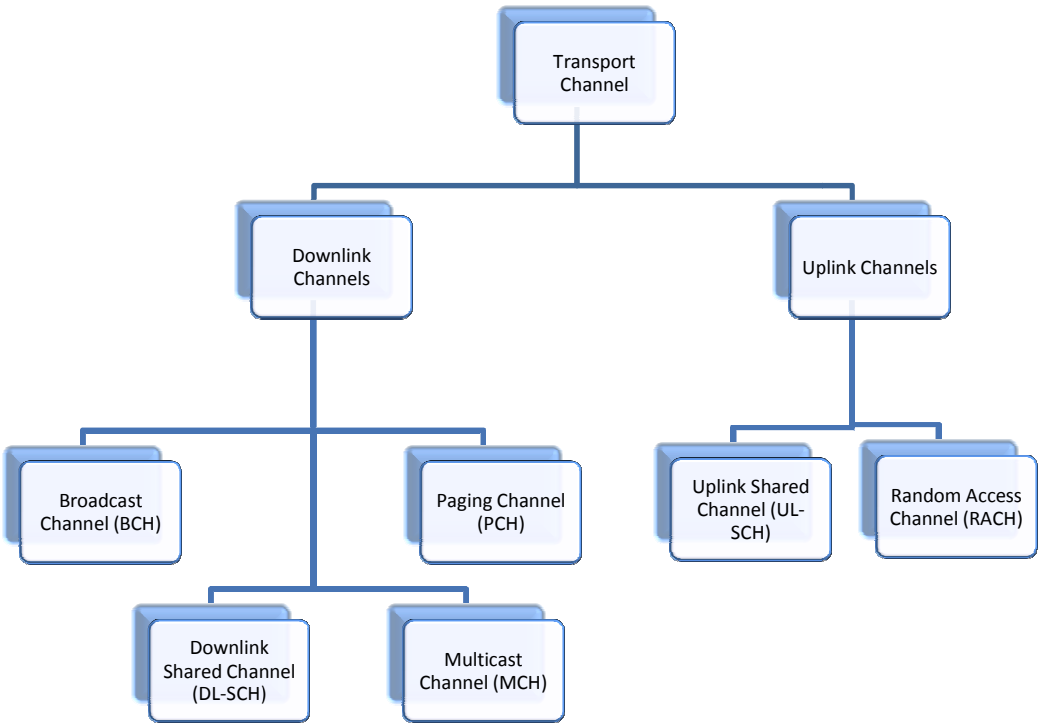

Figure 21. Transport channels in LTE. After [28].

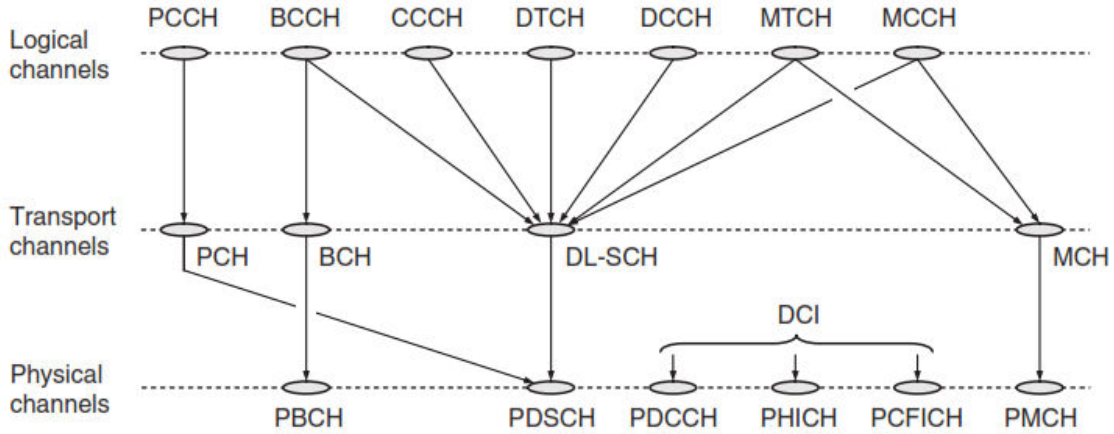

Figure 22. Downlink mapping of logical to transport channels in LTE. From [29].

The physical channels defined in LTE include the physical broadcast channel (PBCH), which carries part of the system information required by the terminal in order to

access the network. The physical downlink shared channel (PDSCH) is used for unicast transmission and for transmission of paging information. The physical downlink control channel (PDCCH) is used for downlink control information, mainly scheduling decisions and for scheduling grants enabling transmission on the physical uplink shared channel (PUSCH). The physical hybrid-ARQ indicator channel (PHICH) carries the hybrid-ARQ acknowledgement to indicate to the terminal whether a transport block should be retransmitted or not. The physical control format indicator channel (PCFICH) is a channel providing the terminals with information necessary to decode the set of PDCCHs. The physical uplink shared channel (PUSCH) is the uplink counterpart to the PDSCH. The physical uplink control channel (PUCCH) is used by the terminal to send hybrid-ARQ acknowledgements, indicating to the eNodeB whether the downlink transport block(s) was successfully received or not, to send channel-status reports aiding downlink channel-dependent scheduling, and for requesting resources to transmit uplink data upon. Finally, the physical random access channel (PRACH) is used for random access. [29]

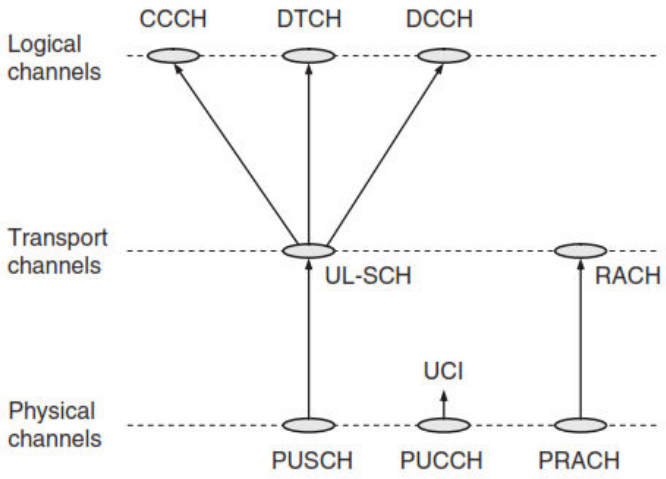

Figure 23. Uplink mapping of logical to transport channels in LTE. From [29].

2. RLC [30]

The RLC layer is the interface between the upper layers to the MAC layer as illustrated in Figure 24. The RLC layer at the transmitter end is mainly responsible for

performing segmentation of RLC SDUs, where the IP packet is formatted to a manageable size suitable for transmission at lower layer. The RLC layer at the receiver end is responsible for the reassembly of RLC PDUs, where the PDU is formatted to fit the MAC SDU. The RLC PDU structure is shown in Figure 25. RLC also performs the reordering of RLC PDUs, duplicate detection and protocol error correction through Automatic Repeat Request (ARQ).

The RLC layer provides three different modes: acknowledged, unacknowledged and transparent for data transfer.

The functions of the acknowledged mode are as follows: the segmentation and reassembly of RLC SDUs, the addition of RLC headers, the reliability in sequence delivery service, and the suitability for carrying transmission control protocol traffic [31].

The functions of unacknowledged mode are as follows: the segmentation and reassembly of RLC SDUs, the addition of RLC headers, no guarantee of delivery, and the suitability for carrying streaming traffic [31].

In the transparent mode, there is no segmentation and reassembly of RLC SDUs, no RLC headers added, no guarantee of delivery, but it is suitable for carrying voice [31].

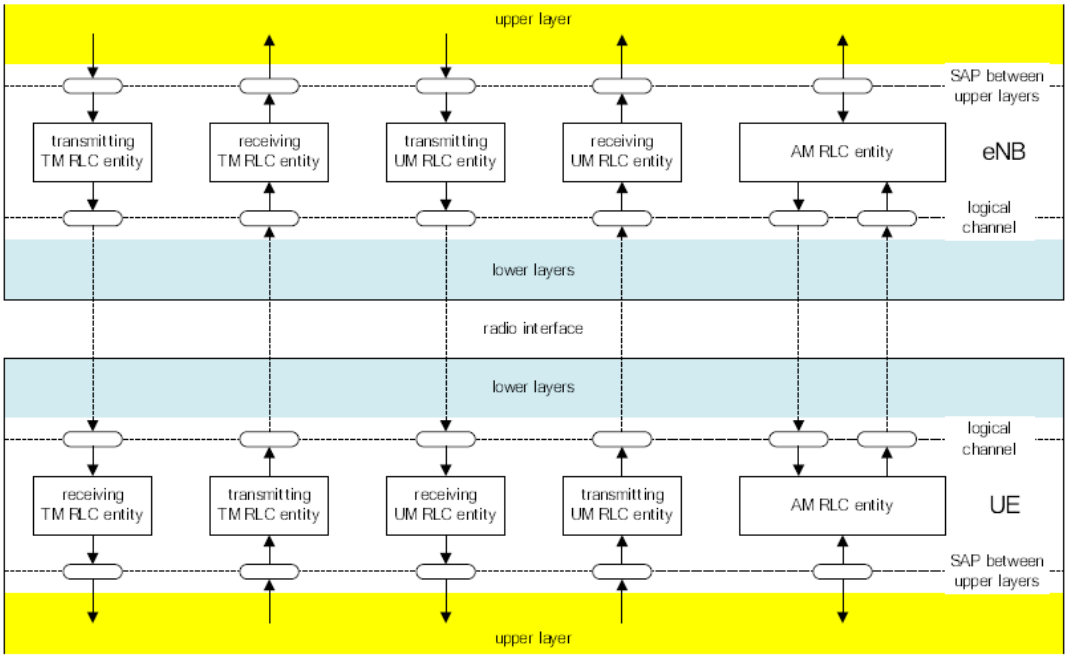

Figure 24. Overview model of RLC sub-layer. From [30].

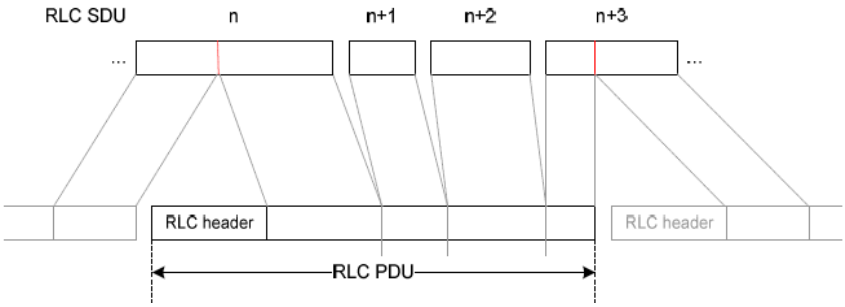

Figure 25. RLC PDU structure. From [26].

3. PDCP [31]

The PDCP layer is mainly responsible for transfer, ciphering and deciphering of user plane and control plane data. This layer also performs header compression and decompression of IP data flows using the Robust Header Compression (ROHC) protocols. Other functions performed by PDCP are integrity protection and integrity verification of control plane data, maintenance of PDCP serial numbers, timer based discard and duplicate discarding. The functional view of the PDCP layer is shown in Figure 26.

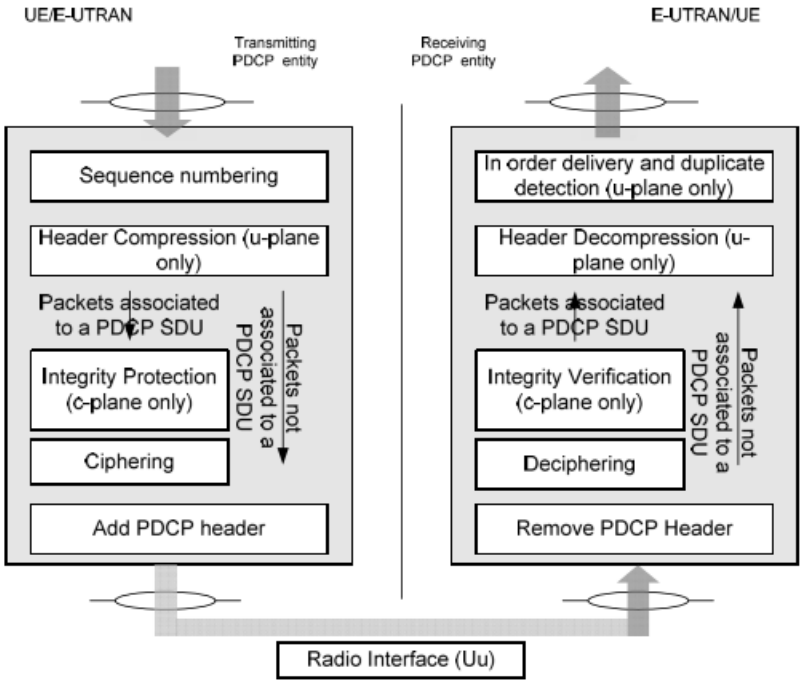

Figure 26. Functional view of PDCP layer. From [30].

4. RRC [33]

The RRC layer is part of the LTE air interface control plane. This layer is responsible for the broadcast of system information related to both the NAS and AS. It performs RRC control such as paging, establishment, modification and release of RRC connection, radio configuration and Quality-of-Service (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.

D. THREAT MODEL

The proposed threat model for the LTE network is shown in Figure 27. In this model, three elements are identified as being vulnerable to attack and are indicated by the red arrows in Figure 27. These elements are the air interface between the UE and the eNodeB, within the eNodeB, and the Internet protocol linkage between eNodeB and the S-GW. There is literature, as mentioned in Chapter II, that discusses the inherent weakness of the IP network, and these weaknesses are susceptible to attacks from Element 3. Thus, we will not discuss Element 3. Element 2, eNodeB, is typically susceptible to physical attacks. We assume that the premises are secure and do not discuss Element 2 either. The focus of this thesis is to study the possible attacks coming from Element 1, which is the air interface between the UE and eNodeB. The objective is to identify and exploit the unprotected control signaling between the UE and the eNodeB and cause disruption or degradation of services to the UEs.

