Qos and security provisioning in 4G/5G LTE-advanced networks

Muhammad Jawad Alam Wahla

2017

Muhammad Jawad Alam Wahla. (2017). Qos and security provisioning in 4G/5G
LTE-advanced networks. Doctoral thesis, Nanyang Technological University, Singapore.

<http://hdl.handle.net/10356/72357>

<https://doi.org/10.32657/10356/72357>

QoS and Security Provisioning in 4G/5G LTE-Advanced Networks

Muhammad Jawad Alam Wahla

School of Electrical and Electronic Engineering

A Thesis submitted to the Nanyang Technological University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy

2016

Abstract

Quality of service (QoS) mechanisms deal with ensuring the high quality services offered by network. Reliability, accessibility and security are some of the main features of any service offered by a network. Support for diverse QoS requirements is one of the key areas of interest in the Long Term Evolution (LTE) and LTE-Advanced based networks. Carrier Aggregation (CA), in which the bandwidth is aggregated across different bands to achieve a higher bandwidth, is one of the most significant among them. Dual Connectivity (DC), Coordinated Multipoint Transmission (CoMP), Device-to-Device Communications (D2D), and Self-Organizing Networks (SON) are some of the other leading technologies introduced in LTE-Advanced. Because of the introduction of these new technologies, existing QoS and security mechanisms in LTE cannot be mapped directly to LTE-Advanced, so there is a need to investigate and develop new mechanisms for LTE-Advanced. The aim of this research is to develop QoS and security provisioning mechanisms for LTE-Advanced based 4G/5G networks

The CA technology has introduced new challenges for LTE-Advanced resource matching. Radio Resources Management (RRM) is one of the key elements for QoS provisioning. We have developed a new RRM technique utilizing game theory. Matching Markets are known to solve different resource-matching problems, such as kidney exchange, child adoption, matching doctors, and college admission. We model the problem of resource allocation as a matching game and propose a solution utilizing game theory, which takes into consideration the QoS demand of the users. The allocation is done based on channel conditions, QoS profiles, and carrier selection. The proposed Matching Game (MG) algorithm finds a stable Pareto efficient matching of resource blocks to users. Theoretical

analysis demonstrates that MG can find an optimal and stable outcome.

Next, we look into RRM techniques for the handover mechanism from a security perspective. 5G networks have stringent latency requirements for meeting the QoS. Authentication and key establishment are the key components of a secure handover. The focus of our research is to perform a secure handover within the latency requirements, so we present a secure handover scheme using Software-Defined Networking (SDN) in 4G/5G Heterogeneous networks (HetNet). In dense HetNet, the frequency of handovers magnifies the challenge of meeting the QoS. SDN will play a crucial role in future networks; moreover, we show that the proposed scheme can fulfill the delay constraints of 5G networks by making use of the centralized capabilities of SDN. Authentication information for the user device is securely transferred along the mobility path to enable fast handovers. We present formal security proof, proof of logic correctness and an informal security analysis of the scheme.

Using the same SDN model, we further explore authentication and key establishment in DC and CoMP scenarios of LTE-Advanced based 4G/5G networks. With the help of these technologies, a user device can simultaneously connect to multiple base stations. LTE specification addresses scenarios in which a direct secure link is available between access points. Due to the dense nature of a 5G HetNet, a direct connection is not possible in many cases. Existing authentication schemes and key establishments will not be able to meet the QoS requirement of the 5G network due to the delay incurred. We develop a security context transfer mechanism, which can pre-authenticate the destination AP by leveraging the SDN architecture. We create a Merkle-tree based authentication mechanism that reduces the computational overhead of authentications. Pre-authentication combined with a fast authentication phase enables this scheme to meet the latency requirements of 5G networks.

Acknowledgments

I would like to thank my supervisor, Dr. Maode Ma for his invaluable advice and guidance during this research. His encouragement has helped me to overcome many difficulties during the research.

I am also thankful to my family. It would not have been possible without their support. To my parents who have always encouraged and supported me in my pursuits. To my beloved wife Ainee for her unwavering support.

Contents

Abstract	i
Acknowledgments	iii
List of Figures	viii
List of Tables	x
List of Abbreviations	xi
List of Tables	xii
1 Introduction	1
1.1 Background	1
1.2 Objective	3
1.3 Contribution	3
1.4 Organization of Thesis	4
2 Background and Literature Review	6
2.1 LTE-Advanced Technologies	6
2.1.1 Carrier Aggregation	6
2.1.2 Relay Nodes	7
2.1.3 Femtocell	8
2.1.4 Coordinated Multipoint Transmission	9
2.1.5 Heterogeneous Networks	9
2.1.6 Self-Organization	10
2.2 LTE-Advanced Radio Resource Management	10
2.2.1 Frame Structure	10

2.2.2	QoS Framework	12
2.2.3	Related Work	14
2.2.4	RRM Through Nature-inspired Algorithms	20
2.2.5	Resource Scheduling	23
2.3	LTE-Advanced Security	26
2.3.1	Security Architecture	26
2.3.2	SDN Architecture	27
2.3.3	Authentication and Key Establishment	29
2.3.4	Handover Security	29
2.3.5	Related Work	31
3	Resource Matching in 4G/5G LTE-Advanced	37
3.1	Introduction	37
3.2	Matching Game	38
3.3	Problem Formulation	39
3.3.1	System Model	39
3.3.2	Problem Formulation	40
3.4	Matching Game Solution	42
3.4.1	Matching Game Model	42
3.4.2	Heuristic Solution Using Matching Game	44
3.4.3	Matching Game	45
3.5	Analysis of Matching Game	48
3.5.1	Proof of Stability	48
3.5.2	Proof of Uniqueness	49
3.5.3	Pareto Optimal Proof	50
3.5.4	Termination and Complexity	51
3.5.5	Simulation Result	51
3.6	Conclusion	59

4	Secure Handover in 5G	60
4.1	Introduction and Background	60
4.1.1	Review of AHM Scheme	62
4.1.2	Our Contribution	64
4.2	SDN Authentication and Handover Scheme	64
4.2.1	Handover Scheme	65
4.3	Security Analysis	70
4.3.1	BAN Logic Analysis	71
4.3.2	Initial Assumptions	73
4.3.3	Goal	74
4.3.4	Idealized Form	75
4.3.5	Analysis and Proof	76
4.3.6	Formal Security Verification Using AVISPA Tool	82
4.3.7	Security Analysis	84
4.4	Performance Analysis	86
4.5	Conclusion	90
5	SDN-Enabled LTE-Advanced CoMP Authentication	91
5.1	Introduction	91
5.2	Background	92
5.2.1	LTE-Advanced Dual Connectivity and CoMP	92
5.2.2	Open Issues	94
5.2.3	Merkle-tree-based Authentication	95
5.3	Proposed Scheme	96
5.3.1	Authentication and Key Establishment	96
5.4	Security Evaluation	101
5.4.1	Proof of Logic Correctness	102
5.4.2	Formal Security Proof	107
5.4.3	Security Analysis	112
5.5	Performance Analysis	113

5.5.1	Communication Overhead	114
5.5.2	Computational Cost	115
5.5.3	Energy Comparison	118
5.5.4	Performance Under An Unknown Attack	120
5.6	Conclusion	121
6	Conclusions and Future Work	122
6.1	Conclusions	122
6.2	Future Work	123
	Publication	125
	References	126

List of Figures

2.1	Types of Carrier Aggregation	7
2.2	Relay Nodes	8
2.3	Resource Block and Frame Structure	11
2.4	Nature Inspired RRM Techniques	20
2.5	Individual CC Selection	24
2.6	Security Architecture	26
2.7	SDN Architecture	28
2.8	EPS AKA	30
2.9	Key Hierarchy	31
2.10	Key Derivation	32
3.1	Downlink Throughput with Random Deployment	54
3.2	Downlink Throughput with Center Deployment	55
3.3	Downlink Throughput with Edge Deployment	55
3.4	Uplink Throughput with Random Deployment	56
3.5	Uplink Throughput with Center Deployment	56
3.6	Uplink Throughput with Edge Deployment	57
3.7	Fairness Evaluation with Random Deployment	57
3.8	Fairness Evaluation with Edge Deployment	58
3.9	Fairness Evaluation with Center Deployment	58
4.1	AVISPA Simulation	83
4.2	Security Protocol Animator's Message Sequence Chart	83
4.3	Authentication Time Under Successful Unknown Attack	89

5.1	Separate Bearer Scenario	93
5.2	Split Bearer Scenario	94
5.3	HeNB Scalability	95
5.4	Merkle-Tree	96
5.5	Merkle-Tree-Authentication	98
5.6	Security Protocol Animator's Message Sequence Chart	110
5.7	Communication Cost for CoMP	115
5.8	Computational Cost for CoMP	117
5.9	Energy Consumption for CoMP	119
5.10	Authentication Time Under Successful Unknown Attack	121

List of Tables

3.1	Notation Used	40
3.2	Simulation Parameters	53
4.1	Notation Used	67
4.2	BAN Logic Notation	71
4.3	Time Costs of Cryptography Operations	87
4.4	Time Costs of Cryptography Operations	87
4.5	Handover Authentication Time	88
4.6	Energy Consumption Comparison for UE	89
5.1	Notation Used	98
5.2	Computational Cost Comparison	114
5.3	Time Costs of Cryptography Operations	116
5.4	Comparison of Computational Cost	118
5.5	Energy Costs of Cryptography Operations	118
5.6	Comparison of Energy Cost	120

List of Abbreviation

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AMBR	Aggregate Maximum Bit Rate
AP	Access Point
API	Application Programming Interface
CA	Carrier Aggregation
CBC	Cipher Block Chaining
CC	Component Carriers
CK	Cipher Key
CoMP	Coordinated Multipoint Transmission
CQI	Channel Quality Indicator
DC	Dual Connectivity
DFT	Discrete Fourier Transform
DoS	Denial of Service
EAP-AKA	Extensible Authentication Protocol -AKA
eNB	Evolved Node B
EPS-AKA	Evolved Packet System - AKA
GA	Genetic Algorithm
GBR	Guaranteed Bit Rate
HARQ	Hybrid Automatic Repeat Request
HeNB	Home eNodeB
HetNet	Heterogeneous Network
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
ITU	International Telecommunication Union
LTE	Long-Term Evolution
M2M	Machine to Machine Communication
MAC	Media Access Control
MBR	Maximum Bit Rate
MIMO	Multiple Input, Multiple Output
MitM	Man-in-the-Middle

MME	Mobility Management Entity
MU-MIMO	Multi User MIMO
NOS	Network Operating System
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
PAPR	Peak-to-Average Power Ratio
QCI	QoS Class Identifier
QoE	Quality of Experience
QoS	Quality of Service
RRM	Radio Resources Management
RSA	Rivest, Shamir, and Adleman
SBS	Small-cell Base Station
SC-FDMA	Single-Carrier Frequency-Division Multiple Access
SCI	Security Context Information
SDN	Software-Defined Networking
SHA	Secure Hash Algorithm
SON	Self-Organizing Networks
SU-MIMO	Single User MIMO
UE	User Equipment
UMTS	Universal Mobile Telecommunications Service
VoIP	Voice over Internet Protocol
WiMAX	Worldwide Interoperability for Microwave Access

Chapter 1

Introduction

1.1 Background

Long-Term Evolution Advanced (LTE-Advanced) is an emerging radio access network technology, standardized in 3rd Generation Partnership Project (3GPP) and is evolving as an evolution of LTE. With the advancements in technologies, the media offered in social networks, and other applications are becoming more and more content rich, which is increasing traffic volume per subscriber at a fast rate. Another factor contributing to the growth of data content is the development of new services like mobile TV, e-learning solutions, online gaming, etc. These services have different QoS and security requirements. QoS and security mechanism will play a significant role in future 4G/5G networks. With the increase in network traffic, QoS provisioning is becoming more important in 4G networks. The increase in the traffic and various type of traffic means that the QoS requirements for the traffics will be different. Network congestion could lead to deterioration of the QoS if not properly handled. With different QoS requirements, new QoS mechanism needs to be developed to support these demands.

The significance of QoS is also important from telecom vendors and operators point of view. From the service providers point of view, service differentiation and subscriber differentiation are important factors in networks, which is why network operators and service providers are pushing towards the development of enhanced QoS mechanism to support this differentiation and demand. Service differentiation means that for the dif-

ferent type of services the service provider should be able to meet the different set of requirements. For example, for file transfer and browsing, a delay of 300-400ms does not have a significant impact. However, for online gaming, this delay could result in a substantial lag and would be more visible to the end users. Another example would be live streaming like mobile TV where QoS requirements are strict than buffered streaming (e.g. youtube). In addition to this, new devices (e.g. iPhone, Android-based smartphones, iPad) are multi-threaded and can support different applications at the same time so a user can be browsing, downloading, chatting, listening to music at the same time. QoS demand for each application can be different, so there is a need for QoS mechanisms in 4G networks to support these scenarios.

From service provider perspective another important factor is subscriber differentiation. Subscriber differentiation means that the service providers would like to have the ability to provide different QoS to different clients. From a commercial perspective, this has a great significance. In future, this could allow the service providers to charge by the quality experience. Currently, most of the charging is done by the amount of data used over the networks but once the data growth increases data quality will take precedence over quantity in networks. Some examples of the subscriber differentiation could be prepaid vs. postpaid customers or emergency calls (911). During a disaster, a different set of QoS could be needed to give high priority to public safety networks related calls for disaster management. The significance of QoS in 4G networks is immense, and there is a need for QoS mechanism in the 4G networks.