E. LTE SECURITY

The LTE security architecture is designed to provide strong protection for control signaling and the user data traffic exchanges between the different entities of the LTE. The LTE architecture supports two distinct functions for the NAS and AS. The NAS function comprises of end-to-end communication between the core network and the UE. The AS function comprises of hop-by-hop communications between the network edges.

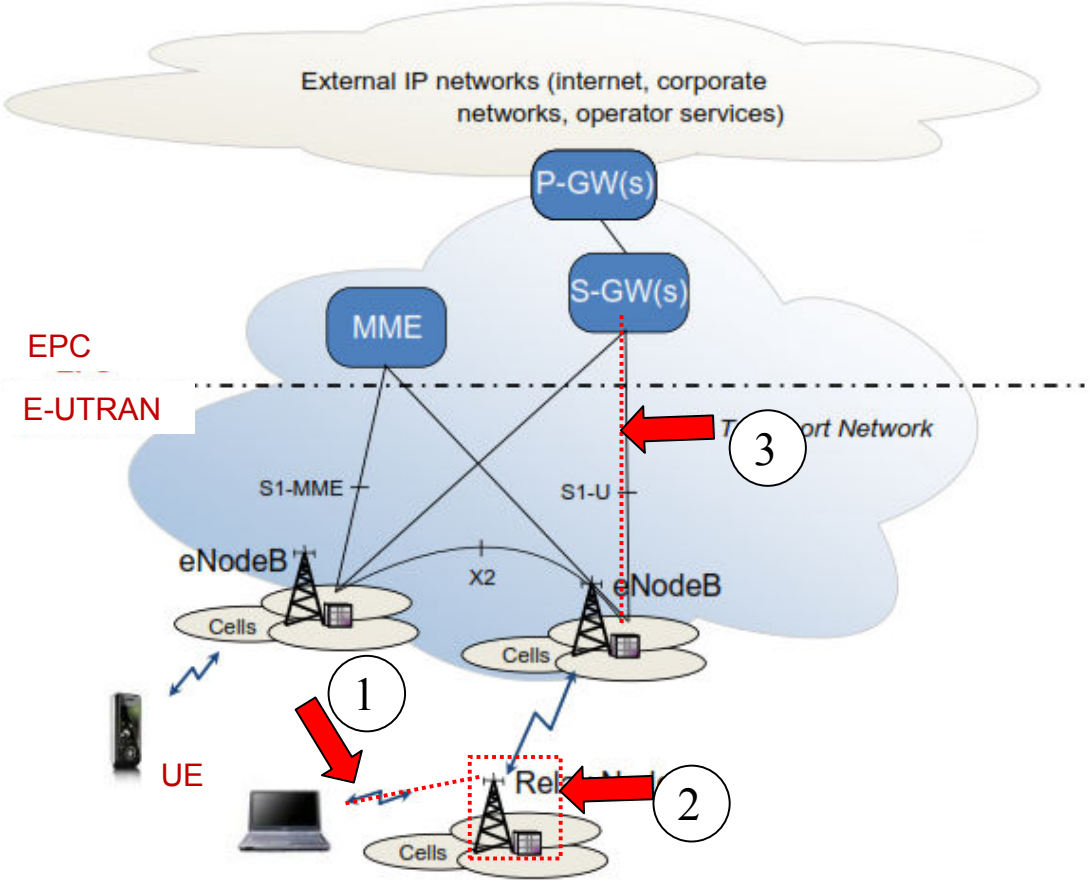

Figure 27. Threat model for LTE network. After [25].

1. Control Plane Security

The LTE entities and the signals to secure the control plane interfaces are shown in Figure 28. The control plane consists of NAS signaling between the UE and the eNodeB, RCC signaling between the UE and the eNodeB, and S1-AP signaling between the eNodeB and the MME. These signals are established between the entities and are indicated in yellow boxes as illustrated in Figure 28. Encryption and integrity protection of the NAS signaling is carried out in the NAS layer, while encryption and integrity protection of the RRC signaling is performed at the PDCP layer. IP Security (IPSec) tunneling is established between eNodeB and MME to carry the S1-AP signaling.

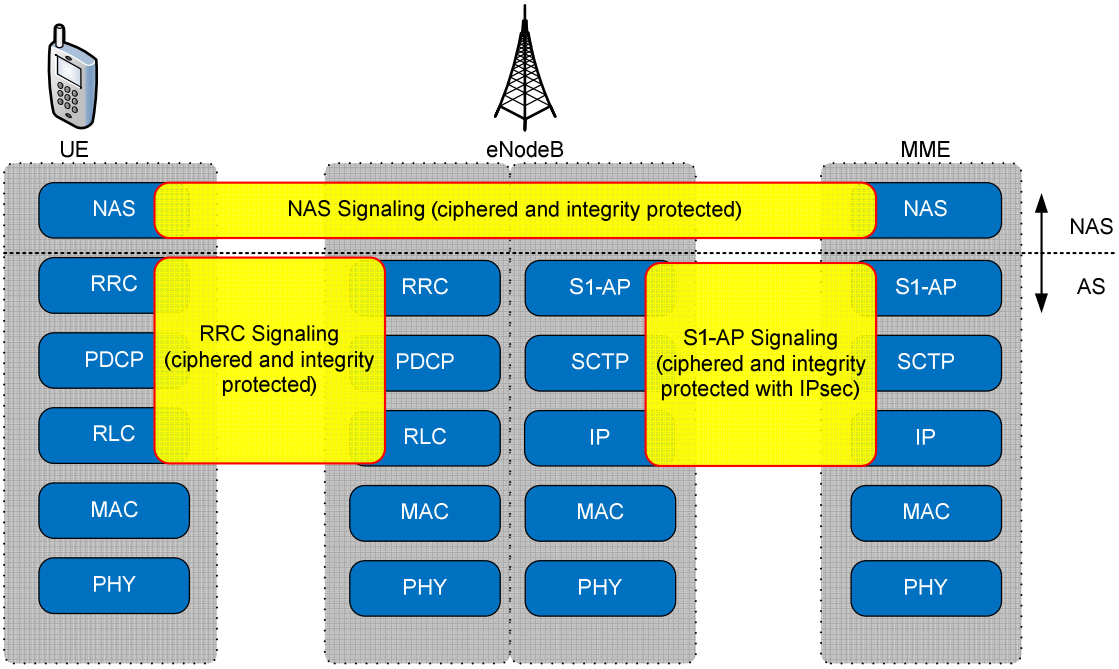

Figure 28. Control plane layered security. After [34].

2. User Plane Security

The LTE entities and mechanisms to secure user data traffic within the user plane are shown in Figure 29. The user plane is protected by application protection between the UE and the application server, user data protection between UE and the eNodeB and user data protection between eNodeB and SAE-GW. These protections are established between the entities and are indicated in yellow boxes as illustrated in Figure 29. Application providers are required to provide application layer protection between the UE and the application server. User data protection between UE and the eNodeB is provided using encryption and integrity protection at the PDCP layer, while user data protection between eNodeB and SAE-GW is provided by established IPSec tunneling [34].

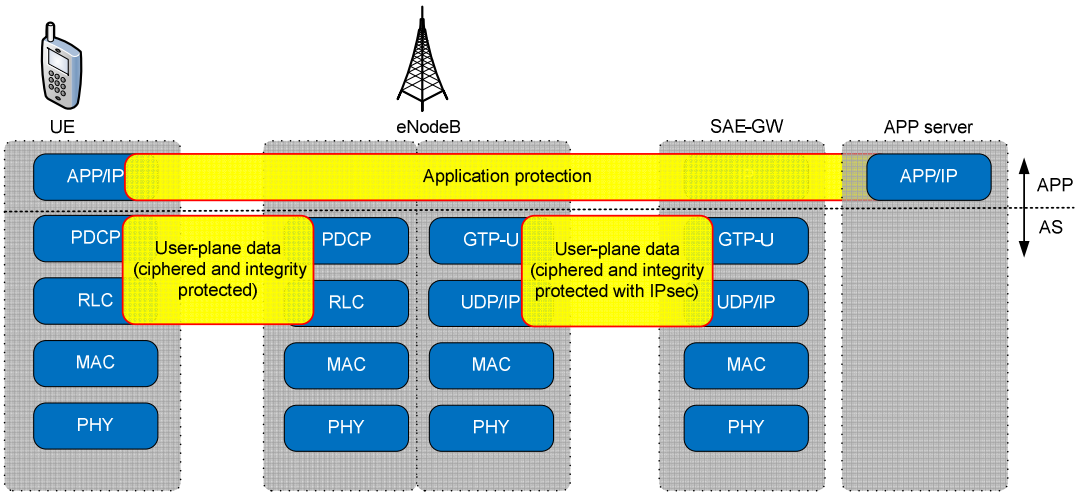

Figure 29. User plane layered security. After [34]

THIS PAGE INTENTIONALLY LEFT BLANK

IV. POTENTIAL WEAKNESS OF LTE SECURITY

Three important metrics of a mobile network are data throughput, delay, and power. The exploitation of the weaknesses in the protocol and the service mechanism that causes service disruption or degradation on these three metrics are discussed in this chapter. The disruption is typically achieved by exhausting the system's limited resources. In this paper, the LTE's power control mechanisms are explored, and the unprotected power control signal is exploited in order to conduct attacks on UEs and degrade their intended services.

The background on the cell type structure used by the LTE network, the interference experienced by UEs and eNodeB, and the power control mechanism utilized by LTE are presented in the following sections. The ways that an adversary can maliciously manipulate the control field of the power control mechanism to sabotage victim UEs are demonstrated. The impacts of an attack on the victim UE, as well as the neighboring eNodeB are evaluated at the end of the chapter.

A. CELL TYPE

In this study, the LTE is assumed to operate in network cell with 120-degree directional antennas, (i.e., each with three sectors per site/cell) with the base station in the center of cell. This is in contrast with the classic network with omni-directional antennas, which introduce more interference. The diagram of the 120-degree directional antenna lobe for one cell sector is shown in Figure 30, while the diagram of a network cell set-up with 120-degree directional antenna and adjacent cells is shown in Figure 31. In Figure 31, the different numbers represent the frequency channel band that users in the particular sector are using.

B. INTERFERENCE

The two types of interference considered include inter-cell and intra-cell interference. Inter-cell interference is generated when the same carrier frequency is used in adjacent cells. Intra-cell interference can arise in systems with non-orthogonal channelization within the same cell. The main interference to the eNodeB is due to inter-

cell rather than intra-cell interference. The amount of interference to the neighboring UEs within the same cell is effectively minimized in the ideal case since the LTE uplink is orthogonal. However, there is a substantial amount of inter-cell interference to the eNodeB from neighboring cells since adjacent cells have same frequencies assignments. Generally, the closer a UE is to the neighboring cell, the stronger the generated interference to that neighboring cell.

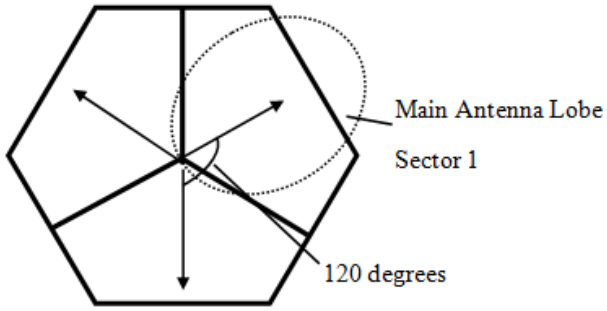

Figure 30. Center cell antenna bearing orientation diagram. From [20].

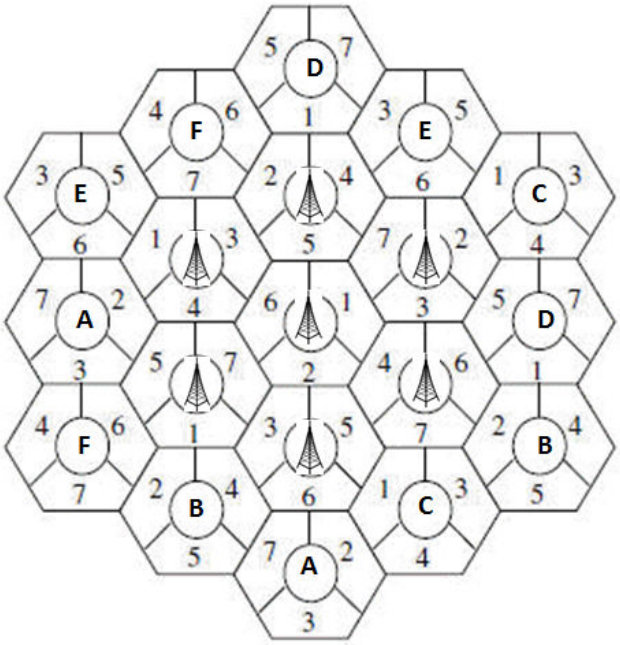

Figure 31. Diagram of the network cell set-up with 120-degree directional antenna. After [35].

C. UPLINK POWER CONTROL

Uplink power control for LTE refers to a set of tools by which the transmit power for different uplink physical channels and signals are controlled to ensure that they are received at the cell site with an appropriate power. The objectives of power control are to improve the system capacity, coverage, and user experiences while at the same time reduce the power consumption of the UE. In order to fulfill these objectives, power control mechanisms are used to maximize the desired received power signal and to minimize the amount of interference caused to the neighboring cells.

Fundamentally, the power control formula consists of two main portions. The first part is computed according to the parameters signaled by the eNodeB. The second part is computed dynamically and updated from sub-frame to sub-frame.

The overall closed loop power control for PUSCH transmission can be described according to [36]. This transmitting power P_T is set at the UE using the parameters signaled by the eNodeB and is calculated as

$$P_T = \min\{P_{\max}, P_0 + \alpha PL_{DL} + 10\log_{10}(M) + \Delta_{mcs} + \delta\}[dBm] \qquad (1)$$

where P_{max} is the maximum allowed transmit power of the particular UE class; P_o is a cell specific parameter that is broadcast as part of the system information, also seen as desired received power; α is the path loss compensation factor; PL_{DL} is the downlink path loss estimated by the UE; M is the instantaneous bandwidth in terms of number of physical resource block (PRB); Δ_{mcs} is the different SINR required for the different modulation schemes and coding rates; and δ is the explicit power control adjustment command.

Since P_{max} is fixed, and the second term of the min function in Equation (1), i.e., $P_o+\alpha PL_{DL}+10log_{10}(M)+ \Delta_{mcs}+\delta$, is variable, the UE transmit power is limited by P_{max}. In addition, the UE transmit power takes the lower value of the function in Equation (1).

To study the impact on the inter-cell interference to the eNodeB, some assumptions and simplifications on the parameters used in Equation (1) are made. In particular, P_{max} is fixed at 23 dBm [24]; P_o is assumed to be constant; α is assumed to be 1 with full compensation of path loss and is equal for all cells. In addition, the parameters PL_{DL}, M and Δ_{mcs} are assumed constant, and finally, δ is maliciously set to its maximum value.

To better appreciate the parameters involved in Equation (1), they are illustrated in Figure 32. The parameters P_o and α are signals that are broadcast at periodic intervals of 160 ms. The parameter δ is the explicit power control command signal from the eNodeB to the UEs at periodic intervals of 1 ms and constitutes to the dynamic part of the power control equation. The typical use of the explicit power control command is to compensate uplink multipath fading, which is not reflected in the downlink path loss. The parameter PL_{DL} is the path loss estimate calculated by the UE. This downlink path loss can be estimated by measuring the received power of the downlink cell-specific reference signals. The parameter P_{max} is the maximum allowed transmit power of the UE.

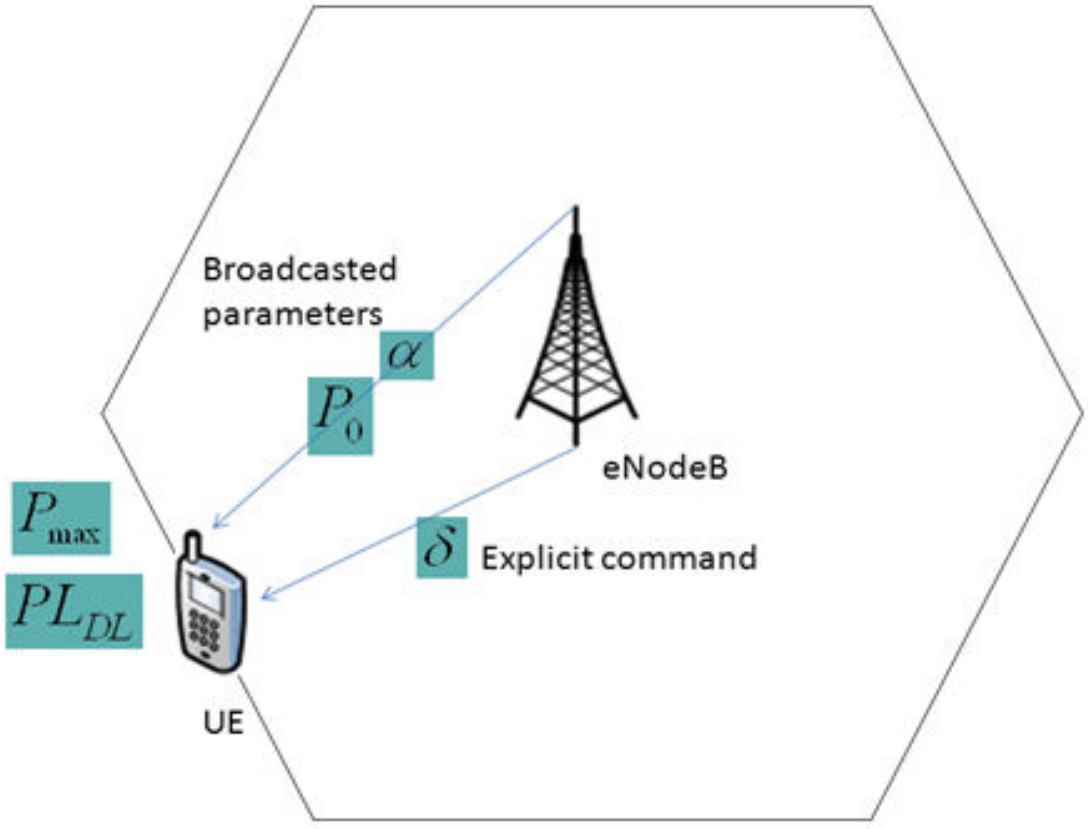

Figure 32. Power control parameters transmitted from eNodeB to UE.

1. Closed Loop Power Control Mechanism (Normal)

Uplink power control for LTE is a combination of an open-loop mechanism, where the UE transmit power depends on estimates of the downlink path loss, and closed loop mechanisms, where the network can directly control the UE transmit power by means of explicit power-control commands transmitted in the downlink.

The closed loop power control mechanism allows the UE to fine-tune the uplink transmit power based on the transmitted closed loop correction value known as the transmit power control (TPC) command. The TPC command is computed based on the desired closed loop signal-to-interference and noise ratio (SINR) and the measured (estimated) received SINR at the UE. When the received SINR is below the desired SINR target, a TPC command is transmitted to the UE to request for an increase in the transmitter power. If not, a decrease in transmitter power is requested. The computation and the steps involved in the closed loop power control are illustrated in Figure 34. In Figure 34, the boxes shaded in blue are actions performed by the eNodeB, while those in brown are actions performed by the UE.

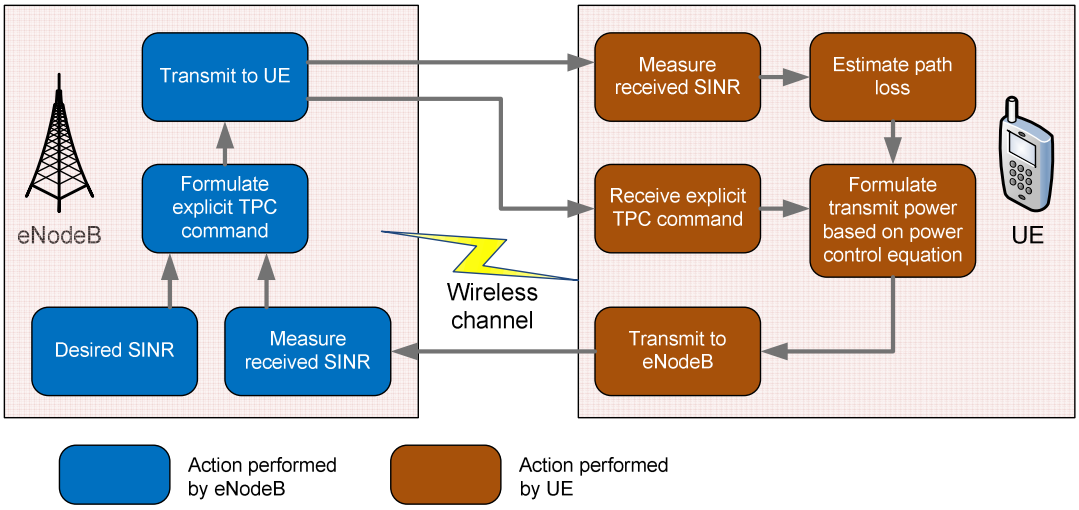

Figure 33. Block diagram of steps involved in the closed loop power control mechanism.

The objectives of the closed loop power control to provide the required SINR are to achieve an acceptable level of communication between the eNodeB and the UE and to reduce the amount of interference received by the neighboring cells. At the same time, power control aids in optimizing the limited battery power of the UE and achieves power efficiency.

2. Closed Loop Power Control Mechanism (Modified)

A malicious adversary can modify the TPC field to a large value during the feedback loop transmission from eNodeB to UE as shown in Figure 34. In Figure 34, the boxes shaded in red are actions performed by the malicious adversary. When the TPC command field is adjusted to 7, corresponding to a value of 8 dB, this can increase the transmit power to P_{max} according to Equation (1) and trick the UE into transmitting power at a higher power level. The respective TPC commands and values are shown in Table 7.

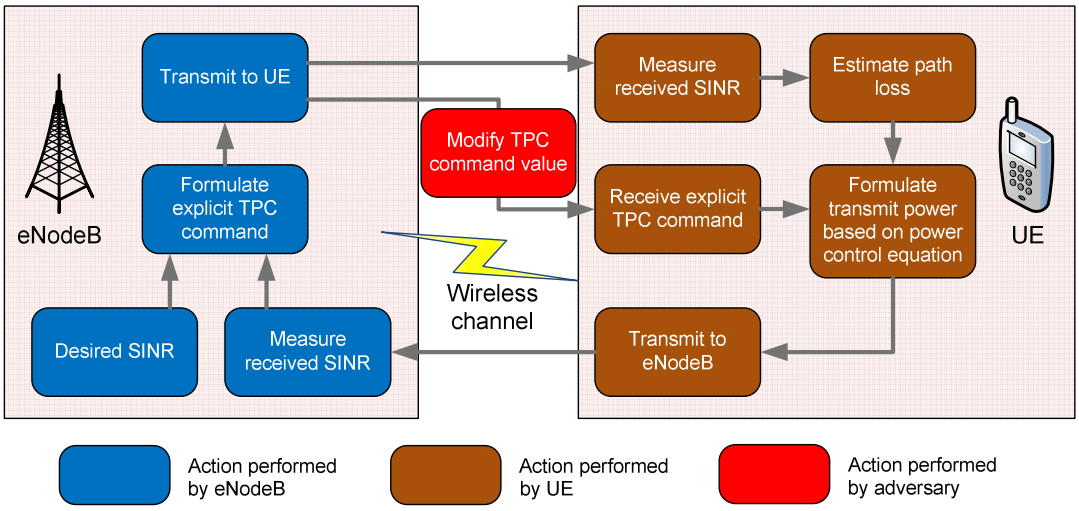

Figure 34. Closed loop power control modified by adversary.

Table 7. TPC commands with their corresponding values. From [36].

TPC Command	Value (in dB)
0	-6
1	-4
2	-2
3	0
4	2
5	4
6	6
7	8

In the case of PUSCH transmission, the explicit power control command controlling the term δ is included in the 20 bits uplink scheduling grants (UL grant). The content of the 20 bits uplink scheduling grants is as shown in Table 8.

Table 8. Content for uplink scheduling grants. From [36].

Field	**Number of bits**
Hopping flag	1 bit
Fixed size resource block assignment	10 bits
Truncated modulation and coding scheme	4 bits
TPC command for scheduled PUSCH	3 bits
UL delay	1 bit
CSI request	1 bit

The UL grant field is in the MAC Random Access Response (MAC RAR), which also consists of three other fields: R, Timing Advance Command and Temporary CRNTI as shown in Figure 35. A MAC PDU consists of a MAC header and zero or more MAC RAR as shown in Figure 36.

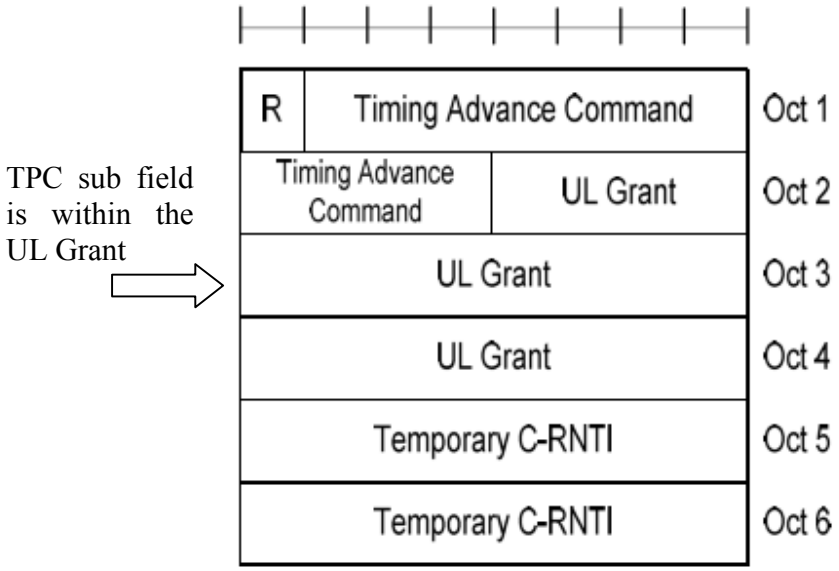

Figure 35. Structure of MAC RAR. From [28].