Security is an important service provided by 4G/5G networks. Security quality of service is measured in terms of the strength of the underlying mechanism against an attack vector. Support of privacy, confidentiality and integrity are some of the core features expected from a secure system. To cope with the growth in data rate, many new technologies have been proposed in the 4G/5G system. Supporting security on these technologies is one of the primary goals. Security provisioning with QoS requirements remains an important research area in LTE-Advanced networks.

1.2 Objective

The objective of this thesis is to explore the QoS and security aspect of the LTE-Advanced networks. 4G/5G based LTE-Advanced networks have introduced many new technologies such as Carrier Aggregation (CA), Coordinated Multipoint Transmission (CoMP), Dual Connectivity (DC), Software-Defined Networking (SDN), Relays, Femtocell, and Self-Organizing Networks (SON). We explore the impact of some of these technologies on the security and QoS of the LTE-Advanced based network and propose a solution to improve them. Radio Resource Management (RRM) techniques can be used to improve QoS in the network. There are many RRM techniques which can impact the QoS; we will focus our research on the resource scheduling mechanism. From a security aspect, we will be focusing our research on the authentication and key establishment procedures. The study will also focus on the performance aspect of the security scheme to see how it impact the QoS of the system. Based on the objectives, the scope of the thesis is limited to following proposals.

- (i) Proposal of a scheduling scheme for CA based 4G/5G LTE-Advanced network. The scheduling procedure will consider the QoS of the system.
- (ii) Proposal of authentication and key establishment procedures in 5G SDN-enabled LTE-Advanced networks.
- (iii) Proposal of an efficient authentication and key establishment scheme for CoMP and DC scenarios in 4G/5G LTE-Advanced networks.

1.3 Contribution

The main contribution of the thesis are:

- (i) We propose a game theory inspired resource matching scheme for CA based LTE-Advanced networks. We model the resource optimization problem as a matching market and propose a heuristic solution for matching. The proposed solution can achieve a stable Pareto optimal matching. The proposed matching is based on

the QoS profile of the user devices and takes into account the changing channel conditions for scheduling. Simulation results show that the proposed scheme is better than the existing scheme.

- (ii) We propose a secure handover scheme in 5G SDN-enabled HetNet. The proposed scheme leverages SDN architecture to perform the authentication and key establishment procedure which meets the latency requirements of the 5G network. We explore the existing 5G SDN secure handover scheme and find it vulnerable to attacks; we then propose a new scheme. We present a proof of logic correctness using BAN (Burrows - Abadi - Needham) analysis. Formal security verification is done using AVISPA, and an informal security analysis is also presented. Performance analysis shows that our scheme is faster and consume less power.
- (iii) We propose an authentication and key establishment scheme for 4G/5G LTE-Advanced CoMP and DC procedures. We use SDN architecture presented in the earlier scheme and use a Merkle-tree based fast authentication. We present formal and informal security analysis along with proof of logic correctness. Performance analysis reveals that our scheme consumes less power compared to the existing scheme. The proposed scheme outperforms in terms of communication overhead and computational cost.

1.4 Organization of Thesis

The first phase of our research is focused on QoS provisioning in LTE-Advanced 4G/5G systems. We have focused on resource scheduling in LTE-Advanced. We propose a game theory based solution for this problem. The second phase of our research is focused on security provisioning in LTE-Advanced based 4G/5G systems. We focus our research on authentication and key management in 5G network. We propose a scheme for secure handover in 5G networks. Next, we propose a scheme for DC and CoMP authentication in the LTE-Advanced network.

In chapter 2, we provide a brief background on LTE-Advanced based 4G/5G networks.

The literature review presented in this chapter covers two main areas. Firstly, we present a high-level view of RRM techniques which are used to improve QoS in the system then we focus on resource scheduling and covers the research done in this area. Next, we focus on the security of LTE-Advanced networks. A brief introduction of security architecture and key management in LTE-Advanced is presented. Then we investigate schemes used for authentication and key establishment in LTE-Advanced based 4G/5G networks.

In chapter 3, we study resource scheduling LTE-Advanced networks. Inspired by the matching markets theory in economics, we model the optimization problem as a matching game and present a heuristic solution to find a stable matching. The study performs a performance analysis of the proposed scheme.

In chapter 4, we explore secure handover in 5G networks. We present an SDN-based secure handover authentication and key management scheme which can meet the requirements of a 5G network. Formal security analysis, BAN analysis, and informal security analysis is carried out on the proposed scheme.

In chapter 5, we study CoMP authentication in LTE-Advanced based 5G networks. The proposed scheme leverages SDN architecture to perform a Merkle-tree based authentication. The proposed scheme will be able to meet 5G network requirements. We present a formal security analysis using AVISPA, proof of logic correctness and informal security analysis. The study also presents a comparison with existing authentication scheme in terms of communication overhead, computational time and power consumption.

Chapter 6 concludes the thesis with some directions for future research.

Chapter 2

Background and Literature Review

2.1 LTE-Advanced Technologies

3rd Generation Partnership Project (3GPP) has designed LTE-Advanced to meet International Telecommunication Union (ITU) requirements for 4G networks. LTE-Advanced has introduced several new technologies which improve the capacity, coverage, performance, reliability, and security of the cellular network. These new technologies have changed the QoS and security requirements of the network. We give a brief introduction to some of these technologies here.

2.1.1 Carrier Aggregation

The maximum bandwidth allowed in LTE as per 3GPP specification is 20MHz. In order to increase the bandwidth, Carrier Aggregation (CA) has been suggested in LTE-Advanced [1]. In CA, multiple Component Carriers (CC) are combined to increase the overall bandwidth of the system. This aggregation allows the network to achieve a higher bandwidth. 3GPP specification allows for a combination of up to five carriers. The bandwidth of an individual component can be 1.4, 3, 5, 10, 15 or 20 MHz, allowing for a maximum combination of 100 MHz. Contiguous and non-contiguous are the two main categories of CA as shown in Figure 2.1. Both contiguous CA and non-contiguous CA can be inter-band or intra-band. For an inter-band CA, the coverage area for the individual CCs will differ, which is due to the fact that bands operating at different

frequencies will experience different path losses. A survey of RRM techniques has been presented in [2]

Figure 2.1: Types of Carrier Aggregation

2.1.2 Relay Nodes

In LTE-Advanced, the concept of relay nodes has been proposed to help increase the coverage and improve the capacity of the network. In relay based communication, a relay station helps to send a message from a base station to a User Equipment (UE), which may be outside the range of the base station. This way, the signal and service of the base station is extended. There are two categories of relays: Type-I and Type-II. The main purpose of Type-I relays is to extend the service and signal and enables the UE, while it is out of range from the base station, to communicate through the relay. Type-II relays improve the service quality and link capacity. In this type, the relay node and the UE are both within the base station coverage and can communicate directly with the base station. Combining relays, CoMP, and DC, we get multipath diversity and transmission gain, which helps to improve the overall system capacity.

Relays have added new challenges to RRM. Relays create additional interference in the network, and relay interference management is an open research area. Relay handoff decisions need to take new requirements into consideration e.g. backhaul availability, load balancing, and security. The total number of relays and the impact of their positioning on the performance needs to be investigated. From a QoS perspective, support for a

relay network needs to guarantee delay and bandwidth in the relay network. Zhao et al. [3] propose a downlink resource allocation scheme for LTE-Advanced Type-I relay nodes. This scheme focuses on maximizing the throughput of worst UEs in the relay enhanced network. From a security perspective, secure handover needs to be completed within the QoS requirements. A secure handover scheme for mobile relays has been presented in [4]. The scheme employs a proxy re-encryption technique where public keys encrypted at mobile management entity (MME) are re-encrypted at the mobile relay node.

Figure 2.2: Relay Nodes

2.1.3 Femtocell

Femtocell technology has been included in the standardization of LTE-Advanced. A femtocell is made of a low-cost base station or Home eNodeB (HeNB) and serves subscribers within a short range or 10-30m. With its reduced cell size, it can achieve high capacity gains. Some of the benefits of a femtocell include improving indoor coverage, boosting spectral efficiency, offloading macrocell network, increasing data rates and removing dead spots. One of the problems with the femtocell technology is that as high numbers of femtocells get deployed, overlaying networks will have cross-tier interference. As the number of femtocells and their locations in a network is unknown, interference management becomes a fundamental problem that needs to be resolved in the femtocell technology. Feilu et al. [5] has investigated small-cell traffic balancing over licensed and unlicensed bands. Interference between different femtocells and macrocells is one of the problems in this area that need to be addressed for QoS guarantee. Resource allocation

for LTE-Advanced HetNet has been investigated in [6]. This method formulate resource allocation as MAX-K cut problem. From a security perspective, handover scenarios of HeNB need to be investigated to provide fast authentications and handovers.

2.1.4 Coordinated Multipoint Transmission

Coordinated Multipoint Transmission is used to improve cell edge users' performance. A cell edge user can receive from or transmit to different cells. If the signal from neighboring cells is coordinated, then user performance can be improved, and system capacity gets enhanced. CoMP is categorized into inter-site and intra-site, based on a base station coordination method. From a QoS perspective, distribution of bearers among different eNB is an open research area. Proportional fair resource allocation for LTE-Advanced CoMP has been investigated in [7]. The scheme introduces a parallel successive convex approximation-based algorithm to solve the optimization problem. Dania et al. [8] introduces an optimized CoMP transmission scheme for a HetNet using enhanced intercell interference coordination method. From a security perspective, a user device needs to be connected to multiple base stations simultaneously, so authentication and key establishment in CoMP transmissions need to be investigated.

2.1.5 Heterogeneous Networks

Support of Heterogeneous networks (HetNet) is one of the most important features of LTE-Advanced, enabling the network to achieve high data rate goal. In HetNet, small cell (microcell, femtocell, Pico cell) and Wi-Fi access points can be used to offload a great share of the network traffic load. Network operators' operating expenses and capital expenses will be reduced by supporting HetNet. In LTE-Advanced, HetNet is increasingly used to complement the coverage and capacity of the conventional cellular network. Macrocell will have a lesser load if dense areas offload some of their data traffic to small networks such as Wi-Fi or small-cell base station (SBS).

2.1.6 Self-Organization

Self-organization is an important feature in LTE-Advanced networks. The specification allows for the network to self-configure, self-optimize and self-heal. In self-configuration, when an eNB is added to the network, it is able to configure automatically with minimal manual support from the outside. This allows a considerable reduction in network deployment and setup time. This also allows for a reduced Capex (capital expenditure) from a network operator point of view. In self-optimization, the network is able to monitor key parameter indicators of the network such as QoS, Quality of Experience (QoE), load capacity and can adjust the parameters to optimize performance. The self-healing features allow the network to recover from any failure or loss of coverage. It involves techniques that can detect failures and help with recovery. Plamen et al. [9] proposes distributed autonomic load balancing through a programmable learning model. It employs machine learning algorithm to solve optimization problems and tasks. Hafiz et al. [10] have explored conflict between different SON functions and proposed a self coordination framework for conflict resolution. A survey of self-configuring and self-optimizing HetNets has been presented in [11].

2.2 LTE-Advanced Radio Resource Management

Radio Resource Management (RRM) is an important way to provide QoS in LTE-Advanced. Link adaption, power control, packet scheduling, Hybrid Automatic Repeat Request (HARQ), admission control, mobility control, and handover are some of the main methods of RRM. The main focus of our research is Resource Scheduling, and in order to explain the scheduling, we provide a brief overview of resource blocks.

2.2.1 Frame Structure

Scheduling is an important tool for efficient RRM. A resource block is the smallest unit of resource scheduling in LTE and LTE-Advanced based 4G/5G networks. The structure of a resource block and frame is similar in LTE and LTE-Advanced. A frame is divided

into ten parts, where each part is called a subframe. Each subframe is of 1 ms and is divided into two equal slots. Each slot consists of 6 or 7 OFDM symbols. Figure 2.3 shows the structure of a frame and a resource block. A resource element is defined as an OFDM symbol over a carrier. The smallest schedulable unit a resource block consists of up to 84 resource elements. The total number of resource blocks available for scheduling is defined by the overall bandwidth of the system. For a 1.4 MHz band, a total of 6 resource blocks are available, and for a 20 MHz band, a total of 100 resource blocks are available. In LTE-Advanced, Orthogonal Frequency-Division Multiple Access

Figure 2.3: Resource Block and Frame Structure

(OFDMA) is used in the downlink channel. It is a multi-user variant of the Orthogonal Frequency Division Multiplexing (OFDM) technique. In OFDM, orthogonal sub-carriers are used to transmit data on them in parallel. The sub-carriers could overlap but at the sampling point, there is no interference due to orthogonality. Adaptive modulation can be used on each of the sub-carriers. Single-Carrier Frequency-Division Multiple Access (SC-FDMA) adds a Discrete Fourier Transform (DFT) to the OFDMA scheme. It helps to reduce Peak-to-Average Power Ratio (PAPR), and it offers better power efficiency than OFDMA. SC-FDMA is used in the uplink due to lower power consumption at the user device.

2.2.2 QoS Framework

QoS in LTE is evolved from the previous 3GPP specifications. QoS support is present in the Universal Mobile Telecommunications Service (UMTS) network, and this support is further enhanced in LTE network. Evolution of LTE leads to LTE-Advanced, and QoS remains significant in these networks. A brief summary of parameters is provided to explain QoS framework in LTE. The main QoS parameters described in the specifications are described below.

2.2.2.1 Bearer

Bearer identifies a packet flow in LTE. A bearer can be considered as a logical connection for a service flow between different nodes. Each bearer has some parameters attached to it which help to provide a QoS for a specific flow of traffic. UE and eNB can have several bearers between them one of each type. Bearer concept is also used during admission control. Admission is granted based on the fact that network will be able to support the requirements for the particular service flow. LTE specifications define default and dedicated bearer as the two types of bearers. These bearers can have guaranteed bit rate (GBR) or non-GBR. According to 3GPP specifications, a default bearer has to be non-GBR. A default bearer is used for the initial connection; it is established once the UE is admitted to the network. A default bearer might need to support a dynamic traffic

where the data rate is not known during the setup. For this reason, a non-GBR setup is preferred. The dedicated bearer can be GBR or non-GBR. Dedicated bearers are created when there are new services requiring support with different QoS requirements. The creation of a bearer involves admission control and charging policy. The charging policy determines charges that would be applied to the service. If a dedicated bearer is dropped, the service or data flow is mapped back to the default bearer. A GBR bearer can block some of the system resources to support the bit rate. However, non-GBR do not have any such requirements and therefore non-GBR bearers can last longer. In CoMP and DC-based LTE-Advanced networks, the traffic is offloaded when a bearer is assigned to the destination eNB.

2.2.2.2 QCI

LTE QoS framework separates service quality into different categories. QoS Class Identifier (QCI) is a QoS class identifier used for differentiating various categories. Each bearer will have a QCI value assigned to it during the bearer setup phase. This QCI value is used to determine the priority and delay requirements for the particular flow of the traffic. These values are pre-configured by the network operators, and they give the operators control of the QoS service. This architecture helps to provide subscriber and service differentiation. QCI ensures that all traffic in the service flow will have some degree of guarantee determined by its priority.

2.2.2.3 Allocation Retention Priority

The Allocation Retention Priority determines the retention priority of the bearer. It deals with the allocation of a bearer, a change in bearer and rejection of a new bearer request. In the case of system overload, it also determines which connections to drop, so as to maintain the QoS of higher priority connections.

2.2.2.4 Maximum Bit Rate/Aggregate Maximum Bit Rate

Maximum Bit Rate (MBR) is the maximum bit rate allowed per bearer, and Aggregate Maximum Bit Rate (AMBR) is the sum of all bearers MBR for a particular UE. The

aggregate bit rate is defined so that a network operator can limit the maximum bit rate which can be used by one subscriber. It is another aspect of the QoS architecture which gives the operator control over subscriber differentiation. Using these parameters, differing quality for the same services can be given to users. In LTE-Advanced-based networks, eNB controls QoS classification. The users or subscribers do not have much control on the QoS of the network, as the control lies with the service providers.

2.2.3 Related Work

Much research has been carried out in LTE/LTE-Advanced RRM techniques. In this section, we will review some of the work done in this area.

2.2.3.1 Link Adaption

Link adaptation procedures adapt the link-related parameters like power control, modulation and bandwidth according to the design. Adaptive modulation and coding are used in LTE/LTE-Advanced meaning that depending upon the channel condition, the modulation and coding schemes will be changed or adapted. For high-quality channels, higher modulation can be used, and when the channel quality starts to decrease, the lower modulation scheme is used, so the end quality experience does not degrade too much. Outer link adaptation algorithms are vendor-specific, and they are used to minimize the block error rate during initial transmission. The combination of these techniques can be used in the link adaptation to improve the QoS. 3GPP specification has specified fractional power control formula, which can be used to determine the transmission power for the user equipment. In [12], the author proposes a downlink adaptation scheme in LTE-Advanced. This method considers enhanced relay systems in LTE-Advanced. In type II relay system, the CQI information is not estimated at UE, due to the lack of a reference signal for the relay. This information is required to select modulation and coding scheme for link adaption. The paper presents a link adaption algorithm for such systems. In [13], power scaling on Physical Uplink Shared Channel (PUSCHs) has been investigated. The study is focused on CA-based uplink power control. In another study

[14], a new method for CQI calculation has been proposed. [15] presents a new adaptive transmission scheme for LTE-Advanced.

2.2.3.2 Load Balancing

Load balancing is a procedure in which the load is equally balanced across the network. In load balancing, highly loaded cells offload some of their network traffic to lightly loaded cells. This balancing improves the utilization of the network under a heavy load. By balancing the load, the overall QoS experience improves. It helps to avoid congestion in the network if the load is evenly distributed. Similarly, underutilization of some portion of the network can also be improved. From an LTE-Advanced QoS perspective, load balancing plays a vital part in improving the key performance indicators. With the introduction of CA, load balancing among different carriers is also an open area of research. Warabino et al. discuss load balancing in a carrier aggregation system [16]. The introduced method in their study provides an improvement over traditional handover-based load balancing. Another study [17] investigates methods for load balancing in LTE-Advanced across multiple carriers with a bursty traffic model. Two load balancing methods have been proposed in [18] to improve performance in CA-based LTE-Advanced systems. Lee et al. focus their investigation on femtocell and suggest a load balancing technique with transmission power control [19]. Wang et al. examine carrier load balancing for allocating component carriers to the users [20]. A dynamic adjusted carrier-coverage-based load balancing method has been recommended in [21]. It shows that better load balancing can increase system throughput. Multi-cell load balancing with CoMP and load balancing across CC in CA remains the main focus of research.

2.2.3.3 Packet Scheduling

Packet scheduling is one of the most important RRM techniques to improve the QoS. In LTE-Advanced, the scheduling decision takes place in the eNB. The Media Access Control (MAC) layer is responsible for the scheduling of the physical resources blocks. Different research work has been carried out in this area whereby improving packet-scheduling methods; overall QoS has been enhanced. Some of the main issues open in

this area are to improve throughput, reduce delay, provide QoS guarantee and provide fairness. Packet scheduling is required by both integrated services and differentiated services architecture for QoS support. Research in LTE-Advanced packet scheduling is related to support different traffic, e.g., VoIP, mixed, or best effort, or it may be related to the improvement of delay, throughput increase, and ensuring fairness.

2.2.3.4 Uplink Scheduling

For the uplink, the OFDMA variant used is called Single Carrier Frequency Division Multiple Access (SC-FDMA). OFDM has a high peak to average power ratio for the mobile terminal, which is a major factor for low-power mobile devices. There is some research work carried out in this area in [22]; the study investigates MU-MIMO or virtual MIMO scheduling in the uplink. The study performs a comparison between SU-MIMO and MU-MIMO. In [23], CA-based LTE-Advanced uplink scheduling performance has been analyzed. It shows that CA improves average user throughput. In a CA system, uplink carrier selection methodology has been examined in [24]; this method differentiates the devices into power limited and non-power limited. Power limited is assigned single carrier, and non-power limited is assigned multiple carriers. Edge-prioritized scheduling has been studied in [25] using a heuristic mechanism. Research in [26] also considers uplink scheduling with MIMO using multi-clusters with carrier aggregation. Delta metric scheduling improves average uplink throughput in [27]. MU CoMP scheduling is investigated in [28]; it concludes that cell edge spectral efficiency can be improved by using CoMP and MU scheduling. A dynamic carrier aggregation scheme to improve energy efficiency is proposed in [29]. The maximum power reduction scheduling algorithm is presented in [30]; it also provides a method to decide SU or MU-cluster scheduling.

2.2.3.5 Downlink Scheduling

LTE-Advanced uses OFDMA for the downlink. OFDM is chosen because of its resilience to interference and multipath delay. In the downlink, subcarriers are divided into resource blocks. Resource blocks (RB) comprise 12 subcarriers for different bandwidths: 1.4(6 RB), 3(15 RB), 5(25 RB), 10(50 RB), 15(75 RB), and 20(100 RB) Mhz. They also

cover one slot in the time frame. OFDMA scheduler can be both time and frequency opportunistic. There is some research carried out in this area. Reinforcement learning based radio resource scheduling in LTE-Advanced has been considered in [31]. Lei et al. propose a scheduling algorithm (RSM-CA) which improves over PF [32]. Chung et al. also uses PF as a base and modify for RT and NRT traffic [33]. The paper concludes that in carrier aggregation, combined scheduling is preferred over independent scheduling. In [34], the author reaches a similar conclusion that aggregated scheduling will perform better than independent scheduling. This method uses a quantized water-filling model. [35] models the problem as a transportation problem and improves over traditional PF scheduling. It can be seen that currently it has been established that aggregated carrier scheduling is better than independent. A CoMP Multi-cell MU-MIMO scheme for downlink has been presented in [36]. This helps to improve cell-edge user throughput. An energy-efficient variant of the proportional fair algorithm has been proposed in [37]. Energy efficient, coordinated scheduling for CA-based systems has been studied in [38]. [39] proposes downlink MU-MIMO scheduling using rank balancing method. Layer adaptive scheduling method has been proposed in [40]. QoS scheduling and backward compatibility with LTE needs to be investigated. Different types of traffics and devices will require new methods to schedule the aggregated traffic, which will be different from the independent scheduling method used in LTE networks. With CoMP, multi-cell scheduling is also an area of interest for latest research.

2.2.3.6 HARQ

The impact of HARQ is also considered for QoS improvement in LTE/LTE-Advanced. Hybrid automatic repeat request is used to minimize the overhead of Automatic Repeat Request (ARQ). ARQ performance is good when the channel quality is good; however, when the signals in a channel are not good, HARQ performs better. When a damaged packet is received, the receiver can request for retransmission, and that is where HARQ comes into play. There is some overhead required for using HARQ, so that if the retransmissions exceed the maximum allowed number, then the retransmissions are stopped.

2.2.3.7 Admission Control

Admission control deals with accepting or rejecting new connections. Using the admission control, the network can ensure a certain QoS guarantee. The admission of a new connection is not accepted if the network cannot support the QoS requirements of the new connection. Call admission plays a major role in QoS provisioning of a network. Call blocking, call dropping, delay and packet loss are some of the key performance indicators which can be improved by improving the call admission mechanism. For the cellular network, many call admission control methods have been suggested. In LTE-Advanced, the addition of support for technologies like femtocells, relays, and interworking with the heterogeneous network, has opened many new areas of research in call admission which need to be addressed. [41] investigates admission control for LTE-Advanced relay systems.[42] proposes a priority and buffer-based admission control mechanism.

2.2.3.8 Handover

Handovers are used when a UE is moving from one cell into another cell. LTE does not support soft handovers. The design and principles of handover within LTE are explained in detail in [43]. To provide a seamless network access across heterogeneous networks handover handling plays an important part. A survey in [44] explains handover framework in LTE-Advanced relay network. This paper proposes a method to extend the handover method in LTE to LTE-Advanced networks. Chang et al. proposes a handover scheme for LTE-Advanced systems in [45]. The method proposes soft handover carrier aggregation (CA) for VoIP traffic. The paper concludes that a fractional soft handover scheme reduces handover outage probability. This scheme also maintains the QoS of VoIP services. [46] proposes a method where primary component carrier and secondary component carrier are considered in an LTE-Advanced system using CA and handover is based on PCell. [47] proposes a self-optimization handover algorithm. The proposed algorithm adjusts handover parameters to optimize handover performance. Parameter optimization is also investigated in [48]. [49] studies the handover procedure for LTE-Advanced in femtocells. [50] evaluates capacity-based CoMP handovers.[51] proposes a

handover scheme for a joint processing method of CoMP. For relay networks, prediction-based handover schemes have been proposed in [52]. A low-overhead handover scheme has been considered in [53] for a two-hop relay network.

2.2.3.9 Relays

A brief introduction of some work done for relay support in LTE-Advanced has been summarized here. The effects of relaying in 3GPP LTE-Advanced is studied in [54]. Zheng et al. perform a performance analysis of L1 relays in [55]. Nagata et al. investigate the performance of L1 relay and compare it with the performance of L3 relays in [56]. L1 relays act like a booster or amplifier to forward signals to UE. L1 relay functionality is simple and has less cost. L3 relays perform demodulation and decoding and then perform other functions like encryption and decryption, after which they modulate and encode data before retransmitting it. This way, inter-cell interference is reduced. The impact of different factors like the location of relays, the number of relays, and the number of back-hauls, have been simulated and showed. Relay deployment issues have investigated in [57]. Some relay nodes and node placement have been studied for finding a cost-efficient deployment method. Another study [58] proposes terminal relaying, and it suggests that instead of using static relays, wireless terminals can also be used as relays. Research directions and problems in this area are highlighted in this study in detail. Multiple relay selection strategies have been analyzed in [59]. The importance of power control parameters is analyzed in [60] to achieve optimal performance in relays using the LTE-Advanced network. Semi-persistent scheduling for Voice over Internet Protocol (VoIP) has been proposed for relay networks in [61]. The studies show that packet delay can be reduced and capacity increased by using a relay, and better QoS can be provided. Multi-hop relay performance analysis has been done in [62] from the point of the relay number to be used and relay placement. Some of the areas open for research in relay network are mobility, multi-hop architecture, multi-carrier transmission, carrier aggregation, power saving, transparent relaying, cooperative transmission, security and QoS support.