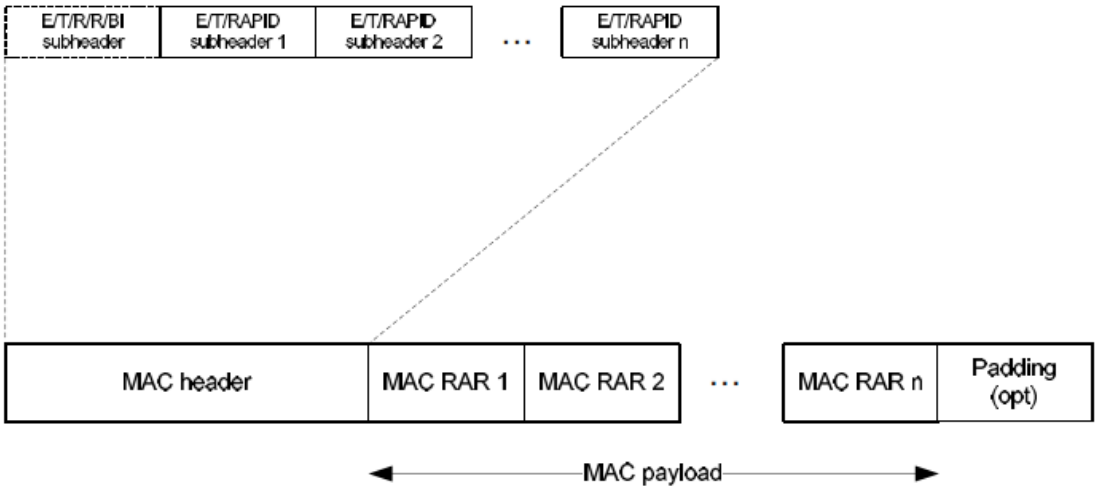

Figure 36. MAC PDU consisting of MAC header and MAC RARs. From [28].

D. SCHEDULING GRANT

The uplink scheduling grant which includes the PUSCH resource indication, transport format, and the command for power control of PUSCH uplink physical channel is carried as Downlink Control Message (DCI) by the Physical Downlink Common

Control Channel (PDCCH). To aid in understanding how to modify the TPC field in the uplink grant, it is imperative to study how this information is carried in the downlink control channel.

1. Downlink Control Signaling

Downlink control signaling is carried by three downlink control channels, namely, the Physical Control Format Indicator Channel (PCFICH), the Physical Hybrid-ARQ Indicator Channel (PHICH), and the Physical Downlink Common Control Channel (PDCCH). Downlink control signaling is located at the start of each downlink sub-frame, which spans up to the first three OFDM symbols.

The PCFICH indicates the size of the control region in term of the number of OFDM symbols used for control signaling and is located in the first OFDM symbol of the respective sub-frame. The PCFICH consists of two bits of information which correspond to a control region size of one, two or three OFDM symbols. These two bits of information are coded into a 32-bit codeword, scrambled with cell-and sub-frame-specific scrambling code, QPSK-modulated for the transmission of 16 symbols. These 16 symbols are then mapped to four Resource Element Groups (REGs) where each REG contains four Resource Elements (REs). These REGs are spread in frequency to achieve good frequency diversity. The overall processing of PCFICH is illustrated in Figure 37. The PCFICH-to-resource-element mapping depends on the cell identity to mitigate the probability of inter-cell interference.

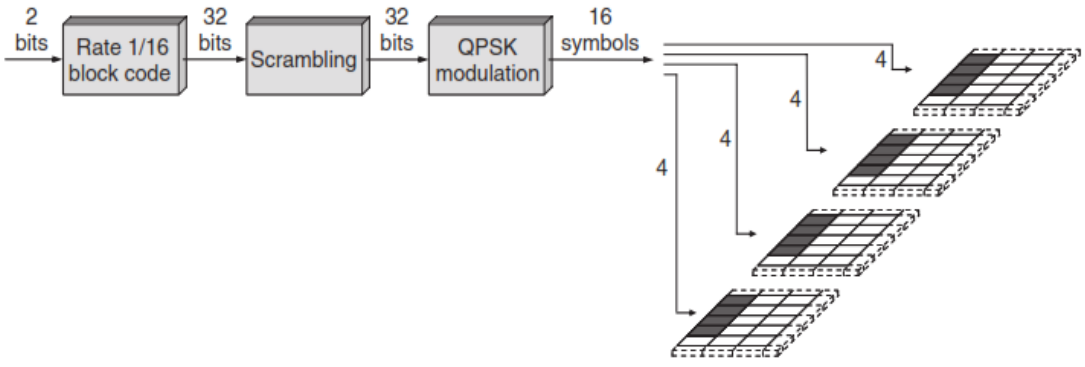

Figure 37. Overview of PCFICH processing. From [29].

The PHICH consists of one bit of information and is used to acknowledge the uplink data transmission. It is located in the first OFDM symbol of the respective sub-frame. The PHICH is spread on multiple REs to mitigate the power differences among the REs and to provide sufficient energy for the transmission. In LTE, a structure is adopted whereby several PHICHs are code multiplexed onto a set of REs as illustrated in Figure 38. A PHICH group consists of eight PHICH (in case of normal cyclic) and is transmitted on the same set of REs. As shown in Figure 39, the one bit of information for the acknowledgement is repeated three times to form three information bits. It is then modulated with binary phase-shift keying (BPSK) scheme on either the I or the Q branch, followed by the spreading with a length-four orthogonal sequence. A composite signal representing the group of PHICH is formed and scrambled. The twelve scrambled symbols are then mapped to three REGs. These REGs are spread across frequency to achieve good frequency diversity and to avoid inter-cell interference.

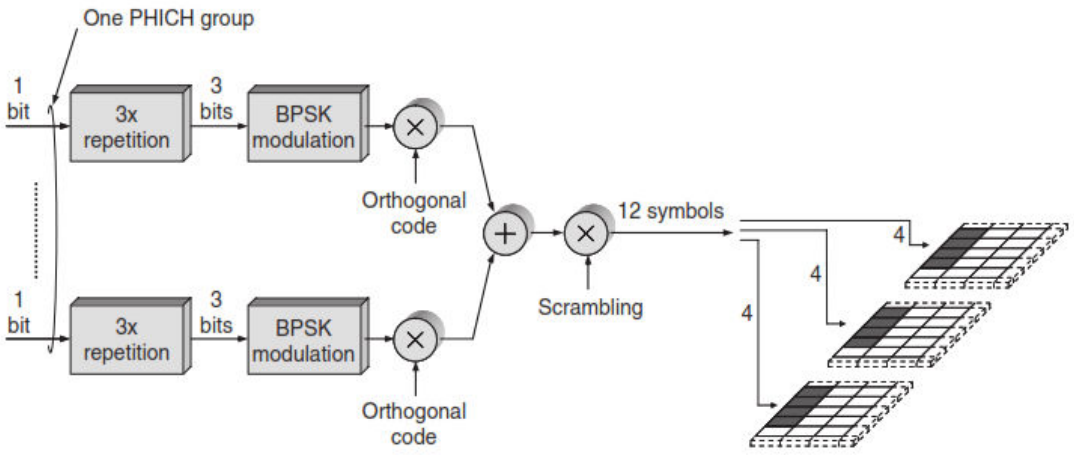

Figure 38. Overview of PHICH structure. From [29].

The PDCCH is used to convey the DCI, including the downlink scheduling assignments, uplink scheduling grants and power-control commands. The PDCCH is mapped onto resource elements in one, two or three OFDM symbols in the first slot of a sub-frame and is sent at every sub-frame interval. The message size of DCI depends on the purpose of the control message. The DCI is defined into different DCI formats based on sizes and usages and is summarized in Table 9.

Table 9. DCI format with corresponding usage. From [29].

	Usage		
Relative DCI size	Uplink grant	Downlink assignment	Power control
Small	–	1C Small contiguous allocations	–
	0	1A Contiguous allocations only	3, 3A
…	–	1B Contiguous allocations with spatial multiplexing	–
	–	1 Flexible allocations, no spatial multiplexing	–
Large	–	2 Flexible allocations, full spatial multiplexing	–

A PDCCH is transmitted on one or a group of several consecutive control channel element (CCE), where a CCE is made up of nine REGs. The number of CCEs transmitted (one, two, four, or eight) depends on the payload size of the DCI and the channel-coding rate [29]. In PDCCH transmission, only those REGs which are not assigned to PCFICH or PHICH are used, and multiple PDCCHs can be transmitted in a sub-frame.

The processing of the downlink signal is shown in Figure 39. First, the DCI message and the RNTI are masked as a CRC attachment, which is then convolutionally coded with a rate of 1/3 before producing the PDCCH bits. The PDCCHs bits to be transmitted in a given sub-frame are then aggregated and scrambled by cell and sub-frame specific scrambling sequence, followed by QPSK modulation, interleaved and cyclically shifted prior to PDCCH resource mapping.

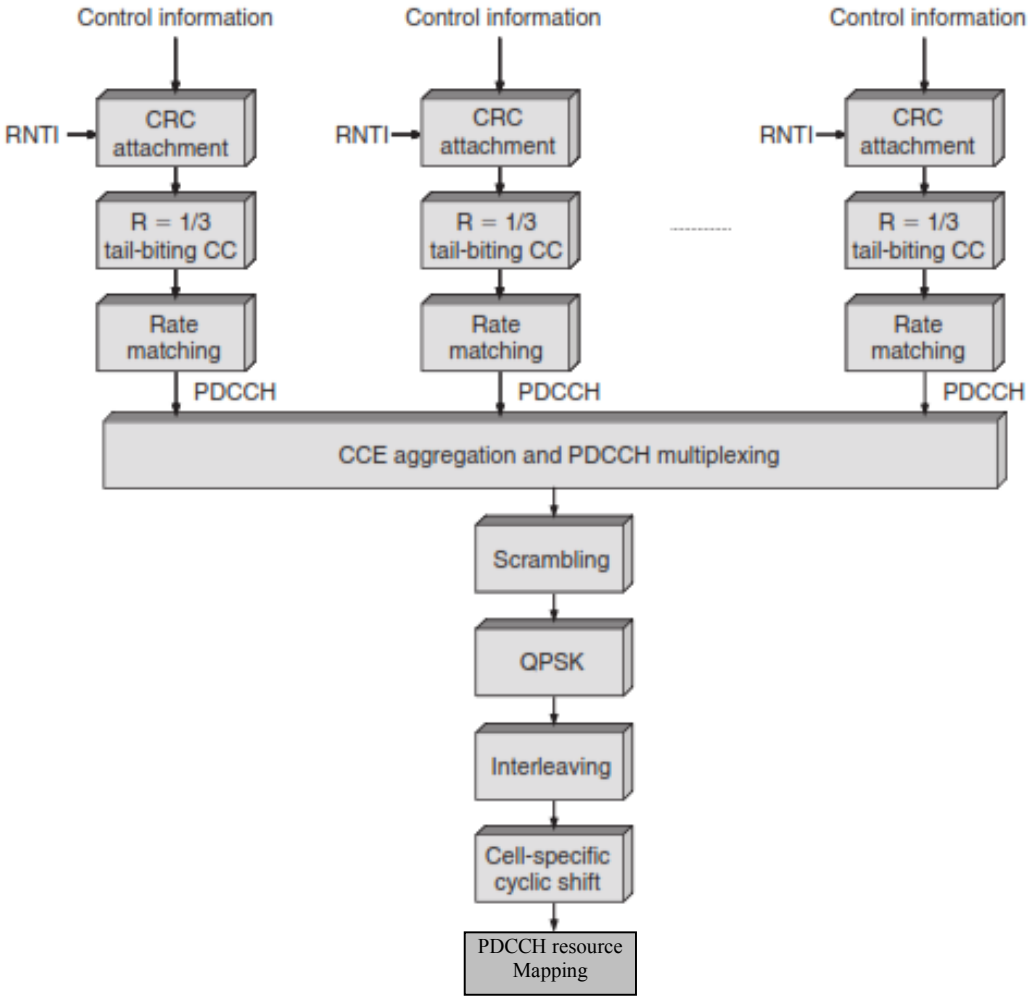

Figure 39. Downlink signal processing of the eNodeB. After [29].

2. Decoding and Search Space

Each PDCCH supports multiple formats, and the format used is unknown to the UE. The UE is informed of the number of OFDM symbols within the control region of a sub-frame but not explicitly informed of the detailed control channel structure. The control region of the sub-frame comprises of PDCCHs for multiple UEs. The UE has to monitor this particular area and blindly attempt to decode the control region in every sub-frame in order extract its own control information. The concept of UE Search Spaces introduced in LTE enhances the UEs' ability to decode the control channel region

efficiently. Instead of decoding the entire control channel region, a UE will only try to decode CCEs within a pre-computed range known as the UE's own Search Space.

An illustration on the mapping of the search space to the respective UEs in the control region is shown in Figure 40. In this illustration, the size of the control region has a length of three OFDM symbols. The specific starting location where the UE begins to decode the CCEs corresponding to the PDCCHs is described in [36] and is calculated as

$$Z_k = Y_k \bmod \lfloor N_{CCE,k} / L_{PDCCH} \rfloor \tag{2}$$

where Z_k is the PDCCH search space staring location in sub-frame number k for CCE aggregation level L_{PDCCH}; N_{CCE} is the number of CCEs in sub-frame number k; L_{PDCCH} is the CCE aggregation level, and sub-frame number k is an integer from 0 to 9.

The parameter Y_k in Equation (2) is determined by

$$Y_k = AY_{k-1} \bmod D \tag{3}$$

where Y_{k-1} is defined as

$$Y_{k-1} = 16(UE\_ID) + \text{sub-frame number } k \tag{4}$$

and A is 39822 while D is 65537.

This particular search space is determined by the sub-frame number and the UE's CRNTI [37]. The UE finds its PDCCH by monitoring a set of PDCCH candidates in every sub-frame to extract downlink control information. Within the search space, the UE

de-masks each control candidate's CRC using its RNTI. If no CRC error is detected, the UE considers it as a successful decoding attempt and reads the control information within the successful candidate.