2.2.4 RRM Through Nature-inspired Algorithms

As described above, many RRM techniques can help to improve the QoS of LTE. The nature-inspired mechanism is one of the important ways to improve the RRM by modeling them as optimization problems. In LTE-Advanced, algorithms which are inspired by nature have been an area of research interest. Resource scheduling can be modeled as an optimization problem where the resources need to be optimally distributed while considering the QoS of the system. Figure 2.4 shows the main categories of the nature-inspired algorithm, which are used for RRM. Particle Swarm, Firefly, and Ant Colony-based solution remain the primary inspiration for solving optimization problems. A brief summary of the inspirations for various RRM techniques is listed below.

Figure 2.4: Nature Inspired RRM Techniques

- Particle Swarm Optimization: This popular technique is inspired by swarms of birds and fish [63].
- Nest Building: This has been a focus of self-assembly algorithms and division of

labor [64].

- Ant Colony Optimization: Routing algorithm inspired from ant foraging behavior has been proposed [65].
- Bee Inspired: The multi-objective optimization problem can be solved using bee inspired techniques [66]. Important features such as bee dance [67], bee foraging [68], nest site selection [69], navigation [70], task selection [71] have been explored.
- Firefly: This has been a focus of optimization problems [72].
- Simulated Annealing: This is inspired by annealing in metallurgy and has been a focus of optimization problems [73].
- Ant cemetery organization is another nature inspired cooperative strategy for solving optimization problems [74] [75].
- Evolutionary Inspired: Another important set of algorithms are inspired by the evolution process, using its techniques of selection, mutation, and inheritance. Genetic algorithm and game theory based solutions have been the main focus of research in this category. Evolutionary algorithms are often used for optimization problems [76].

Resource allocation of a multiuser cooperative system using genetic algorithm has been proposed for LTE-Advanced relays in [77]. The study recommends a centralized scheduler and uses an equal bit algorithm for allocation. The optimization problem is defined as maximizing the throughput under the power constraints. At the start, the initial population is generated randomly. Next, the genetic process has three main steps which the algorithm performs iteratively. As a result, the iteration candidate with the highest fitness parameter is selected. This is called selection. The next two steps are crossover and mutation. Based on the crossover and mutation probability, a new population set is determined. Next follows the selection process, and the whole process is repeated iteratively until the maximum generations are allowed. The study concludes that the genetic

algorithm offers a better throughput compared to the evolutionary-based algorithm. The process involves iterations in which parent solutions are used to select the child solution. As a result, the latest generation shows the lowest energy consumption of the system.

Ali et al. [78] presented a network planning problem solution through the quantum-inspired evolutionary algorithm. The problem is modeled as a multi-objective optimization problem from a network planning perspective. Results show that this method outperforms Genetic Algorithm after several iterations. An iterative tracking method using the Genetic Algorithm is used to minimize the overall energy consumption in the system in [79]. The optimization problem is modeled as minimizing the power consumption. The problem defines three constraint sets on the optimization problem. Selection of the coding gain and rate, selection of the modulation rate and QoS of the system are the constraints.

Thompson et al. [80] have proposed an adaptive scheduler for LTE which focuses on reducing the Inter-cell interference. In this study, Evolutionary algorithms have been used to optimize the scheduling parameters. In the proposed solution, Evolutionary algorithm chromosome represents the adaptive scheduler parameter. The Roulette-wheel selection operator is applied to select the parents; then uniform crossover is applied to produce two children in each generation. The next step is a mutation, where a single gene mutation is involved. After this population selection, the next iteration is done. If the mutation results in a child that is better than the current worse child, than the population selection step will select it. The study shows an improvement in the cell-edge user throughput.

Game theory inspired solution have been the focus of many optimization problems. Evolutionary game theory has been used to model some of the solutions. Resource management in LTE-Advanced M2M is a main area of research. M2M will add many devices to the network which could lead to congestion. Resource management and load balancing have been an open research area in M2M. In [81], the authors propose an evolutionary game theory inspired algorithm solution for this problem. In the model, MTC devices are players and the strategy is based on the selection of the base station.

Replicator dynamic is defined in terms of the rate of change of the strategy selection; this continues until the equilibrium is reached. Equilibrium is the state in which there is no incentive for a player to change their strategy, i.e., no further payoff improvement can be achieved. The devices use the Access Class Bearing (ACB) mechanism to randomly access the network. The process starts with the selection of an ACB value. Once the equilibrium is reached, the ACB value is broadcasted to the network. For access to the network, each device draws a random number and compares it to the ACB value. This decides whether the device can access the network on the current turn or must wait for the next turn.

2.2.5 Resource Scheduling

The focus of our research is resource scheduling in LTE-Advanced with carrier aggregation. In this section, we will review the work related to this area. With the introduction of CA, the resource scheduling process needs to take care of an additional step of carrier selection. There are two possible ways to carry this out. Carrier selection can take place before resource assignment on the selected carrier as shown in Figure 2.5 or both can be done in one step. Research in carrier selection can be categorized into three broad categories as described below.

2.2.5.1 Random Selection

In this method, the individual Component Carriers (CC) are randomly selected. The main advantage of this approach is to improve load balancing; however, it has a major shortcoming of network underutilization. Random and round-robin selection methods are investigated for carrier aggregation in [82]. After the carrier aggregation is done, the resource scheduling uses a proportional fair and Modified Largest Weighted Delay First (M-LWDF) algorithm. The study provides a new selection method for non-contiguous CA CC.

In [83], a similar model of CC selection is used in which the carrier is selected separately. The novelty of this approach is that the LTE-Advanced user can be assigned

Figure 2.5: Individual CC Selection

to all CC. This scheme provides the load balancing using a mobile hashing algorithm. In this method, the hash values are uniformly distributed and are mapped directly to the CC. The study also compares cross-carrier scheduling with single carrier scheduling. Results show that cross-carrier scheduling outperforms single-carrier scheduling. Load balancing across the carriers is also examined in [17]; this study suggests using round robin load balancing when the assignment is limited to a single CC per user. The scope of the research is restricted to the bursty traffic model. The theoretical formulation in [20] compares the two popular approaches to round robin mobile hash balancing. The study suggests a new cross-carrier scheduling algorithm which is a variant of a PF scheduler over multiple CC. [84] and [85] consider load balancing in a carrier aggregation scenario.

2.2.5.2 Round Robin Selection

The second method for carrier selection is a circular selection. Performance analysis carried out in [86] and [85] shows that this approach offers better utilization than the random selection. A dispatching policy is used to schedule the resources. Circular dispatching and least load dispatching are the policies considered in the study. The study also concludes that an optimal dispatching policy is impossible to realize.

2.2.5.3 Lead Load Selection

The third method is to select a carrier based on the Least Load (LL) [86], [87] and [20]. The performance analysis of these studies shows that it offers better load balancing than the round robin mechanism. The main shortcoming of this technique is that it does not consider the channel condition for carrier selection. LTE-Advanced devices can be scheduled over multiple carriers. If the selection is made on the least load carrier, then it might not be the carrier with the best channel condition. This results in a lower network throughput and low throughput for LTE-Advanced devices.

2.2.5.4 Joint Scheduling

Subsequently, several studies show that joint scheduling is better than single-carrier based scheduling. Zhang et al. [88] compared joint scheduling and single-carrier scheduling. It is concluded that joint scheduling is better when compared with the single-carrier scheduling. In [33], the scheduling system is divided into real time and non-real time queues. The classical PF algorithm [89] is used for joint scheduling. Chen et al. [87] uses a joint and disjoint queue scheduler, whereas the packet scheduling is done with PF.

2.2.5.5 Resource Assignment

For distribution of the resource blocks, the main selection categories are RR, PF, and delay-based selection. In RR [84], [85], [87] and [88], channel condition and load balancing factors are not considered. Proportional fair in [20] and [83] remains the most popular and widely accepted mechanism. The delay based assignment in [82] and [34] is based

on M-LWDF [90] variants. This is focused towards real-time traffic, which is sensitive to delays.

In [91], the author proves that in LTE the resource scheduling problem is an NP-hard problem. With CA in LTE-Advanced, the overall complexity of the problem has increased. In our research, we will address this issue using a heuristic solution based on game theory.

2.3 LTE-Advanced Security

2.3.1 Security Architecture

A brief introduction of LTE security architecture is necessary to explain the related work. The security relations between important network components such as Mobile Equipment (ME), Universal Subscriber Identity Module (USIM), Access Network (AN), Home Environment (HE), and Serving Network (SN) is shown in Figure 2.6. 3GPP divides the security architecture into five feature groups:

Figure 2.6: Security Architecture

- (i) Network access security: The radio access link is protected through the network access security features. It provides protection to access between ME, USIM, the

core network.

- (ii) Network domain security: These features protect the network against wireline attacks and allow different network entities to exchange the signaling information between them securely.
- (iii) User domain security: It provides users with secure access to the mobile stations and mutual authentication.
- (iv) Application domain security: This allows the user applications to exchange data with the network domain securely.
- (v) Visibility and configurability of security: These features allow one to see if security setup is or is not in operation.

2.3.2 SDN Architecture

Software-Defined Networking (SDN) is an emerging technology that will be integral for 5G networks. A layered view of the network functionality is shown in Figure 2.7. In SDN, transfer of data between source and destination is called a flow. Network devices, which are used to carry a flow, such as routers, switches, firewalls, middle boxes or other forwarding devices, are categorized as data plane devices. These devices interact with the SDN controllers, which are running the Network Operating system (NOS). Applications running on top of NOS provides application programming interface (API), which communicates with the data plane devices. The data plane consists of flow forwarding devices, the control plane consists of an SDN controller, and the management plane has the programming interfaces for the network. The main advantage of this architecture is that, if there is a need to modify network policies, then a low-level device-specific configuration is no longer required. Instead, a high-level programming interface can perform such an activity quickly. SDN networks provide two programming interfaces, Northbound and Southbound. The Southbound interface defines the interface for a communication protocol between the forwarding devices and control plane devices. The Northbound interface

Figure 2.7: SDN Architecture

provides a high-level interface for developing applications. The high-level interface abstracts the low-level commands and API of the southbound interface. M Feng et al. [92] has investigated architecture and technical aspects of SDN for wireless networks. The study highlights various open problems in this area. From a security perspective, SDN brings advantages as well as challenges. Centralized control over the network means that it is easier to monitor the network and gather traffic statistics. The SDN controller can run an intrusion detection system to monitor patterns of known attacks. Once a pattern is detected, it is easier to isolate and fix. Such self-healing methods provide improved security as compared to traditional IP-based networks. SDN provides an improved resilience against DoS attacks. The forwarding device can be programmed to report a flow once it exceeds a certain traffic threshold within a specified period. A detailed survey on SDN security has been done in [93]. Security issues in software defined mobile networks

have been explored in [94]. Providing low latency and a secure authentication is the primary challenge in the 5G handover. In a high mobility scenario, providing secure low latency handovers across multiple radio access technologies is challenging. A compromise is required between security and latency. A more secure handover will involve multiple messages passing for authentication, while a low latency handover requires few messages passing.

2.3.3 Authentication and Key Establishment

Authentication and Key Establishment is the most important area of research in LTE-Advanced security, and the specification has laid down the mechanism for these operations. Mutual authentication between the device and network is achieved through the Authentication and Key Agreement (AKA) protocol. During the process, the ciphering key (CK) and the integrity key (IK) are generated, and they are further used to generate the session keys. Figure 2.8 shows EPS-AKA protocol between a user and Mobility Management Entity (MME). The hierarchy of the keys generated during the process is shown in Figure 2.9. For a non-3GPP access, Extensible Authentication Protocol-AKA (EAP-AKA) or Improved EAP-AKA (EAP-AKA') is used. There are various scenarios of connecting to EPC through non-3GPP, but the basic principle is that the user device will authenticate with an Authentication, Authorization, and Accounting (AAA) server before getting the network access. Once an attach request is received from the UE, MME will request for the authentication vector (AV) from the authentication server. The server will verify the user identity from IMSI and generate the AV from the pre-shared key. MME will receive the AV and send an authentication request including AUTH and RAND. UE will verify the authentication request and send a response to MME. MME will verify the response and generate the session keys.

2.3.4 Handover Security

Handover security is specified in LTE/LTE-Advanced specifications. A new key management scheme is introduced and used for secure handover. Initially, the user device

Figure 2.8: EPS AKA

is authenticated to the network using the procedure EPS-AKA. During this procedure, session keys such as K_{eNB} and K_{ASME} are generated. The user device and MME will also generate a Next Hop (NH) parameter from the K_{eNB} and K_{ASME} as shown in the Figure 2.10. Each K_{eNB} and NH has a chaining counter (NCC) associated with it. During the handover procedure, a new session key K'_{eNB} is generated from the currently active K_{eNB} or NH. NCC starts at a value of zero and is reset when NH is refreshed. During the handover procedure, the source eNB will generate the key and send it to the destination eNB. This new key generation will use Physical channel identity (PCI) as well.

Figure 2.9: Key Hierarchy

2.3.5 Related Work

2.3.5.1 Handover Authentication and Key Management Vulnerabilities

Researchers have highlighted several gaps in the 3GPP specifications. Authentication procedure privacy leakage [95], lack of Denial of Service (DoS) protection [95][96], lack of online authentication in some roaming scenarios [97], and vulnerability to Man-in-the-middle attack [98] are some of the main issues with the authentication procedures. Similarly, for the handover procedures, desynchronization attacks and relay attacks have highlighted some vulnerabilities [99]. The handover key management also lacks perfect backward/forward security [100]. Lack of mutual authentication between HeNB and UE leaves the network vulnerable to a range of attacks [101]. Providing a seamless handover and fast authentication remains the main research interest in this area. Several studies have been carried out to address the main security vulnerabilities and gaps. A brief summary of the scheme is presented here. LTE/LTE-Advanced handover authentication and key management schemes can be categorized into four broad categories as described below.

Figure 2.10: Key Derivation

2.3.5.2 Server Based Authentication

In server-based authentication, a server is involved in the authentication process. One of the primary concerns in this approach is that the Authentication Server (AS) becomes the bottleneck and single point of failure. The second main concern with this method is that it involves a lot of message exchange between the user device and server. This results in communication overhead and increases the overall delay. In [102] the author proposes a method to pre-distribute the keys to reducing the delays, and during the handover, a 4-way handshake is required. The trade-off in this scheme is that more resources are needed. In [103], authors investigate secure handover from a QoS perspective. This scheme proposes the use of a Hybrid Interconnection Unit (HIU) as a relay, which will consider the QoS parameter during handover. This scheme will increase the overall overhead and deployment cost with the introduction of HIU. A server-based solution

with pre-authentication and pre-distribution is presented in [104]. This scheme requires a trust relationship with the server. There is also a problem if the connection with the server is lost.

2.3.5.3 Security Context Transfer Authentication Schemes

In the Security Context Transfer (SCT) scheme, the security context is transferred to the next eNB. With the relevant information available at the destination, it is easy to verify the authenticity of the user. The main advantage of this scheme is less traffic between the authentication server and eNB. The overall delay is also shorter compared to the AS approach. This method also requires a trust relationship to be established between the source and target eNB. A direct connection is not always feasible, so if the eNB are on different networks, then first this trust needs to be established. A security context transfer scheme using pre-authentication to achieve fast handovers has been presented in [105]. However, the scheme performs an authentication similar to EPS-AKA with the destination networks which adds some overhead and some of the compatibility, and performance problems are not addressed. Security context transfer schemes have been studied in [106], [107] and [108].

2.3.5.4 Two-Party Authentication Schemes

These schemes are based on a variant of Public Key Infrastructure (PKI). The main concern with this approach is the computational cost and energy consumption. Public key cryptography is more computational intensive, and this adds delay to the authentication process. For mobile devices, power consumption is one of the main performance criteria. Zheng et al. [109] present a hybrid PKI trust authentication scheme that also provides a non-repudiation service. It employs public key infrastructure (PKI) and combines it with the dynamic password scheme. A broadcast protocol system is designed so that there is no need for a certificate. This resolves the problem of multiple trust sources in the network. The cost of public cryptography is the main concern with this approach. Another concern is storage cost, as the scheme is using a broadcast mechanism. An identity-based cryptography (IBC) scheme is presented in [110]. The primary concern

with the approach is the general key escrow problem with IBC-based systems. The introduction of Private Key Generator (PKG) introduces additional complexity in the system. Another concern with this approach is the use of a Pairwise Master Key (PMK). If the private key is compromised, then the adversary can derive the session key.

Several lightweight handover authentication schemes have been presented using chameleon hash functions. The scheme in [111] compromises user anonymity, as it sends its certificate which includes its identity to the BS. The scheme in [112] and [113] cannot ensure untraceability, as the hash function effects on the message sent from the device are similar so they can be linked to the source device. Another study [114], carries out a cryptanalysis of the scheme [113] to show that it cannot achieve perfect forward/backward secrecy as claimed by the authors. An authentication scheme based on bilinear pairing functions is proposed in [115]. It shows that the scheme is vulnerable to a key compromised attack and a proposed fix for this scheme was suggested in [116]. Investigation in [117] presented a successful key compromised attack on the suggested fix to reveal its weakness.

2.3.5.5 Hybrid Authentication Schemes

Hybrid proxy signature generation-based schemes have been proposed in [118] and [119], which also assume a trust relationship between the *eNB*. A proxy signature is generated on behalf of the server, and the user device will be authenticated based on the proxy signature. The main concern with this approach is that a secure channel is not available between the *eNB*, and trust is not established in many of the LTE-Advanced handover scenarios. Computational complexity and knowledge of the public keys are another concern in this approach. The study in [120] is focused towards LTE network handover using a proxy-based signature. An improved proxy signature scheme has been presented in [121], which achieves a uniform handover in LTE. The scheme provides a significant improvement over previous methods when a direct link between *eNB* is not available; however, the communication overheads by this scheme are significantly more when compared with the 3GPP proposed LTE scheme. The vertical Handover scheme [122] provides a general method for vertical handover between heterogeneous networks.

2.3.5.6 5G Handover Security

HetNet handovers have to communicate over legacy networks. Traditional IP network handover methods have a lot of signaling and message passing overhead in the handover, which will not satisfy the 5G latency constraint. There is a need to develop new methods which can meet the latency requirements of a dense HetNet. [123] has presented a new handover scheme for 5G networks. The presented scheme addresses the high-speed railway scenario in 5G networks. It uses gray system theory to make a better handover trigger decision, thus increasing the probability of a successful handover. [124] studies 5G HetNet handover from an energy consumption point of view. [125] investigates 5G HetNet Coordinated Multi-Point (COMP)-based handover. [126] suggests using 5G SDN and providing the handover functionality as a service. A detailed survey of SDN has been done in [127].

There has been research carried out on secure handovers in traditional LTE/LTE-A Networks. These schemes assume a trust relationship between the access points. Hybrid proxy signature generation-based schemes have been proposed in [118] and [119], which also assume a trust relationship between the *eNB*. [121] and [120] are studies focused towards LTE network handover. There has been limited research on the security aspect of 5G handover. So far, the only solution for secure handover in SDN 5G has been presented in [128], which leverages SDN capabilities to provide security mechanisms for handover.

The scheme proposes an authentication and handover module (AHM) to be used in SDN controller. AHM creates a secure context information (SCI) for every user and shares it along their projected mobility path. The relevant APs along the mobility path will prepare the required resources for the handover. The SCI attributes consist of identity, location, moving speed, direction, and physical layer. The number of attributes to be used during authentication will be based on the security level requested. As an example, bank transactions or online purchases can achieve higher levels of security by employing more SCI attributes, whereas online browsing or gaming can use few attributes for a lesser security level. The latency reduction is achieved by using non-cryptographic

techniques. The study also proposes an algorithm for providing privacy to user data such that no link can be established between the information and its owner. In the proposed scheme, the controller will choose multiple paths to transmit different data streams. The number of network paths is decided based on the delay threshold. Once the data is received at the destination, the user can decrypt it using his private key. The decrypted data can be reorganized as a single output stream from multiple input streams. This mechanism ensures the data privacy if any AP has been compromised since only a partial stream of data is available at any AP. The authentication of AP is shifted to off-peak times to reduce the network load. This scheme is vulnerable to a range of attacks such as replay, impersonation, man-in-the-middle, and typing.

Chapter 3

Resource Matching in 4G/5G LTE-Advanced

3.1 Introduction

Resource scheduling is one of the most important RRM techniques that's used to enhance the network's performance. Improving network resource utilization is one of the main goals in a scheduling algorithm. An efficient scheduling mechanism will reduce the under-utilization of the network's resources. However, even at maximum utilization resource scheduling mechanism will offer varying performance results depending on the underlying goal. The underlying goal could be to improve the overall data rate or to reduce delay for a specific time-sensitive traffic. The most widely accepted goal in a cellular network in this regard is to meet the QoS requirements. Another important goal is service differentiation where the scheduling algorithm will provide the network operator with the ability to offer a different level of performance for network traffic, based on their QoS requirements. Thus subscriber differentiation and service differentiation remains desirable features for next generation networks. Carrier aggregation has been specified as the main method to achieve a higher bandwidth. In LTE-Advanced, up to five CC can be combined to increase the overall bandwidth. LTE-Advanced Pro is another step forward toward the goal of 5G communication. In LTE-Advanced Pro, carrier aggregation can support up to 32 carriers. It can be seen that with the evolution of technology, carrier aggregation will remain a fundamental technique to enhance the network performance in 5G. Resource scheduling

over aggregated carriers remains an open area of research. The resource optimization problem in LTE-Advanced has been proved to be an NP-Hard problem [91]. Therefore, heuristic solutions are required for this. In this chapter, resource scheduling over the CA-based LTE-Advanced network is the focus of our research. We propose a Pareto efficient solution using game theory that considers QoS profiles of the users in scheduling decisions.

3.2 Matching Game

The concepts of matching markets originate from the field of economics. The matching theory provides the mathematical framework that models the relationship between matching parties. The matching game can be categorized under cooperative game theory. Cooperative games are games where agents cooperate in the decision-making process. Matching game has many applications, and the topic has been extensively researched. The matching game solution has been applied to various problems such as college admissions process, kidney donor matching, job matching in the hospital, and stable marriage problems. A successful application of the theory provides a stable matching. The most important work in this field was done by Nobel Laureates David Gale and Lloyd Shapley in their paper “College Admissions and the Stability of Marriage”, published in The American Mathematical Monthly in 1962 [129]. This study proposes a solution concept for two-sided matching markets. In the marriage model, there is a set of men and women each with a preference ranking over the other side. The algorithm does a matching between the pairs. The marriage matching solution presented, is proved to be a stable matching. In a stable match, there is no incentive for a matched pair to make a new match, which implies that each agent has the best possible match for it to be stable. The problem can be generalized to any two set of agents which needs to be matched according to a preference list. This problem has attracted researchers in several areas, including mathematics, economics, game theory, computer science. Feng et al. [130] has investigated stable marriage in cognitive femtocell networks. The proposed scheme maximize the sum rate of a full-duplex cognitive femtocell network using a greedy channel

allocation algorithm.

3.3 Problem Formulation

3.3.1 System Model

In LTE-Advanced, the scheduling decisions are made within the eNB. For this problem, we assume there is one eNB in the system supporting CA. CA setup consists of non-contiguous CC, and the user devices include 3G, 4G, and 5G devices. Varying channel conditions for the devices is considered. OFDMA is used in the downlink and SC-FDMA is employed in the uplink.

Let set $\mathcal{U} = \{U_1, U_2, U_3, \dots, U_L\}$ be the devices in the system. Resource block in the system is denoted by $\mathcal{N}$, where $\mathcal{N} = \{1, 2, \dots, N\}$, the maximum number of resource blocks N , is derived from the total system bandwidth as per 3GPP specifications. Modulation and coding schemes (MCS) for the resource blocks will vary depending on the channel condition. The MCS index value is derived from the CQI value using 3GPP specifications. Let's assume that the maximum supported MCS index of all UEs in different RBs be modeled as $\mathcal{L} = \{1, 2, \dots, M\}$. In the system, each device can support a different number of component carriers depending on its capability and if it is within the coverage area of a CC. C_{max} denotes the maximum number of CCs in the system. A 3G device will support only one carrier, whereas 4G and 5G devices can support up to 32 CC. Let $\mathcal{C}$ denote the set of CC in the system and $\mathcal{J}$ is the maximum number of simultaneous carriers supported on any device in $\mathcal{U}$ where:

$$\mathcal{C} = \{C_1, C_2, \dots, C_{MAX}\} \quad (3.1)$$

$$\mathcal{J} = \begin{cases} 1, & \text{if 2.5G, 3G, 3.5G device} \\ C_{MAX}, & \text{if 4G, 5G device} \end{cases} \quad (3.2)$$

Scheduling will be performed in both uplink and downlink. The decision is made on a sub-frame basis. For the uplink scheduling, the resource assignment is done in terms of a group (RBG). If R denotes a group of RB, then the total number of RBGs in the uplink

Table 3.1: Notation Used

Symbol	Description
CC	Component carrier
$\mathcal{U}$	Set of user devices
$\mathcal{N}$	Set of resource blocks in the system
$\mathcal{L}$	Set of maximum supported MCS index of all UE
C_{max}	Maximum number of UE in the system
α	Resource block allocation decision indicator
$\mathcal{B}$	Maximum allowed MCS index on a UE
P_{ue}	Preference list of user devices
P_{rb}	Preference list of resource blocks
μ	Matching function
$\varphi(ue)$	Downlink preference function for UE
$\gamma(rb)$	Downlink preference function for RB
$\partial(rbg)$	Uplink preference function for rbg
$\pi(ue)$	Uplink preference function for ue
Ω	The band support or coverage factor
O_n	The order of RB within a sub-band
Q_c	Channel conditions indicator

system can be calculated as:

$$N_{RBG}^{UL} = \frac{N_{RB}^{UL}}{R} \quad (3.3)$$

In the uplink, the power consumption of user devices remains the main challenge because of which only a limited number of RBG can be assigned to a device. For multi-cluster scheduling, in the uplink, non-adjacent clusters with a minimum distance of one RBG are required. For the downlink system, the power of eNB is used so it is no more a limitation of the scheduling algorithm. Due to the mobility of a user in the system, the channel conditions will vary according to the distance from the eNB. Similarly, the coverage area of each CC is different, so at any particular time, a device can only support the CC within the range. The scheduling algorithm needs to consider these two factors. Another factor to consider will be the change of QoS requirements, as new bearers are formed or the old terminated, the QoS requirements for the user will vary.