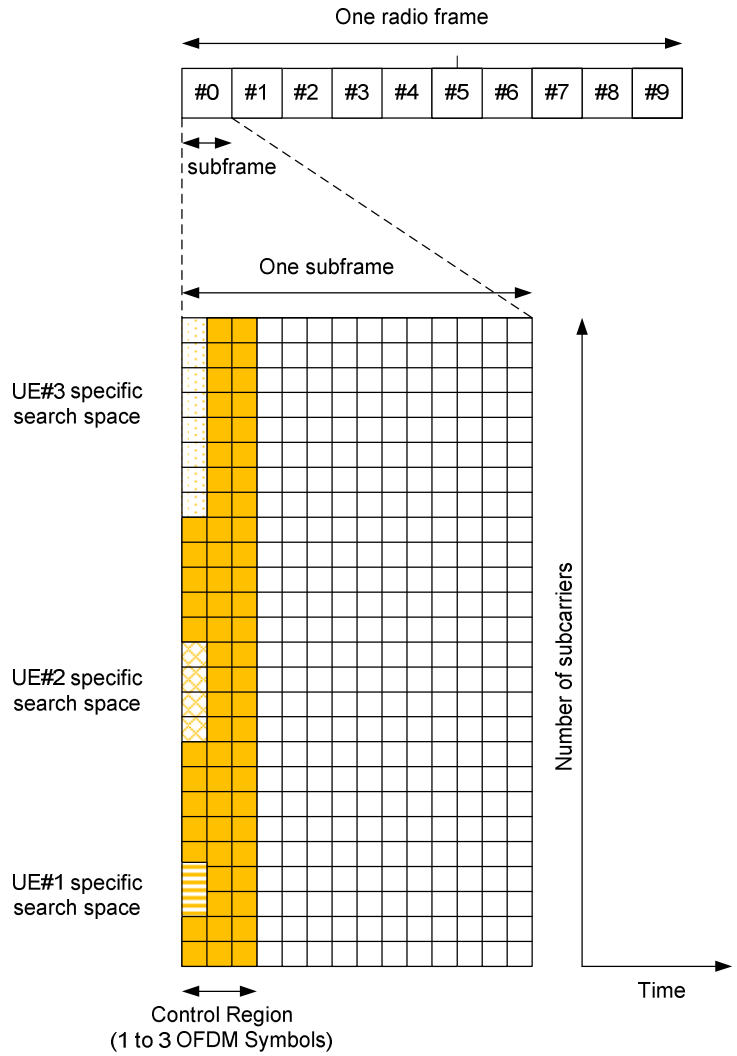

Figure 40. Search space of UEs in the control region.

E. APPROACH

The attacker acts as a combination of eNodeB and the UE. Initially, the attacker impersonates a UE and connects to the genuine eNodeB to obtain the cell–specific reference signal. At a later stage the attacker presents itself as bogus eNodeB and generates false messages to the victim UE. The attacker can perform a message injection attack on the victim UE, and this is to be performed in three stages. Stage 1 involves the extraction of the messages between the victim UE and the eNodeB to obtain Cell Radio Network Temporary Identifier (CRNTI). Stage 2 involves the calculation of the timing

advance in order to synchronize the false message frame to the victim UE. Stage 3 involves the injection of false messages with the TPC field sub field adjusted to the designated value to change the behavior of the victim UE.

1. Stage 1– Acquisition of Cell Radio Network Temporary Identifier (CRNTI)

CRNTI provides unique end UE identification (UEID) at the cell level, and it is assigned to the associated UE by the network during the initial establishment of uplink synchronization. To achieve fast and flexible scheduling capability, the CRNTI is transmitted with its scheduling information in the Layer 1 downlink control signal in plain text [17]. Thus, the identity, CRNTI and its related resource allocation and other Layer 1 control information are transmitted in the clear and are readable by anyone. The vulnerabilities of the initial establishment of uplink synchronization provide the opportunity for a man-in-the-middle attack machine to impersonate the legitimate UE and the eNodeB. The adversary can exploit the fact that CRNTI is transmitted in the clear and misuse it for malicious purposes.

As mentioned in the previous section, the eNodeB can perform CRC calculation masked with the UE's CRNTI on the control information, and the UE can de-mask the control information using its own CRNTI within the search space. Thus, with the captured CRNTI, the adversary can impersonate the eNodeB and inject false control messages with adjusted control information field at predetermined timing and change the intended behavior of the UE.

2. Stage 2- Synchronization of Frame

Since OFDM systems are sensitive to time and frequency synchronization error and in order to have the false message arrive at the UE simultaneously with the legitimate message generated by the eNodeB, there is a need to acquire some form of synchronization with the cell.

The adversary needs to perform cell search (similar to normal UE) to acquire frequency and symbol synchronization to a cell, acquire frame timing of the cell that determines the start of the downlink frame [29], and identify the cell–specific reference

signal. Based on the distance between the eNodeB and adversary UE and the distance between the eNodeB and the victim UE, the adversary is able to calculate the time difference of the two UEs upon reception of the same frame from the eNodeB. With the calculated time difference, the adversary can determine the position of time slot relative to the adversary's UE when the first OFDM symbol (control region) of the frame reaches the victim UE. With another round of calculation, the adversary can pre-determine the timing advance required for the false message to be transmitted from the adversary's UE position. This enables the synchronized false message to arrive at the victim UE simultaneously with the legitimate message.

3. Stage 3- Message Injection

The adversary is able to determine the victim UE's search space using the pre-captured CRNTI and construct message to the particular UE's search space and, thereafter, inject the message according to the pre-determined timing. The injected false message arriving at the victim UE will be of higher power than the message transmitted from the legitimate eNodeB; thus, the legitimate message will be overwritten. Upon receiving the message, the victim UE decodes the content of the control channel region according to the search space and processes the information such as the scheduling assignment and the scheduling grants.

a. Power Requirement for Message Injection

A typical set-up of a MITM attack is shown in Figure 41. In this set-up, the position of the victim UE, the attacker and the eNodeB form an extended line. The distance between the eNodeB and the victim UE and the transmitted power of the eNodeB are denoted as d_1 and $P_{T,1}$, respectively. The distance between the malicious attacker and the victim UE and the transmitter power of the malicious attacker are denoted as d_2 and $P_{T,2}$, respectively. The received power at victim UE from eNodeB and attacker are denoted as $P_{R,1}$ and $P_{R,2}$, respectively.

The received false-signal-to-legitimate-signal ratio SIR_{Pr2}/SIR_{Pr1} at the victim UE is derived in the following steps. The parameter SIR_{Pr1} is calculated as

$$SIR_{\mathrm{Pr1}} = \left(\frac{P_{R,1}}{I} \right) \tag{5}$$

where I is the total co-channel interference received, and $P_{R,1}$ is determined by

$$P_{R,1} = G_{T,1} G_R L^{-1} P_{T,1} \tag{6}$$

where $G_{T,1}$ is the gain of the transmitter at eNodeB; G_R is the gain of the receiver at the victim UE; and L is the propagation loss. Substituting (6) into (5), we get

$$SIR_{\mathrm{Pr1}} = \left(\frac{G_{T,1} G_R L^{-1} P_{T,1}}{I} \right). \tag{7}$$

The power law equation is determined as

$$L = \beta d_1^{\,n} \tag{8}$$

where β is a proportionality constant that is a function of the antenna heights of both transmitter and receiver and the carrier frequency, and n is the path loss component factor. Substituting (8) into (7), we get

$$SIR_{\mathrm{Pr1}} = \left(\frac{G_{T,1} G_R \beta^{-1} d_1^{\,-n} P_{T,1}}{I} \right). \tag{9}$$

Similarly, for the attacker, the SIR_{Pr2} is calculated as

$$SIR_{\mathrm{Pr2}} = \left(\frac{G_{T,2} G_R \beta^{-1} d_2^{\,-n} P_{T,2}}{I} \right) \tag{10}$$

where $G_{T,2}$ is the gain of the transmitter at attacker.

Assuming $G_{T,1} = G_{T,2}$ and dividing (10) by (9), we get the received false-signal-to-legitimate-signal ratio as

$$\frac{SIR_{\mathrm{Pr2}}}{SIR_{\mathrm{Pr1}}} = \left(\frac{d_2^{\,-n} P_{T,2}}{d_1^{\,-n} P_{T,1}} \right). \tag{11}$$

The power required for the malicious attacker to inject the false message is dependent on the received SIR of the victim UE. This received SIR is in turn dependent on both transmitters' power, the distance between the transmitter and the receiver, and

the path loss component n as illustrated in (11). The set-up is assumed to be in lossy environment where n is four. In order to effectively overwrite the legitimate message from the eNodeB, the power of the injected false message must be significantly higher than that of the former.

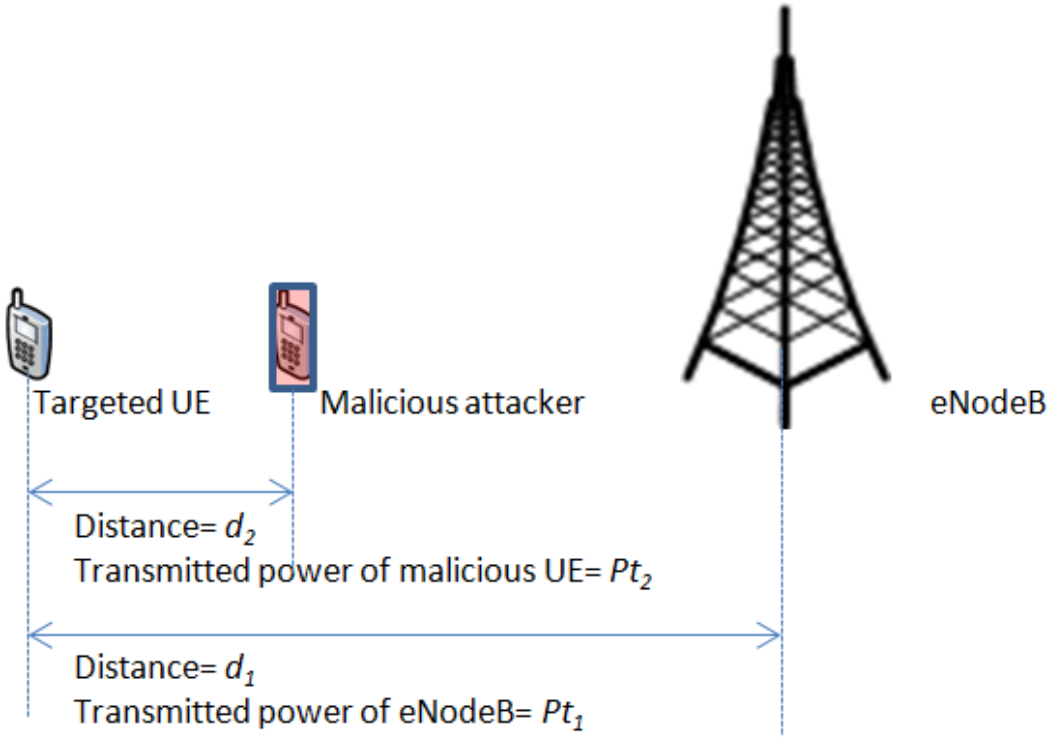

Figure 41. Set-up position for MITM attack.

A graph for the required power of the injected message can be derived based the distance ratio d_2/d_1 and the desired received false-signal-to-legitimate-signal ratio $P_{R,2}/P_{R,1}$ at the victim UE as shown in Figure 42. The relationship between the proximity of the attacker to the victim UE and the required attacker's transmitted power is shown in Figure 42.

An example is used to illustrate the required transmitted power of the attacker based on the various false-signal-to-legitimate-signal ratios. In this example, the

victim UE is located 2 km from the eNodeB, while the attacker is 200 m from the UE. This yields a distance ratio of 0.1. The eNodeB is transmitting at 30 W. From Figure 42, we see that the required transmitted power of the attacker is only 0.02 times the amount of the transmitted power of the eNodeB when the desired received SIR ratio at the victim UE is 3 dB. This equates to only 0.6 W of power required for the attacker's transmitter. The required transmitted power of the attacker for the various remaining false-signal-to-legitimate-signal ratios is tabulated in Table 10. In general, the closer the attacker is to the victim UE, the lower the power required to conduct the attack.

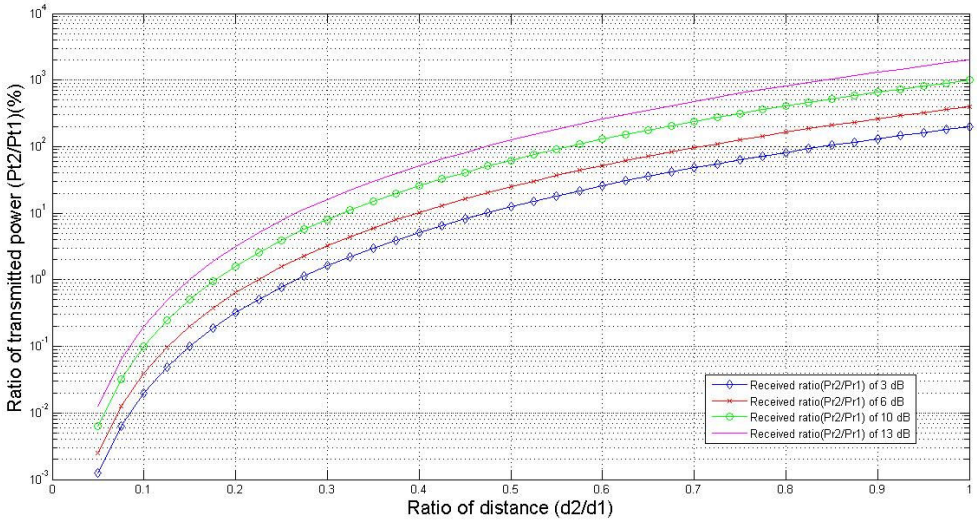

Figure 42. Relation between the proximity of the attacker to the victim UE and the required attacker's transmitted power (n=4).

Table 10. Required transmitted power of attacker for various false-signal-to-legitimate-signal ratio.