3.3.2 Problem Formulation

The primary objective of resource allocation is to obtain a stable matching. The optimization problem is to improve the performance of the system while maintaining the QoS for the user. To improve the performance, we need to maximize the throughput of

the system within the constraints and ensure fairness among the users. Let $\alpha_u^r \in \{0, 1\}$ be the resource block allocation decision indicator, where

$$\alpha_u^r = \begin{cases} 1, & \text{if RB } r \text{ is assigned to UE } u \\ 0, & \text{if not allocated} \end{cases} \quad (3.4)$$

Let $R_u = \sum_{r=1}^{RB_{max}} \alpha_u^r R_u^r$ denote the achievable sum-rate over allocated RB(s) for UE u .

The optimization problem is to maximize

$$Max \sum_{u=1}^{\mathcal{U}_{max}} \sum_{cc=1}^{CC_{max}} \sum_{r=1}^{RB_{max}} \alpha_u^r R_u^r \quad (3.5)$$

Subject to

$$R_{u_l} \geq \mathcal{Q}_{u_l} \forall u_l \in \mathcal{U} \quad (3.6)$$

$$\sum_{u=1}^{\mathcal{U}_{max}} \sum_{cc=1}^{CC_{max}} \sum_{r=1}^{RB_{max}} \alpha_u^r \leq m \quad (3.7)$$

$$\sum_{u=1}^{\mathcal{U}_{max}} \alpha_u^r \leq 1, r \in \mathcal{R} \quad (3.8)$$

$$\mathcal{S}_n = \{\dots, n-1, n, n+1, \dots\} \quad (3.9)$$

$$1 \leq \min\{\mathcal{S}_n\}, \max\{\mathcal{S}_n\} \leq \mathcal{N} \quad (3.10)$$

$$\mathcal{L}_{\mu, \mathcal{RB}} \leq \mathcal{B}_{\mu, \mathcal{RB}} \quad (3.11)$$

CC_{max} is the maximum CC available, and RB_{max} is the maximum RBs available in one CC. $\mathcal{L}$ is the MCS assigned to a UE and $\mathcal{B}$ is the maximum allowed MCS on CC for a UE. The constraints in (3.6) are to ensure the minimum data rate requirement. Constraint (3.7) shows that the system has m RB. Constraint (3.8) states that each RB can be assigned to at most one user. MCS constraint is applied in (3.11), ensuring that the assigned MCS to a UE is less than the maximum supported MCS in each of the assigned RBs. The constraints in (3.9) and (3.10) are the adjacency constraints for the uplink, where n return the indices of the RBs in $\mathcal{S}_n$. As the problem has been proved to be NP-hard, an exhaustive search to find optimal matching would be impractical. We propose a heuristic solution which can achieve a Pareto efficient matching.

3.4 Matching Game Solution

First, we will model a matching game and then present a heuristic solution.

3.4.1 Matching Game Model

In game theory, the agents involved in the interaction are called players. In a 5G wireless network, the user devices and the base station will form a set of players. In our model, there is one base station involved, but many user devices, so it would seem that this is a one-to-many matching. However, if we model the resource blocks as players, then it becomes a many-to-many matching. Our proposed system model consists of a set of devices $\mathcal{U}$ such that for all $u \in \mathcal{U}$, u is free and has a preference list P_{ue} containing each RB $rb \in \mathcal{N}$. A set of resource blocks RB such that for all $rb \in \mathcal{N}$, rb is free and has a preference list P_{rb} containing each UE $u \in \mathcal{U}$. In a matching game, players can take several actions which offer a payoff. In a matching game for scheduling, the action could be a request to get some scheduling resource, and the payoff would be a resource block offering a certain data rate. The payoffs are defined in terms of utility functions based on the actions. Once the agents, actions, and payoffs are defined, the system will try to reach a state of equilibrium. In the case of the matching game, an equilibrium is gained once a stable matching is found. There is no further incentive for any agent to gain more payoff after equilibrium, ensuring the system stability. A definition of matching market and matching game for the system is given below.

Definition I: A matching market for downlink can be defined in the form (UE, RB^{dl}, P) where

$$UE = \{UE_i, UE_{i+1}, UE_{i+2}, UE_{i+3}, \dots, UE_{i+m}\} \quad (3.12)$$

$$RB^{dl} = \{RB_j^{dl}, RB_{j+1}^{dl}, RB_{j+2}^{dl}, \dots, RB_{j+N}^{dl}\} \quad (3.13)$$

$$UE \cap RB = \emptyset \quad (3.14)$$

User devices and resource blocks are two set of agents in the game model. The preference of UE for the RB is based on a set of preference defined by the preference

function. Let P be the list of preference then P_{ue} is the preference of UE and P_{rb} defines the preference list of resource blocks. It can be defined as:

$$P_{ue}^{dl} = \{\varphi(ue), \varphi(ue^2), \varphi(ue^3), \dots, \varphi(ue^m)\} \quad (3.15)$$

$$P_{rb}^{dl} = \{\gamma(rb^1), \gamma(rb^2), \gamma(rb^3), \dots, \gamma(rb^N)\} \quad (3.16)$$

where agent $\varphi(ue)$ and $\gamma(rb)$ are the preference functions of UE and RB.

Definition II: A matching for downlink is a function:

$$\mu : RB \cup UE \rightarrow RB \cup UE, \text{ such that} \quad (3.17)$$

$$\mu(ue) = rb \leftrightarrow \mu(rb) = ue \text{ for all } rb \in RB, ue \in UE \quad (3.18)$$

$$\mu(rb) \notin UE \rightarrow \mu(rb) = rb \text{ for all } rb \in RB \quad (3.19)$$

$$\mu(ue) \notin RB \rightarrow \mu(ue) = ue \text{ for all } ue \in UE \quad (3.20)$$

where μ is the matching function. If matching a UE results in an RB, the matching of that RB will result in same UE. If there is no match for a UE, then it is matched to itself and same holds to an RB. Let ϑ be a utility function of (ue, rb) belonging to $RB \times UE$. Then, a matching game can be expressed as (RB, UE, ϑ) .

Definition III: A matching market for an uplink can be defined in the form (UE, RBG^{ul}, P) where

$$UE = \{UE_i, UE_{i+1}, UE_{i+2}, UE_{i+3}, \dots, UE_{i+m}\} \quad (3.21)$$

$$RBG^{ul} = \{RBG_j^{ul}, RBG_{j+1}^{ul}, RBG_{j+2}^{ul}, \dots, RBG_{j+N}^{ul}\} \quad (3.22)$$

$$UE \cap RBG^{ul} = \emptyset \quad (3.23)$$

UE contains all the UE in the system. RBG is the second set of game players. For each RB, eNB holds its preference list of the UEs. Let P be the list of preference agents, P_{ue}^{ul} be the preference of agent UE , and P_{rbg}^{ul} be the preference list of agent RBG. The preference list for the uplink can be described as:

$$P_{ue}^{ul} = \{\pi(ue), \pi(ue^2), \pi(ue^3), \dots, \pi(ue^m)\} \quad (3.24)$$

$$P_{rbg}^{ul} = \{\partial(rbg), \partial(rbg^2), \partial(rbg^3), \dots, \partial(rbg^N)\} \quad (3.25)$$

where agents $\partial(rbg)$ and $\pi(ue)$ are the preference functions of an agent.

Definition IV: A matching for uplink is a function:

$$\mu : RBG \cup UE \rightarrow RBG \cup UE, \text{ such that} \quad (3.26)$$

$$\mu(ue) = rbg \leftrightarrow \mu(rbg) = ue \text{ for all } rbg \in RBG, ue \in UE \quad (3.27)$$

$$\mu(rbg) \notin UE \rightarrow \mu(rbg) = rbg \text{ for all } rbg \in RBG \quad (3.28)$$

$$\mu(ue) \notin RBG \rightarrow \mu(ue) = ue \text{ for all } ue \in UE \quad (3.29)$$

The outcome of the matching process is a formation of pair of matches between the agents on two sides. If a match is not found, then the player is considered to be matched to itself. Let $\vartheta(ue, rbg)$ be a utility function of (ue, rbg) belonging to $RBG \times UE$. Then, a matching game can be expressed as (RBG, UE, ϑ) .

3.4.2 Heuristic Solution Using Matching Game

A heuristic solution to the matching game problem will be to find a stable matching with a set of preference lists. In matching markets, a matching game is defined by two sets of agent lists which are matched with each other. In classic matching games, the number of players for matching is the same, so the problem becomes a direct matching problem where a stable solution is reached once each agent is matched. In 5G scheduling, the number of resource blocks and the number of scheduled users is not the same. Each user device would be assigned a varying number of blocks depending on its demand and QoS requirement. We will use a modified variant of the classical matching market to solve this problem. A lot of research has been carried out on various variants of the matching markets problem. An extensive survey of the type of matchings has been summarized in [131]. Roth proposed a solution for a two-sided matching market in [132]. The proposed algorithm provides a solution for the matching of two-sided markets and results in a Pareto optimal matching.

In LTE-Advanced 5G network, the user devices will be a mixed set of 3G, 4G, and 5G devices. With CA, each device will support a different number of CC. CA is not supported on 3G devices. 4G devices will support 4 or 8 CC aggregations, while 5G

will support an even higher number of CC aggregations. In addition to that, each CC will have a different network coverage, so all devices will not have access to all CCs during scheduling. This adds complexity to the scheduling algorithm since it needs to be aware of which band is supported for a particular device. In our proposed algorithm, the resource blocks are taken from a big pool, preference list will decide the selection of the best RB from the pool. If a CC is not currently supported by the device, then the band support factor would make the payoff less on the said RB. If the payoff is less or none, then it will list low in the preference list and will not be selected. If the same payoff is achievable on multiple RBs, then we will take the current load of CC into account during the scheduling decision. In our solution, resource block matching and their allocation have been combined into a single comprehensive algorithm.

3.4.3 Matching Game

For a stable matching, a match should be established such that there is no incentive to increase the overall system output by taking any further action. As a first, the preferences of the agents will be clearly defined. In our game model, UE will prefer high data rates, for this they will list down the RB in order of the data rate they can achieve on those RBs. It will depend on the CQI over a particular RB. In LTE-Advanced, a UE regularly reports its CQI to the eNB. For the downlink, the system preferences of $UE\ i$ over $RB\ j$ can be defined by the following equation:

$$U_{i,j}^{dl} = (C_i + Q_c) \times \Omega \quad (3.30)$$

$$U_{i,j}^{ul} = (O_n + C_i + Q_c) \times \Omega \quad (3.31)$$

where Ω is the band support or coverage factor $\Omega \in \{0,1\}$. If a device is not within the range of a CC or does not support CA on a particular CC, then this will zero for all the RB on that band. This way, the unsupported band would be listed lower in the preference list of a user device. C_i is a factor that can give control over carrier selection to the scheduler. A higher value would mean that $UE\ i$ prefers the CC of $RB\ j$. Q_c is a channel conditions indicator computed from the CQI value reported to eNB by the

device. According to 3GPP specifications, a group of RB forms a sub-band, the size of which is configurable by the network operator. CQI is reported on a sub-band basis where each RB within the sub-band has the same CQI. Selection of an RB with a sub-band needs to be considered by the scheduling algorithm. We define O_n as the order of RB within a sub-band which will provide control over the selection of RB . Earlier research has concluded that localized allocation in a sub-band is preferred in the uplink due to the power constraints. By using O_n to assign a higher value to the edge RB , we can ensure sequential localized scheduling. The preference list created from the above function will be sorted according to the preferences. However, if there is a tie among two agents, then we will make a random pick. With strict preference defined, the matching algorithm ensures stable and optimal matching.

The procedure will be repeated to create a preference list for the RBs in eNB. There are two main criteria for preference list creation at eNB QoS and fairness. We will use QoS as the main criteria for preferences. 3GPP specifications specify bearer QoS profiles. We will use that setup information for scheduling. The preference function V_i of RB i for UE j can be defined as

$$V_{i,j} = (QCI_j - \beta) \quad (3.32)$$

Where QCI j is the QoS profile of UE j flow. UE can have different flows with varying QoS requirements. β is a preference factor used to control the allocation preference of a device. If a device can be scheduled over multiple CC, then it will have a lower preference value for the CC. For RBs the utility function would be to minimize value of $V_{i,j}$.

An optimal matching is one that can maximize/minimize the corresponding utility function for matching μ (Definition II).

$$\text{Maximize } \sum_{i,j} U_{i,j} \quad (3.33)$$

$$\text{Minimize } \sum_{i,j} V_{i,j} \quad (3.34)$$

The matching game algorithm will start by listing the preference of the agents. Once the lists are formed, they will sort according to the preference. In the first iteration, UE

Algorithm 1: Matching Game algorithm: Resource block allocation

Input : A set of devices $\mathcal{U}$ such that for all $u \in \mathcal{U}$, u is free and has a preference list $\mathcal{P}_u^x$ containing each RB $rb \in \mathcal{N}$, where $x \in \{ul, dl\}$
 A set of resource blocks $\mathcal{N}$ such that for all $r \in \mathcal{N}$, rb is free and has a preference list $\mathcal{P}_r$ containing each ue $u \in \mathcal{U}$

Output: A stable matching μ between $\mathcal{U}$ and $\mathcal{N}$, $\forall u \in \mathcal{U}, r \in \mathcal{N}$

- 1 **Initialization;**
- 2 Set $V_{u,r,c,l} = 0, U_{u,r,c,l}^x = 0 \forall c \in \mathcal{C}, l \in \mathcal{L}$;
 // Phase 1
- 3 **while** $\exists u$ with $\sum_{r=1}^N \alpha_u^r < m$ **or** $\exists r$ with $\sum_{u=1}^L \alpha_u^r = 0$ **and** $\mathcal{P}_u \neq \emptyset \forall u \in \mathcal{U}, r \in \mathcal{N}$ **do**
- 4 $U_{r,c,l}^x \leftarrow$ from eq (3.30) and eq(3.31);
- 5 Set $S_{bm}^u \leftarrow$ best matching rb $r \in \mathcal{R}$ from $\mathcal{P}_u$ which gives highest utility function $U_{r,c,l}$;
- 6 **if** $\alpha_u^r = 0$ **then**
- 7 $\mathcal{S}_r \leftarrow \mathcal{S}_r \cup S_{bm}^u$;
- 8 $\mathcal{P}_u \leftarrow \mathcal{P}_u \setminus \{\pi(u), \varphi(u)\}$;
- 9 **end**
- 10 **end**
- 11 **while** $\exists u$ with $\sum_{r=1}^N \alpha_u^r = 0$ **and** $\mathcal{S}_r \neq \emptyset \forall u \in \mathcal{U}, r \in \mathcal{N}$ **do**
- 12 **if** $\mathcal{S}_r \neq \emptyset$ **then**
- 13 Set $S_{bm}^r \leftarrow$ best matching ue $u \in \mathcal{U}$ from $\mathcal{S}_r$ based on $\mathcal{P}_r$ which gives lowest $V_{r,c,l}$;
- 14 Set $\alpha_u^r = 1$;
- 15 pair (u,r) ;
- 16 **foreach** *successor request* $\hat{S}_{bm}^r$ **do**
- 17 $\mathcal{S}_r \leftarrow \mathcal{S}_r \setminus \hat{S}_{bm}^r$;
- 18 **end**
- 19 **end**
- 20 **end**

will request for the RBs. Once all the requests are sent, RB will perform a selection of the request from the available request list. At the end of the selection, each RB which was made any offer, will have a matching pair formed. If an RB gets multiple requests, it will select one request and reject the remaining. For the rejected requests, they will try to form a new pair in the next iteration. The process will continue until we have a stable matching. It can be seen that at each iteration the best proposal is selected, and

Algorithm 2: Matching Game algorithm: Continued

```

// Phase 2 upto Phase K.
1 foreach  $u$  with  $\sum_{r=1}^N \alpha_u^r < m$  and  $\mathcal{P}_r \neq 0$  do
2    $\mathcal{S}_r \leftarrow \mathcal{S}_r \cup S_{bm}^u$ ;
3    $\mathcal{P}_u \leftarrow \mathcal{P}_u \setminus \{\pi(u), \varphi(u)\}$  ;
4    $\mathcal{P}_r \leftarrow \mathcal{P}_r \setminus \{\gamma(r), \partial(r)\}$  ;
5 end
// Matching
6 foreach  $r$  with  $\sum_{u=1}^L \alpha_u^r = 0$  and  $\mathcal{P}_r \neq 0$  do
7   if  $\mathcal{S}_r \neq \emptyset$  then
8     select best request based on eq (3.32);
9     Set  $\alpha_u^r = 1$ ;
10    pair  $(u, r)$ ;
11    foreach successor request  $\hat{S}_{bm}^r$  do
12       $\mathcal{S}_r \leftarrow \mathcal{S}_r \setminus \hat{S}_{bm}^r$ ;
13    end
14  end
15 end

```

for a rejected proposal it can be logically inferred that a better pair was created. The rejection would not have occurred if it was the best match from the system performance perspective. Due to the changing conditions of the wireless channel and changing nature of network traffic, the QoS and CQI values will be changing during the execution of the protocols. This means that the preference lists need to be refreshed to match the network conditions.

3.5 Analysis of Matching Game

3.5.1 Proof of Stability

The system can be proved to be stable if there are no blocking pairs in the matching. If the eNB ε prefers $\mathcal{UE}_1$ to $\mathcal{UE}_2$, then we can denote this as

$$UE_1 >_{\varepsilon} UE_2 \quad (3.35)$$

Definition V A matching i is blocked by an individual UE ; if UE prefers being single to being matched with i . i.e.

$$UE >_{ue} i(ue) \quad (3.36)$$

A matching i is blocked by a pair of agents (ue,rb) if they each prefer each other to the partner they receive at i , i.e.

$$RB >_{ue} i(UE) \quad (3.37)$$

and

$$UE >_{rb} i(RB) \quad (3.38)$$

Definition VI: An assignment of a resource block will be called unstable if there are two $\mathcal{UE}$ α and β who are assigned to $\mathcal{RB}$ A and B , although β prefers A to B and A prefers β to α .

Proposition 1: A stable matching outcome can be found using the algorithm.

Proof: The proof of the proposition can be done by observing a few facts. The algorithm always stops as no $\mathcal{UE}$ proposes twice to the same $\mathcal{RB}$. No $\mathcal{UE}$ ever proposes to an unacceptable $\mathcal{RB}$, and no $\mathcal{RB}$ accepts the offer of an unacceptable $\mathcal{UE}$. If some $\mathcal{UE}_i$ prefers to be matched to an RB_j other than the current assigned $\mathcal{RB}_k$, then according to the algorithm, the UE_i must have already proposed to that $\mathcal{RB}_j$ and the $\mathcal{RB}_j$ must have rejected $\mathcal{UE}_i$, which means that $\mathcal{RB}_j$ prefers a different $\mathcal{UE}_m$. Hence, they cannot form a blocking pair according to the definition of the blocking pair. If there is no blocking pair, from the above definition, it can be inferred that the matching is stable.

3.5.2 Proof of Uniqueness

A unique stable matching can be obtained if there are sufficient resource blocks ($N > U_L$).

Proposition 2: Consider two preference profiles $\mathcal{P}_u$ and $\mathcal{P}_r$. If the preference profiles satisfy the following conditions

$$\forall u_i \in \mathcal{U} : u_i >_{r_i} u_j \quad \forall j > i \quad (3.39)$$

$$\forall r_i \in \mathcal{R} : r_i >_{u_i} r_j \quad \forall j > i \quad (3.40)$$

$$\mu'(r_i) = u_i \forall i \in \{1, 2, \dots, N/2\} \quad (3.41)$$

then μ' is a unique stable matching.

Proof: Let μ be a stable matching which is different from μ' for some i , $\mu(r_i) = u_k$, $k \neq i$. As μ satisfies the stable matching definition, it can be followed that there must exists some $j \neq k$ such that matching $\mu(u_j) = r_l$, $l \neq j$. Let's assume ξ and ζ such that:

$$\xi = \min\{i : \mu(r_i) = u_k, k \neq i\} \quad (3.42)$$

$$\zeta = \min\{j : \mu(u_j) = r_l, l \neq j\} \quad (3.43)$$

Since $\mu'(r_\xi) = u_\zeta$, it follows that $\xi = \zeta$.

Then $\mu(r_\xi) = u_k$ implies $\xi < k$ and $\mu(u_\xi) = r_l$ implies $\xi < l$. Given (3.42) (3.43), it follows that

$$u_\xi >_{r_\xi} u_k \quad (3.44)$$

$$r_\xi >_{u_\xi} r_l \quad (3.45)$$

As a result, μ is not a stable matching as r_ξ and u_ξ makes a blocking pair which contradicts the original assumption that a stable matching always exists.

3.5.3 Pareto Optimal Proof

Proposition 2: A UE-optimal matching outcome is obtained from the algorithm.

Definition VII: A stable matching outcome is called optimal if every agent is at least as well off under it, as under any other stable outcome.

Pareto Efficient A matching is Pareto efficient if there is no matching v such that $v(ue)$ is preferred over $\mu(ue)$ for an individual ue , thus, stability implies Pareto efficiency. A stable matching to such a game would be Pareto efficient.

Proof: The proposition can be proved by the fact that no UE is ever rejected by an RB who could be matched at a stable matching. To further prove, let's assume Φ is the stable outcome we get by using the algorithm. Let γ be the stable outcome which is better than Φ . If the outcome is better, it means that there exists a UE_i who is matched to RB_j in γ and RB_j is matched to UE_k in Φ . This implies that Φ is blocked by a pair

(UE_i, RB_j) . It contradicts the initial assumption that Φ is stable from the definition of a blocking pair. Therefore, there is no stable outcome γ better than Φ , thus Φ is optimal.

On the basis of these theorems, an optimal stable matching can be found using the matching game model proposed by Matching game (MG). It can be seen that Resource allocation using such a game model will have a stable and optimal outcome.

3.5.4 Termination and Complexity

In each iteration of the Matching Game algorithm, each u will send one proposal. The preference list will be updated at the end of the step to remove the proposed r from the list. This way no r is proposed twice; this holds $\forall u \in \mathcal{U}$ and $r \in \mathcal{N}$. The total number of requests cannot exceed $L \times N$. This guarantees the termination. For each u , the complexity to build the preference profile using any standard sorting algorithm is $\mathcal{O}(N \log N)$. Similarly, the complexity to build the preference profile for rb will be $\mathcal{O}(L \log L)$. Finding a stable matching will take $\mathcal{O}(n^2)$ where n is the number of pairs.

3.5.5 Simulation Result

For simulation, we will perform scheduling within a single eNB. Summary of the simulation parameter is defined in Table 3.2. The uplink and downlink bandwidth will be divided into j resource blocks which will be allocated to the user devices. We have assumed an infinitely backlogged traffic model so that eNB will be able to schedule all RB in each slot. The channel conditions and QoS of the user will be varying randomly during simulation. We have used LTE-Advanced specifications to model the system close to the real environment. Three deployment scenario are used random, center and edge. The channel quality range is defined over these placements. CQI (channel quality indicator) is used to determine the quality of the channel. From LTE specifications, MCS index (Modulation and Coding Scheme) for a resource block can be determined from CQI value. In the simulation due to mobility, we have modeled changing channel conditions. Once a user enters the system, it is assigned a random CQI based on location (center or edge). The channel condition will be improving or degrading based on the last CQI value. The

channel quality will be changing over the duration of the simulation. The matching game will generate a new preference list according to the new values. To simulate CA, we have defined 4 CC using both the contiguous and non-contiguous model. The user devices will be selected from 3G, 4G, and 5G. We will be choosing different ratios of the devices to analyze the algorithm. 4G and 5G devices will support CA, whereas 3G devices will not.

For distribution of devices in the coverage area of the eNB, we have modeled three deployment strategies. First is the random deployment, in this the user devices are randomly distributed across the coverage area of the network. The channel quality is best in the center of a cell. To analyze the performance of an algorithm under good channel conditions, we use a center deployment method for the second scenario. For the last deployment scenario, we use a cell edge distribution. The channel quality is usually worse at the edge of a cell. PF is the most widely used and accepted algorithm for scheduling [133] [134] [135], so we will be using this for comparison study. PF provides a compromise between throughput and user fairness. The main aim of PF scheduling is to maintain a balance between the two goals of throughput and fairness. It does so by taking ratio of potential data rate to its historic average data rate for any allocation.

The result of our simulation shows that MG is able to achieve an optimal and stable matching. We perform a comparison of the average cell throughput in random, center and edge scenario. Due to better channel conditions at the center of the cell, center deployment scenario is expected to have best average throughput. As the channel conditions vary, the scheduling algorithm can reassign the RB based on new CQI values. The results in Figure 3.1 shows that MG can achieve a better throughput compared to the PF. At the start when LTE-Advanced devices are not present in the network, the performance of the two algorithms is almost the same. This is because we are not taking advantage of CA as it is not supported by the LTE devices in the network. Once we capitalize on the CA, we can see the performance difference between the two algorithms. Results of the center deployment method are shown in Figure 3.2. A similar conclusion can be established that MG outperforms PF with CA. Results for edge deployment method are shown in Figure 3.3. Average throughput achieved by MG is better than

Table 3.2: Simulation Parameters

Parameters	Values
System bandwidth DL	80Mhz, 4 <i>CC</i>
System bandwidth UL	80Mhz, 4 <i>CC</i>
Number of <i>RBG</i>	100 (UL)
Subcarriers per <i>RB</i>	12
Number of bands in DL	2 Bands
Number of <i>RB</i>	400 (DL)
Users	Mix of 2.5G/3G/4G/5G devices
Transmission time interval	1 ms
Traffic model	Infinitely backlogged
Admission control constraint	<i>UE</i> accepted if QoS is supported
<i>RB</i> size	180 kHz
Sub carrier size	15 kHz
CA type	Non-contagious CA
QoS support	QCI (1-15)
Channel conditions	CQI (1-15)
Number of <i>UE</i> in the system	40,50,60,70,80,90,100

PF. From the results it can be seen that overall throughput is increasing as the number of LTE-Advanced devices are increasing in the network. This is due to CA support on LTE-Advanced devices. At the start of MG iteration, a UE will propose to an RB. For a UE if the candidate pool increases, then the chance of getting a better RB will increase as well. LTE-Advanced devices will end up with a higher data rate RB as they can choose from multiple CCs. With MG, the scheduling algorithm is able to modify the preference list so it can adjust to the changing network conditions. Uplink throughput comparison for the random scenario shows a similar trend in Figure 3.4. For the uplink, the best average throughput is achieved by the center deployment scenario as shown in Figure 3.5. For the uplink edge scenario, Figure 3.6 indicates that MG outperforms PF for edge users. The data rate in the uplink is less when compared with the downlink. The uplink assignment is limited by the power of the device. However, another factor is the localized

Figure 3.1: Downlink Throughput with Random Deployment

assignment of RBs in the uplink.