False-signal-to-legitimate-signal ratio (dB)	**Transmitted power of attacker to eNodeB ratio (times)**	**Transmitted power of attacker (Watt)**
3	0.02	0.6
6	0.04	1.2
10	0.1	3
13	0.2	6

F. IMPACT

The adversary's action has two results. First, it depletes the limited battery power of the UE at a faster rate and reduces the intended operation period. Second, it causes interference to the neighboring cells. A combination of this interference from the neighboring cells increases the interference perceived by the eNodeB and reduces the desired SIR of the eNodeB. The decoding capability at the eNodeB is determined by the SIR instead of the absolute received power. Thus, the increase of inferences of neighboring UEs to the eNodeB reduces the SIR and changes the modulation and coding scheme (MCS) to one, which lowers the maximum throughput. This in turn, restricts the legitimate UEs to accessing their desired network services at a much lower data rate.

1. Depletion of Battery Power

The battery lifespan of an end device is dependent on many parameters including the device operation system, use applications, and user profiles. These applications in turn determine the required bandwidth and the required transmit and receive power of the end device. An approximate approach is used to explore the depletion rate of the battery power of a device transmitting at 23 dBm, which is the maximum UE power specified in [24]. Typically, a bandwidth demanding application like streaming video will require higher transmit power for data transmission. As such, in this study, we assume the estimated battery life of a phone continuously streaming video or browsing the web to represent the battery life of the phone transmitting at 23 dBm. Also, we assume that the estimated battery life of the phone performing an idle push email function to represent the battery life of the transmitting at average power value. The estimated battery life of four types of LTE phones by applications is plotted in Figure 43. For purposes of comparison, we use the data of the Skyrocket phone to illustrate the UE depletion rate of battery power for the various applications. From Figure 43, it is shown that Skyrocket will have 210 minutes of battery lifetime for streaming of video and will have 640 minutes of battery lifetime for idle-push email. Analogously, a phone transmitting a maximum power of 23 dBm has only 210 minutes of battery lifetime, which is a reduction of 430

minutes from a phone transmitting at nominal power. The phone battery lifetime is reduced to 33% of the original battery lifetime when transmitting at maximum power.

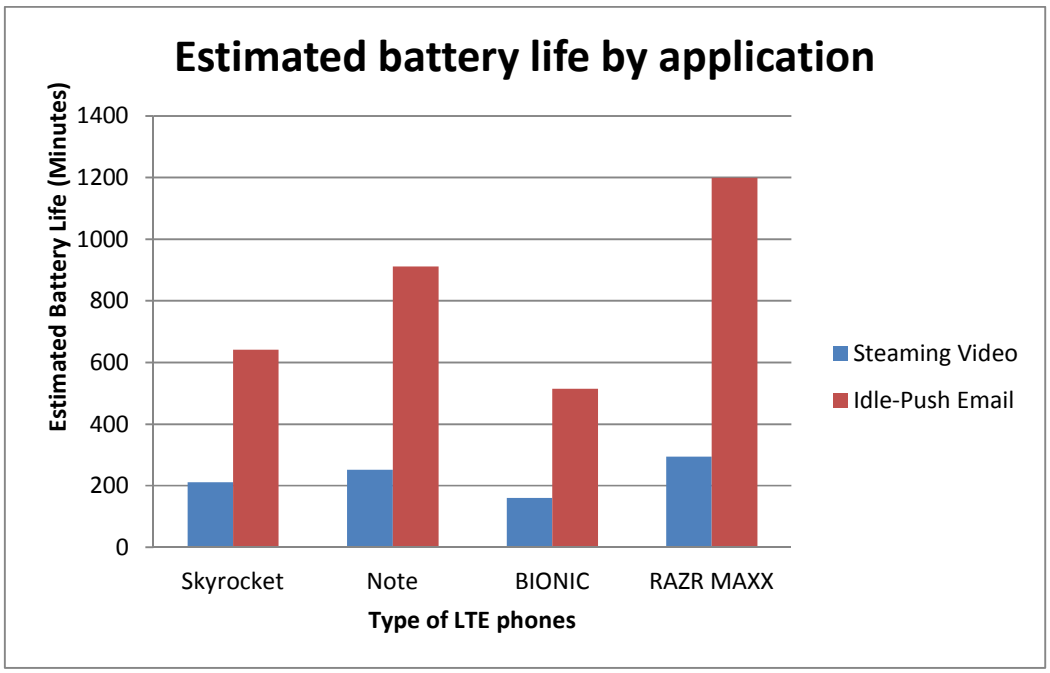

Figure 43. Battery lifespan of four LTE phones by applications. From [38].

2. Reduction of Reverse Channel SIR

The inter-cell interference condition is illustrated in Figure 44. The solid green line indicates the desired transmit signal from the legitimate UE (UE4) located at the corner of the outer cell of cell O to the eNodeB. Since the neighboring cell edge users adopt sectoring, only cells D, E and F in the first tier which are facing the intended sector (Channel 2) contribute to the co-channel interference (CCI). However, as none of these three cells are using Channel 2, the interference comes from the second tier. In the second tier, the only cells using Channel 2 and facing the intended sector are bottom cell A and two cells B. The locations of UEs are designated as UE1, UE2 and UE3, respectively, as shown in Figure 44. The solid red lines indicate the interference generated to the eNodeB by UEs (UE1, UE2 and UE3) of adjacent cells.

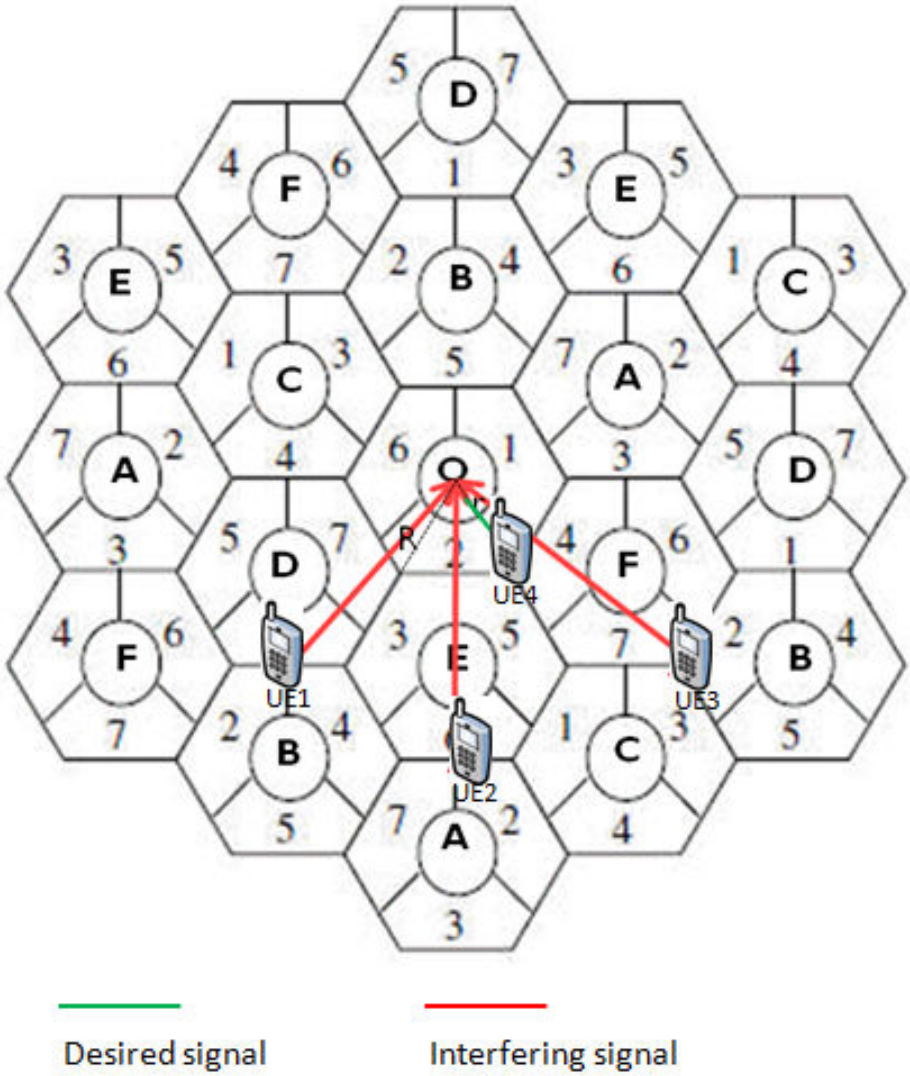

Figure 44. Reverse channel interference analysis for edge area. After [37].

The total co-channel interference I received by the eNodeB in cell O is given in [41] and restated as follows

$$I = \left(\frac{G_T G_R P_{T,B}}{L_B}\right) + \left(\frac{G_T G_R P_{T,A}}{L_A}\right) + \left(\frac{G_T G_R P_{T,B'}}{L_{B'}}\right) \tag{12}$$

where G_T is the gain of transmitter at the neighboring UE; $P_{T,A}$, $P_{T,B}$ and $P_{T,B'}$ are the transmitted power from UE2, UE1, and UE3, respectively; and L_A, L_B and $L_{B'}$ are the propagation loss of transmitted power from UE2, UE1, and UE3, respectively. By rearranging (12), we get

$$I = \left(G_T G_R\right)\left(L_B^{-1} P_{T,B} + L_A^{-1} P_{T,A} + L_{B'}^{-1} P_{T,B'}\right). \quad (13)$$

The reverse channel SIR of the cell edge area (CE) for 120º-sectoring [41] $SIR_{CE,120^\circ}$ is defined as

$$SIR_{CE,120^\circ} = \left(\frac{P_{R,O}}{I}\right) \quad (14)$$

where $P_{R,O}$ is the received power from UE4 (legitimate user) and is calculated as

$$P_{R,O} = G_T G_R L_O^{-1} P_{T,O} \quad (15)$$

where L_O is the propagation path loss between UE4 and eNodeB, and $P_{T,O}$ is the transmitted power of UE4. Substituting (13) and (14) into (15), we obtain

$$SIR_{CE,120^\circ} = \left(\frac{G_T G_R L_O^{-1} P_{T,O}}{\left(G_T G_R\right)\left(L_B^{-1} P_{T,B} + L_A^{-1} P_{T,A} + L_{B'}^{-1} P_{T,B'}\right)}\right) \quad (16)$$

where L_B, L_A, $L_{B'}$ and Lo are the path losses for UE1, UE2, UE3 and UE4, respectively. The L_B value is calculated as

$$L_B = \beta_B^{-1}\left(\frac{\sqrt{21}}{2}R\right)^{-n}. \quad (17)$$

where β_B is a proportionality constant that is a function of the antenna heights of UE1, and eNodeB, and R is the radius of the cell. The L_A value is calculated as

$$L_A = \beta_A^{-1}\left(\frac{3\sqrt{3}}{2}R\right)^{-n} \quad (18)$$

where β_A is a proportionality constant that is a function of the antenna heights of UE2 and eNodeB. The $L_{B'}$ value is calculated as

$$L_{B'} = \beta_{B'}^{-1}\left(\sqrt{7}R\right)^{-n} \quad (19)$$

where $\beta_{B'}$ is a proportionality constant that is a function of the antenna heights of UE3 and eNodeB. The L_O value is calculated as

$$L_O = \beta_O^{-1} R^{-n} \quad (20)$$

where βo is a proportionality constant that is a function of the antenna heights of UE4 and eNodeB.

Substituting (17) to (20) into (16), we determine $SIR_{CE,120^o}$ as

$$SIR_{CE,120^\circ} = \left(\frac{\left(\beta_O^{-1} R^{-n}\right) P_{T,O}}{\left(\left(\beta_B^{-1} \left(\frac{\sqrt{21}}{2} R\right)^{-n}\right) P_{T,B} + \left(\beta_A^{-1} \left(\frac{3\sqrt{3}}{2} R\right)^{-n}\right) P_{T,A} + \left(\beta_{B'}^{-1} \left(\sqrt{7} R\right)^{-n}\right) P_{T,B'} \right)} \right). \quad (21)$$

Assuming that $\beta_O=\beta_A=\beta_B=\beta_{B'}$ for the coverage area, we get the reverse channel SIR of the CE as

$$SIR_{CE,120^\circ} = \left(\frac{P_{T,O}}{\left(\left(\frac{\sqrt{21}}{2}\right)^{-n} P_{T,B} + \left(\frac{3\sqrt{3}}{2}\right)^{-n} P_{T,A} + \left(\sqrt{7}\right)^{-n} P_{T,B'} \right)} \right). \quad (22)$$

From (22), we observe that the SIR is dependent on the power transmitted by the UEs and is independent of the cell radius. The average SIR can be computed to indicate the average SIR experienced by the eNodeB and is given by

$$SIR_{Average} = \sum_{i=1}^{M} p_i SIR_i \quad (23)$$

where SIR_i represents the SIR experienced by the eNodeB computed by the respective transmitted power combination of UE1, UE2, UE3 and UE4 as shown in Table 11. The parameter p_i represents the probability of that SIR value occurring, computed within the specified transmitted power range, and M represents the number of transmitted power combinations of UE1, UE2, UE3 and UE4.

Two types of average SIR, namely $SIR_{Ave,normal}$ and $SIR_{Ave,maximum}$ experienced by the eNodeB are computed. The $SIR_{Ave,\ normal}$ is the average SIR experienced by the eNodeB based on the normal scenario where all the interfering power is random. On the other hand, $SIR_{Ave,\ maximum}$ is the average SIR experienced by the eNodeB based on the extreme scenario where all the interfering power is at a maximum.

To formulate the value of the average $SIR_{Ave,\ normal}$ experienced by eNodeB, it is assumed that sampling is performed on the transmitted power of UE1, UE2, UE3 and UE4. The transmitted powers can assume one of the twenty values, which range from 10 mW to 200 mW with steps of 10 mW. The $SIR_{Ave,\ normal}$ is computed based on (22) and (23), with various input combinations for the different transmitted power of UE1, UE2, UE3 and UE4. There is a total of 20^4 =160,000 combinations of SIR with run-number 1 computed based on transmitted power of UE1, UE2, UE3 and UE4 being 10 mW and run number 160,000 based on transmitted power of UE1, UE2, UE3 and UE4 being 200 mW as shown in Table 11. A relatively lossy environment with n 4 is assumed in the computation, and p_i is 1/(number of combinations) where each combination of transmitted power is equally likely to occur.

The results of the $SIR_{Ave,normal}$ for the various combinations of the transmitted power are simulated using Matlab code and are shown in Figure 45. The enlarged figure for the first 100 combinations is shown in Figure 46.

Region 1 can be observed in Figure 45, while region 2 is illustrated in Figure 46, which shows the first 100 data points of Figure 45. In region 1 of Figure 45, formed by the first 8,000 combination runs, the SIR increases significantly to 10 dB at combination run-number 21 as compared to the previous run. This occurs when the transmitted power of UE3 is reset to 10 mW, while the transmitted power of UE2 is set to 20 mW. There is an overall decrease in the interfering power from combination run-number 20 to 21. The SIR generally follows a downward trend for this region until the transmitted power of UE4 is set to 20 mW. At combination run-number 8,001, the SIR increases significantly as the desired transmitted power of UE4 is set 20 mW as compared to the previous 10,000 combinations where the transmitted power of UE4 is at 10 mW. This pattern can be observed for the subsequent 15,000 combination runs. Overall, the SIR increases as the desired transmitted power of UE4 increases.

We observe that in region 2 of Figure 46, formed by the first 20 combination runs, the SIR decreases as the interfering power of UE3 increases from 10 mW to 200 mW for corresponding runs while the transmitted power of UE1, UE2, and UE4 remain at 10 mW. The SIR is inversely proportional to the interfering power.

Table 11. Various input combinations of UEs' transmitted power to compute $SIR_{Ave,normal}$.

	Transmitted power (mW)			
Run Combination Number	**UE4 (Desired)**	**UE1 (Interfering)**	**UE2 (Interfering)**	**UE3 (Interfering)**
1	10	10	10	10
2	10	10	10	20
3	10	10	10	30
4	10	10	10	40
5	10	10	10	50
…	…	…	…	…
80001	20	10	10	10
…	…	…	…	…
159996	200	200	200	160
159997	200	200	200	170
159998	200	200	200	180
159999	200	200	200	190
160000	200	200	200	200

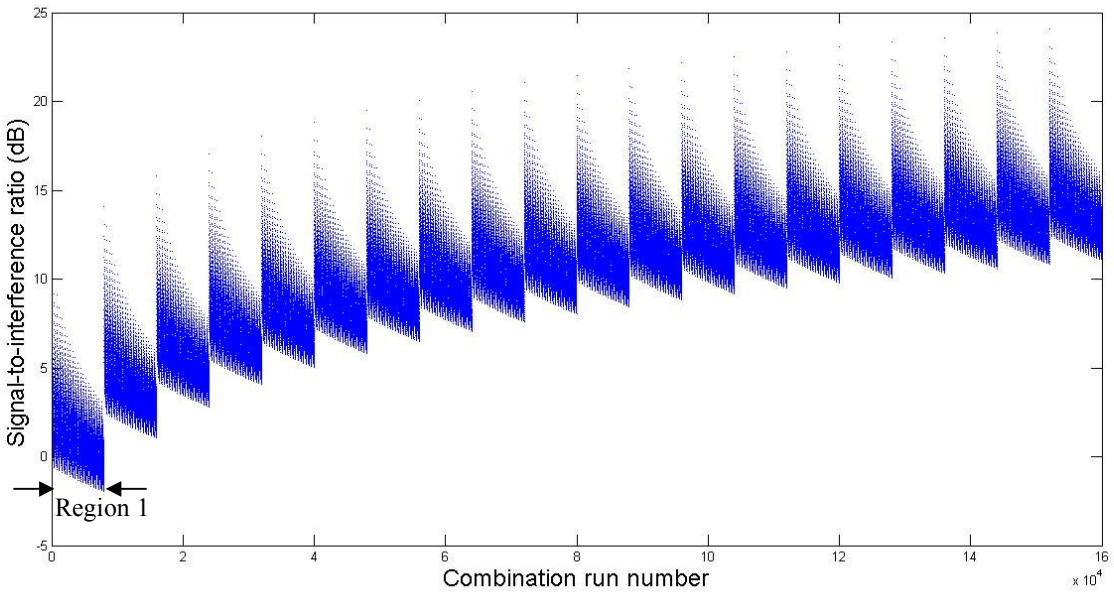

Figure 45. Signal-to-interference ratio for various combinations of UEs' transmitted power (UE1, UE2, UE3 and UE4 range from 10 mW to 200 mW).

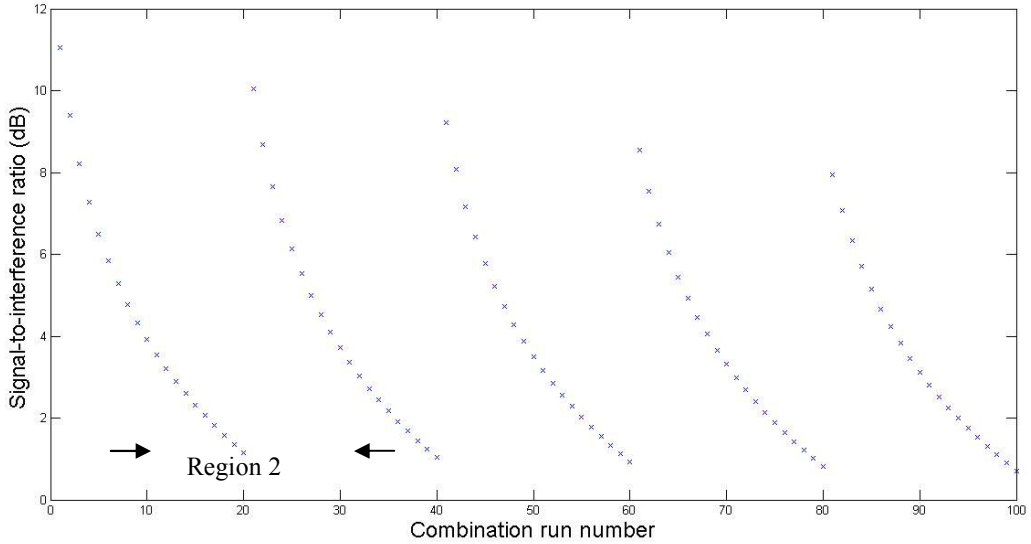

Figure 46. Signal-to-interference ratio for first 100 combination of UEs' transmitted power to compute $SIR_{Ave,normal}$.

A Matlab simulation code is used to calculate the average $SIR_{Ave,normal}$ experienced by eNodeB according to (23) and the computed value is 11.7 dB.

When UE1, UE2 and UE3 are transmitting at maximum power of 200 mW each, several assumptions were adopted to formulate the value of $SIR_{Ave,\ maximum}$ experienced by the eNodeB. First, it is assumed that the interfering transmitted power of UE1, UE2 and UE3 was fixed at 200 mW. Second, the transmitted power of UE4 can assume one of the 20 values, which ranges from 10 mW to 200 mW with steps of 10 mW. The $SIR_{Ave,\ maximum}$ is computed based on the various combinations of different transmitted powers of UE1, UE2, UE3 and UE4. There are a total of 20 combinations of SIR with run-number 1 computed based on transmitted powers of UE1, UE2 and UE3 being 200 mW and UE4 being 10 mW, while run-number 20 is based on transmitted powers of UE1, UE2, UE3 and UE4 being 200 mW as shown in Table 12. Third, a relatively lossy environment with n 4 is assumed, and the parameter p_i is 1/ (number of combinations), where each combination of transmitted power is equally likely to occur. With these assumptions, the value of the average $SIR_{Ave,\ maximum}$ experienced by eNodeB was formulated.

Table 12. Various input combinations of UEs' transmitted power to compute $SIR_{Ave,maximum}$.

	Transmitted power (mW)			
Combination Number	UE4 (Desired)	UE1 (Interfering)	UE2 (Interfering)	UE3 (Interfering)
1	10	200	200	200
2	20	200	200	200
3	30	200	200	200
4	40	200	200	200
5	50	200	200	200
…	…	…	…	…
16	160	200	200	200
17	170	200	200	200
18	180	200	200	200
19	190	200	200	200
20	200	200	200	200

The results of the $SIR_{Ave,\ maximum}$ are simulated using Matlab code, and they are shown in Figure 47. In Figure 47, we observe that when the transmitted power of UE4 is 10 mW, the SIR is -2dB. This is because the overall CCI is higher than the desired received signal of UE4, which resulted in the negative SIR. Overall, the SIR increases as the desired transmitted power of UE4 increases. A Matlab simulation code is used to calculate the $SIR_{Ave,\ maximum}$ experienced by eNodeB, and the computed average value is 8.3dB.

The results show that there is a reduction in SIR of eNodeB by 3.4 dB, which is calculated as 11.7 dB - 8.3 dB, when the interfering transmitted power of UEs (UE1, UE2 and UE3) are fixed at maximum of 200 mW as compared to when the interfering transmitted power of UEs varied from 10 mW to 200 mW. This lowers the MCS that can be adapted by the victim UE with the eNodeB and reduces the data throughput significantly.

The maximum throughput that can be achieved by a given MCS is the product of the coding rate and the number of bits per modulation symbol [39]. Coding refers to addition of redundant bits to the data bits and provides forward error correction on the

received bits, while coding rate is the proportion of the code bits to the data bits. The order of modulation refers to the number of coded bits which can be transmitted per modulation symbol.

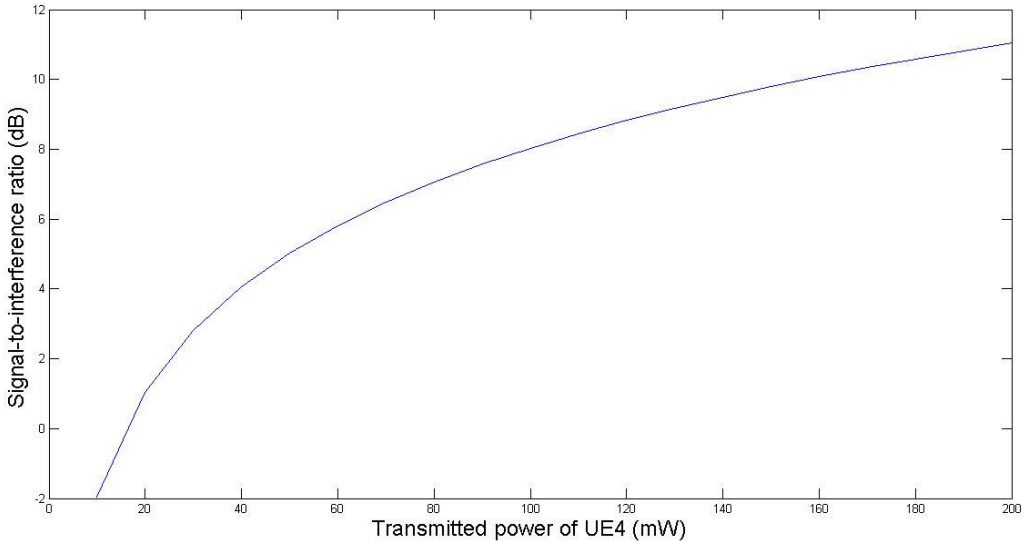

Figure 47. Signal-to-interference ratio for various combinations of UEs' transmitted power (UE1, UE2 and UE3 are fixed at 200 mW).

A graph of throughput for various MCS as a function of SINR is displayed in Figure 48 [38]. Since mobile network is interference-limited where SNR has negligible effect, SINR can be approximated to SIR [42]. Thus, Figure 48 is plotted against SINR and can be used directly for our evaluation. A particular MCS requires a certain SIR in order to operate with a suitably low bit error rate at the output. In general, a MCS with a higher throughput requires a higher SIR. From Figure 48, we observe that to maximize the throughput at around 11.7 dB, MCS-10 (16 QAM, R=4/5) corresponding to throughput of 3.2 bits per second per hertz is the suitable MCS. When the SIR is reduced to 8.3 dB, the MCS is MCS-8 (16 QAM, R=1/2), which corresponds to only 2.0 bits second per hertz. Thus, the reduction in SIR of eNodeB from 11.7 dB to 8.3 dB will decrease the maximum throughput of the UE by 37.5% from 3.2 bits per second per hertz to 2.0 bits per second per hertz.

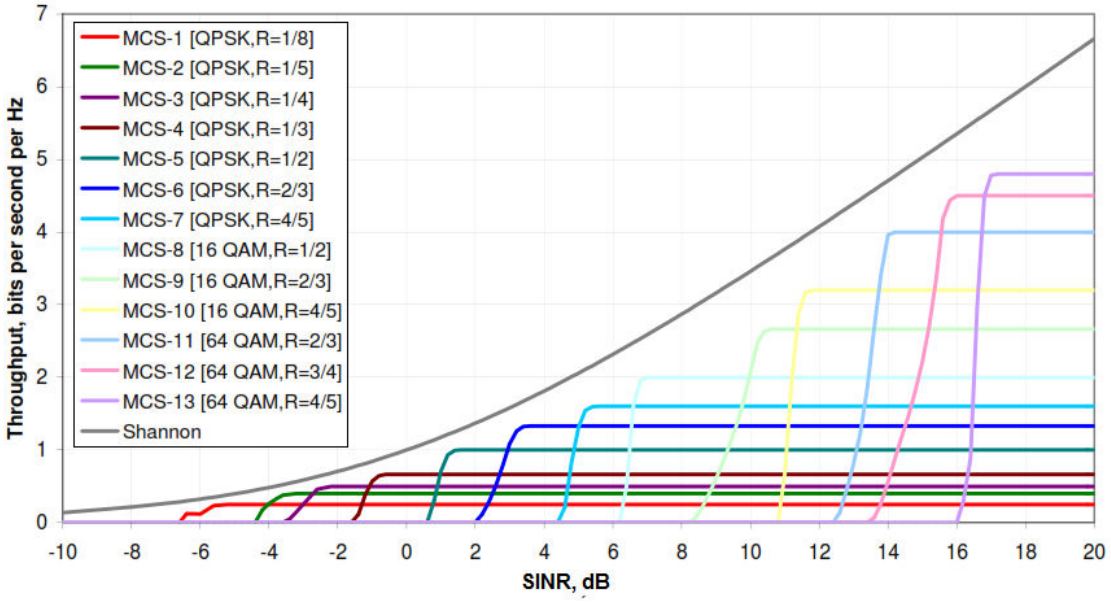

Figure 48. Throughput of a set of coding and modulation combination. From [39].

V. CONCLUSIONS AND FUTURE WORK

A. CONCLUSIONS

This study consists of a comprehensive investigation of the LTE specifications pertaining to Layer 2 protocols. As discussed in the literature review, the previous studies on the security exploitation of Layer 2 protocols are not exhaustive. These studies are limited to listing security vulnerabilities and do not elaborate further on the details and the impact of respective threats.

This research has identified other potential vulnerabilities in the Layer 2 protocol and demonstrated the potential of exploiting the unprotected power control message and extracted CRNTI to change the intended behavior of the UEs. In particular, the victim UE is tricked by a false message generated by a bogus eNodeB to transmit at a much higher than required power, which introduced significant inter cell interference to the adjacent eNodeB.

The impacts of the attack include depleting the limited battery power of the victim UE at a much faster rate and reducing the reserve channel SIR of the eNodeB. The intended phone battery lifetime is reduced to 33% of the original battery lifetime when transmitting at maximum power. The simulation results show that there is a reduction in reverse channel SIR of eNodeB by 3.4 dB, and this decreases the maximum possible throughput of the UE by 37.5% from 3.2 bits per second per hertz to 2.0 bits per second per hertz.

B. FUTURE WORK

1. Verification and Validation of Desired Received SINR

One important practical consideration that influences the amount of interference is the changing environment where the LTE may be deployed, and the environment can affect the path loss. This variation in environment was not simulated in this thesis. In addition, the received SINR determines a range of MCS that can be adopted by the UE, and the throughput varies for a different MCS at the same SINR. In this thesis, the analysis is based only on the maximum possible throughput. The actual throughput loss

experienced by the UE when it operates with a SINR of 11.7 dB instead of 8.3 dB may even be larger. Collection of the actual data can be used to validate and refine the results of this research.

2. Investigation on Other Control Messages

A thorough investigation can be conducted on RRC layer, in particular to the unprotected RRC signaling. Some of these messages can be sent unprotected prior to security activation, and some of the messages can be sent unprotected even after security activation. The details on these messages can be found in 3GPP.36.331.

APPENDIX A- MATLAB SIMULATIONS

A. CALCULATION AND PLOT OF FALSE SIGNAL TO LEGITIMATE SIGNAL RATIO

```
clear all;
close all;

n = 4;      %Path loss exponent
P=0.01:0.01:0.2;   %From LTE (Rel-8), the maximum UE transmit power is
23dBm, that is, 200mW.

i=1;
improvement_3dB = 2;
improvement_6dB = 4;
improvement_10dB = 10;
improvement_13dB = 20;

for dist_ratio=0.05:0.025:1
                power_ratio =  dist_ratio ^ -n / improvement_3dB;
                Display_3dB(i)= 1/power_ratio *100;
                i=i+1;

end
i=1;
for dist_ratio=0.05:0.025:1
                power_ratio = dist_ratio ^ -n / improvement_6dB;
                Display_6dB(i)= 1/power_ratio *100;
                i=i+1;

end
i=1;
for dist_ratio=0.05:0.025:1
                power_ratio = dist_ratio ^ -n / improvement_10dB;
                Display_10dB(i)= 1/power_ratio *100;
                i=i+1;

end
i=1;
for dist_ratio=0.05:0.025:1
                power_ratio = dist_ratio ^ -n / improvement_13dB;
                Display_13dB(i)= 1/power_ratio *100;
                i=i+1;

end
figure;
semilogy(0.05:0.025:1, Display_3dB, '-db');
hold on;
semilogy(0.05:0.025:1, Display_6dB , '-xr')
hold on;
semilogy(0.05:0.025:1, Display_10dB , '-og')
hold on;
```

```
semilogy(0.05:0.025:1, Display_13dB , 'magenta-')
grid on;
legend( 'Received ratio(Pr2/Pr1) of 3dB','Received ratio(Pr2/Pr1) of
6dB','Received ratio(Pr2/Pr1) of 10dB','Received ratio(Pr2/Pr1) of
13dB');

xlabel('Ratio of distance (D2/D1)')
ylabel('Ratio of transmitted power (Pt2/Pt1)(%)')
title('Plot of relationship between ratio of distance vs ratio of
transmitted power for various received power ratio')
```

B. CALCULATION AND PLOT OF $SIR_{AVE, NORMAL}$

```
clear all;
close all;

n = 4;      %Path loss exponent
P=0.01:0.01:0.2;   %From LTE (Rel-8), the maximum UE transmit power is
23dBm, that is, 200mW.
i=1;


    for Pto=0.01:0.01:0.2
        for Pta=0.01:0.01:0.2
            for Ptb=0.01:0.01:0.2
                for Ptbl=0.01:0.01:0.2
                SIR_ceu1_rev = (Pto/(((((sqrt(21))/2)^-n)*Ptbl) +
((((3/2)*(sqrt(3)))^-n)*Pta) + (((sqrt(7))^-n)*Ptb)));
                Display(i)= 10*log10(SIR_ceu1_rev);
                i=i+1;
                end
            end
        end
    end



figure, plot(Display, 'blueo', 'Markersize', 1);
xlabel('Combination run number')
ylabel('Signal-to-interference ratio (dB)')
title('Plot of Signal-to-interference ratio for various combinations of
UEs transmitted power')
```

C. CALCULATION AND PLOT OF $SIR_{AVE, MAXIMUM}$

```
clear all;
close all;

n = 4;      %Path loss exponent
P=0.01:0.01:0.2;   %From LTE (Rel-8), the maximum UE transmit power is
23dBm, that is, 200mW.
```

```
%Interfering source at max of 23dBm, ie, 200mW
Pta=0.2;
Ptb=0.2;
Ptbl=0.2;

Z1_rev=0;
i=1;

for Pto=0.01:0.01:0.2
                SIR_ceu1_rev = (Pto/(((((sqrt(21))/2)^-n)*Ptbl) +
((((3/2)*(sqrt(3)))^-n)*Pta) + (((sqrt(7))^-n)*Ptb)));
                Display(i)= 10*log10(SIR_ceu1_rev);
                i=i+1;
end

figure, plot(10:10:200,Display);
xlabel('Transmitted power of UE4 (mW)')
ylabel('Signal-to-interference ratio (dB)')
title('Plot of Signal-to-interference ratio for various transmitted
power of UE4 (Desired)')
```

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Global mobile Suppliers Association (2012, January). *GSM/3G Market/Technology Update* [Online]. Available: http://www.gsacom.com

[2] 4Gamericas. *Long Term Evolution* [Online] Available: http://www.4gamericas.org/index.cfm?fuseaction=page&sectionid=249

[3] Radio Electronics. *3GPP Long Term Evolution* [Online]. Available: http://www.radio electronics.com/info/cellulartelecomms/lte-long-term-evolution/3g-lte-basics.php

[4] Global mobile Suppliers Association (January 2012). *LTE report* [Online]. Available: http://www.gsacom.com/news/gsa_344.php4

[5] Wikipedia (January 2012). *3GPP LTE Evolution Country Map: Adoption of LTE as of January 5, 2012* [Online]. Available: http://en.wikipedia.org/wiki/File:3GPP_Long_Term_Evolution_Country_Map.svg]

[6] 3GPP (2012). *LTE* [Online]. Available: http://www.3gpp.com/LTE

[7] Wikipedia (January 2012). *LTE (Telecommunication)* [Online]. Available: http://en.wikipedia.org/wiki/3GPP_long_term_evolution

[8] S.T. Baker, "Introduction and Background" in LTE – The UMTS Long Term Evolution; From Theory to Practice, Wiley, pp 1-20, 2009.

[9] LTE World. *Evolution of LTE.* [Online] Available: http://lteworld.org/blog/lte-advanced-evolution-lte

[10] Radio Electronics. *3GPP Long Term Evolution* [Online]. Available: http://www.radioelectronics.com/info/cellulartelecomms/lte-long-term-evolution/3g-lte-basics.php

[11] C.B. Sankaran, "Network Access Security in Next-Generation 3GPP Systems: A Tutorial," *IEEE Commun. Mag*., vol. 47, no. 2, Feb. 2009.

[12] D. Forsberg, "LTE Key Management Analysis with Session Keys Context," *ELSEVIER Computer Communication*, vol. 33, no. 16, Oct. 2010.

[13] R.Narmadha, and Dr.S.Malarkkan, "Review of security Analysis in LTE and WIMAX Environment" *IEEE International Conference on Computational Intelligence and Computing Research*, 2010.

[14] G. M. Køien, "Mutual Entity Authentication for LTE," *IEEE IWCMC*, Jul. 2011.

[15] Y. Park, et al., "A Survey of Security Threats on 4G Networks," *IEEE GLOBECOM Workshop on Security and Privacy in 4G Networks*, Nov. 2007.

[16] Beaumont, J.-and Doucet, G, "Threats and Vulnerabilities of Next Generation Satellite Personal Communications Systems: A Defence Perspective," *Globecom Workshops, IEEE,* pp.1-5, 26-30 Nov. 2007.

[17] D. Forsberg, et al., "Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface," *IEEE PIMRC*, Sep. 2007.

[18] ROHDE & SCHWARZ (April 2009). *LTE technology and LTE test;a deskside chat* [Online]. Available: http://www.telecom-cloud.net/wp content/uploads/2010/11/Rohde-and-Schwarz-LTE-Tutorial.pdf

[19] Wikipedia (2012 January). *MIMO* [Online]. Available: http://en.wikipedia.org/wiki/MIMO

[20] *Technical Specification Group Radio Access Network; Feasibility Study for Orthogonal Frequency Division Multiplexing (OFDM) for UTRAN enhancement*, 3GPP TR 25.892.

[21] 4GWirelessjob(2012). *LTE MIMO Concepts* [Online]. Available: http://4gwirelessjobs.com/articles/article-detail.php?LTE-MIMO-Concepts&Arid=MTQz&Auid=OTY=

[22] *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation*, 3GPP TS 36.211, 2011.

[23] J. Zyren, "Overview of the 3GPP Long Term Evolution Physical Layer", 3GPPEVOLUTIONWP, 2007.

[24] *Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment radio transmission and reception,* 3GPP TS 36.101, 2012.

[25] Magnus Lindstrom," LTE-Advanced Radio layer 2 and RRC aspect". 3GPP LTE-Advanced Evaluation Workshop, 2009.

[26] Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2, 3GPP TS 36.300, 2012.

[27] Freescale, "Long Term Evolution Protocol Overview" LTEPTCLOVWWP, 2008.

[28] *Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification*, 3GPP TS 36.321, 2012.

[29] E.Dahlman, S.Parkvall, J.Slold, P.Beming et al., "3G Evolution HSPA and LTE for Mobile Broadband", 2nd ed. Academic Press, 2008.

[30] *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) protocol specification*, 3GPP TS 36.322, 2011.

[31] EventHelix (2009). *3GPP LTE Radio Link Control sub-layer* [Online]. Available: http://www.eventhelix.com/lte/presentations/3GPP-LTE-RLC.pdf

[32] *Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification*, 3GPP TS 36.323, 2011.

[33] Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification, 3GPP TS 36.331, 2012.

[34] C. Han, "Security Analysis and Enhancements in LTE-Advance Networks". Ph.D. Dissertation, Dept. Mobile Systems Eng, Sungkyunkwan Univ, 2011.

[35] F. Xiangning; C. Si; Z. Xiaodong; , "An Inter-Cell Interference Coordination Technique Based on Users' Ratio and Multi-Level Frequency Allocations," *International Conference on Wireless Communications, Networking and Mobile Computing,* pp.799-802, Sept. 2007.

[36] *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures*, 3GPP TS 36.213, 2011.

[37] Roke*, LTE MAC Scheduler & Radio Resource Scheduling* [Online]. Available: http://www.roke.co.uk/resources/white-papers/0486-LTE-Radio-Resource.pdf

[38] Computerworld. *4G LTE networks hit battery life on some smartphones, Metrico finds* [Online]. Available: http://www.computerworld.com/s/article/9226883/4G_LTE_networks_hit_battery_life_on_some_smartphones_Metrico_finds

[39] *LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Frequency (RF) system scenarios,* 3GPP TS 36.942, 2011.

[40] D. Yu; W. Wen, "Non-access-stratum request attack in E-UTRAN," *Computing, Communications and Applications Conference (ComComAp)*, pp.48-53, Jan. 2012.

[41] T. Hong, "Crosslayer Optimisation in LTE network to reduce the effect of Co-channel Interference," unpublished.

[42] T. Ha, *Theory and Design of Digital Communication Systems*. Cambridge, United Kingdom: Cambridge University Press, 2011.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Chairman, Code EC
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

4. Tri T. Ha
   Naval Postgraduate School
   Monterey, California

5. Weilian Su
   Naval Postgraduate School
   Monterey, California

6. Tat Soon Yeo
   Temasek Defence Systems Institute (TDSI)
   National University of Singapore
   Singapore

7. Lai Poh Tan
   Temasek Defence Systems Institute (TDSI)
   National University of Singapore
   Singapore

8. Teo Tiat Leng
   Defence Science and Technology Agency
   Singapore

9. Too Huseh Tien
   Naval Postgraduate School
   Monterey, California