Jain's Index [136] is widely accepted criteria for evaluating fairness among different parties.

$$Fairness = \frac{(\sum x_i)^2}{(n \sum x_i^2)} \quad (3.46)$$

where x_i is the average transmission rate for i . Fairness is normalized on a scale of 0 to 1, where 1 would mean fair system. For a fair distribution, the index should return a value close to one. For the purpose of fairness comparison, the ratio of devices supporting CA and without CA is kept equal and constant. Fairness analysis for random deployment is shown in Figure 3.7, for edge deployment in Figure 3.8, and for center deployment in 3.9. The fairness analysis is done on the matching game downlink (MG-D) and uplink (MG-U). For the PF, both downlink (PF-D) and uplink (PF-U) algorithms are evaluated as well. Random, Edge, and Center are the three deployment strategies used in this simulation. From the fairness results, we can see that the fairness of MG and PF is of the same order. It can conclude from the results that MG provides better average throughput and similar fairness to the users in the network.

Figure 3.2: Downlink Throughput with Center Deployment

Figure 3.3: Downlink Throughput with Edge Deployment

Figure 3.4: Uplink Throughput with Random Deployment

Figure 3.5: Uplink Throughput with Center Deployment

Figure 3.6: Uplink Throughput with Edge Deployment

Figure 3.7: Fairness Evaluation with Random Deployment

Figure 3.8: Fairness Evaluation with Edge Deployment

Figure 3.9: Fairness Evaluation with Center Deployment

3.6 Conclusion

In this chapter, we have studied the resource allocation problem for 4G/5G LTE-Advanced networks. We use game theory to model the resource allocation problem as a matching game. The optimization problem is to maximize the performance of the system under QoS constraints. The matching game is able to provide a sub-optimal matching which is stable. We first prove the stability and Pareto optimality of the proposed solution. Next, we perform a comparison with PF scheme and show that the MG outperform PF in terms of average throughput. Next, we look into the fairness and prove that MG offers a similar level of fairness as PF.

We claim the matching to be UE-Pareto optimal which implies that to improve further a trade-off will be required. An improvement can be gained at the expense of reducing the performance of another user. The claim is appropriate for the matching done based on preference list which was created. With the given set of agents and preferences, the matching is optimal for the agent who proposes first, so this is UE optimal. If it is UE-optimal, conversely it will not be optimal for the other set of agents. An RB-optimal matching can be obtained by allowing RB to propose first, such a matching would not be optimal for UE. There has been some research carried out on balanced matchings. Main categories of these optimization criteria are Egalitarian stable matching, Minimum-regret stable matching, Median stable matching. Our proposed scheme is not considering other QoS parameters such a delay, latency. The framework can be expanded by using a different utility function for creating preference list. Proportional fair criteria can be used to create preference list which tries to balance the fairness among users.

Our proposed scheme is limited to a single eNB. With the introduction of CoMP technologies, the edge users in the network are able to communicate with multiple base stations. In order to provide a fair resource allocation in such a scenario, cooperation is required between the two base stations.

Chapter 4

Secure Handover in 5G

4.1 Introduction and Background

Heterogeneous networks (HetNet) are critical towards low-cost, high-capacity 5G communication network deployment. The growth in data rate could only be met by making use of dense HetNet. Stringent latency requirements bring new challenges in secure handover and authentication in 5G HetNets. The frequency of handovers increases the challenge due to the dense nature of networks. SDN will play a major role in 5G networks. Centralized control over the network and the ability to manage the network with high-level application programming interface (API) makes SDN a desirable technology in 5G. One of the main advantages of SDN is the deployment of policies on devices from the management layer. A low-level configuration of each device is not required anymore, with the help of SDN controller the network API's can achieve this task easily. Efficient routing path can be created dynamically based on changing network traffic patterns. From a security perspective, SDN architecture could be leveraged to deploy security procedures more efficiently. Our contribution is to provide a method, to perform secure handover authentication and key management using SDN, which can meet the requirements of a 5G network.

Mobile data has been growing at fast rate. With the advent of new technologies, this trend is expected to continue. A recent survey [137] concluded that the growth rate is projected to continue at 53% compound annual rate till 2020 and the monthly mobile traffic

generated will reach 30 Exabyte by that time. 5G networks are expected to cope with the data. In addition to the data rate support, next generation networks are expected to be reliable, efficient, and secure. Support of Heterogeneous networks (HetNet) will be a cornerstone in pursuing the goal of support for a higher data rate in 5G networks. In HetNets, a small cell such as microcell, femtocell, picocell and wifi access points can be used to offload a great share of the network traffic load. Network operator's operating expense and capital expenditure will be reduced by supporting HetNets. The study in [137] highlights that 50% of the monthly mobile data traffic is being offloaded through femtocells or Wifi. In 5G networks, HetNet will be increasingly used to complement the coverage and capacity of the conventional cellular network. Secure handovers, under the delay requirements, are one of the main challenges for a 5G HetNet.

Some of the main features expected from 5G networks are to provide an uninterrupted connectivity, high-speed connection, and low latency. The industry standard for the 5G networks are still in infancy stage, but the requirements and expectation for the 5G network have been laid down. Devices are expected to connect ubiquitously. Extremely low latency of 1 ms is expected from 5G [138][139][140]. Support for data rates in the order of 10-100 Gb per second is expected. Support for data volume 10Tb/s/Km², reliability of 99.999%, connections up to 1M terminal/km² and service deployment time of 90 minutes is expected from 5G [141]. A detailed survey of the 5G network has been presented in [142]. A multi-tiered architecture has been adopted for 5G networks where a macro base station covers many small cells inside it. The small cell will complement the coverage and capacity of the network. 5G HetNet will support the integration of different radio access technologies such as 3G, 4G, LTE, WiMAX, LTE-Unlicensed, LTE-Advanced, mm-Wave Frequencies and Device to Device (D2D) communications.

SDN will be one of the main technologies in 5G based LTE-Advanced networks. Low cost and ease of scalability are leading a shift towards SDN-based architecture. From a security perspective, SDN brings advantages as well as challenges. Centralized control over the network means that it will be easier to monitor the network and gather traffic statistics. SDN controller can run intrusion detection system to monitor for patterns of

known attacks. Once a pattern is detected it will be easier to isolate and fix it. Such self-healing methods provide improved security as compared to traditional IP-based networks. SDN provides an improved resilience against denial-of-service attack (DoS attack). The forwarding device can be programmed to report a flow once it exceeds a certain traffic threshold within a period. A detailed survey on SDN security has been done in [93].

When a mobile device moves from the range of one base station to another base station, a handover takes place. First, the authentication process will occur where the user is identified and verified; next key establishment will take place. At the end of key establishment process, both parties will have a shared key to communicate. The main entities involved are user equipment (UE), a base station (BS)/ eNodeB (eNB) and authentication servers such as AAA or HSS. For a secure handover, cryptographic messages are passed to establish new key between the destination BS and user equipment. Low latency requirements in 5G bring a challenge to perform this procedure within the latency requirement. A detailed survey of existing methods has been provided in chapter 2. The existing methods of secure handover are unable to meet the latency requirements of 5G networks. There is a lack of a direct link in HetNet, so a secure communication channel is not available between source and destination AP. So far the only solution for secure handover in SDN 5G has been presented in [128], which can meet the latency requirements but has several weaknesses. In this section, we will review the proposed scheme and its weakness.

4.1.1 Review of AHM Scheme

Duan et al. [128] leverage SDN capabilities to provide a security mechanism for handover. The scheme proposes an authentication and handover module (AHM) to be used in SDN controller. AHM creates a secure context information (SCI) for every user and shares it along the projected mobility path of the user. The relevant Access Point (AP) along the mobility path will prepare the required resources for the handover. The SCI attributes consist of identity, location, moving speed, direction, and physical layer attributes. The number of attributes to be used during authentication will be based on the security level

requested. As an example, bank transaction or online purchase can achieve a higher level of security by employing more SCI attributes whereas online browsing or gaming can use few attributes for lesser security level. The latency reduction is achieved by using non-cryptographic techniques. The proposed method in [128] uses an SDN-enabled network to reduce the latency. The algorithm simplifies the handover and reduces authentication procedure complexity at the expense of security. We explore the study to find that it is vulnerable to a range of attacks.

- User anonymity and trace-ability: Due to the lack of encryption the identity of a user is exposed during the authentication, thus compromising the privacy. In addition, the roaming path and current location is also compromised as the information is sent in plain.
- Replay attack: Attacker may be able to record the message and replay to a destination server. As long as the correct SCI is passed, the AP will be able to authenticate the user. The freshness of an authentication request is implicitly assumed by using SCI. Recording and replaying SCI message will authenticate the attacker.
- Lack of Revocation: There are no revocation procedures, once the SCI is available at an access point then an attacker can request handover and get authenticated access to the network.
- Guessing Attack: Different security levels have been defined based on the application used. The simulation example presented in the paper uses the relative distance from the AP and moving direction as SCI. Given a small cell size in HetNet, it is possible to do a brute force attack and guess the approximate values of these two parameters.
- Impersonation attack: There is no ability to detect re-registration with the same identity. If an attacker is able to derive or capture SCI, then it can impersonate as the user.

- **Vulnerability in SCI update:** The proposed algorithm allows SCI to be updated during handover phase without the involvement of AHM. Invalid values of SCI can be updated making the actual user unable to authenticate.
- **Man-in-the-Middle Attack:** In this attack, an attacker may try to act as a valid user or server. Handover request originates from destination AP to current AP based on SCI. SCI recorded during the update phase could be used in the new request. Authentication with AHM is not required to make such an attack if SCI can be gathered by other means.

There are several flaws in the existing scheme. We propose a new scheme for authenticated handover.

4.1.2 Our Contribution

A secure handover in 5G HetNet which can meet the latency requirements is an open issue. The only solution for secure handover in SDN 5G has been presented in [128]. We explore to find that it is vulnerable to a range of attacks. We propose an SDN Authentication and Handover scheme (SAH) which takes advantage of SDN architecture to reduce the latency of a secure HetNet handover. To the best of our knowledge, this is the first piece of work which provides a secure HetNet handover using SDN. We complement the scheme presented in [128] by using cryptographic techniques in order to prevent malicious attacks. SAH can meet 5G latency requirements. SAH will create a secure channel between source and destination access points. The scheme achieves mutual authentication between entities, and secrecy of the keys established is verified using formal methods.

4.2 SDN Authentication and Handover Scheme

An authentication scheme is expected to provide mutual authentication of the users. In addition, security properties such as integrity, non-repudiation, confidentiality, privacy are expected. A key establishment scheme is expected to generate session keys between

the communicating parties. Perfect forward and backward security are expected such that a loss of a private key will not impact future and past sessions. For the design of any security scheme, the attack vector needs to be defined first. We have used Dolev-Yao threat model [143]. In this model, the attacker can hear, interpret and gather information over the channel. It is assumed that public key of every user is available to the attacker. The attacker can start many sessions and can do concurrent execution in the session, the information available in one session can be concurrently used in another session. In our scheme, we will be using a cryptographic hash function. A collision-resistant one-way hash function can be defined as an algorithm which takes an input string $x \in \{0, 1\}^n$ and outputs a string $y \in \{0, 1\}^n$ of length n [144]. Let x and x' be two random inputs for hash function then the advantage of an adversary can be defined as $Pr[(x, x') : x \neq x', Hash(x) = Hash(x')]$. A hash function is called collision resistant if the chance of collision $\leq \varepsilon$, for a sufficiently small $\varepsilon > 0$.

4.2.1 Handover Scheme

In this section, we propose a handover authentication scheme for a 5G HetNet. For a HetNet handover scenario, we assume that the *UE* is already authenticated within a macro-cell so that the initial registration and initial authentication has been taken care off. The *UE* moves into the coverage area of the neighboring base station and the handover has to take place. The proposed algorithm can be broken into two phases, phase 1 is a pre-authentication phase and phase 2 is authentication and confirmation phase. In the pre-authentication phase, we will prepare the destination BS for handover procedure. In this, authentication and key establishment take place between the base stations. This step is done before the actual handover request is made. In the second phase, request for the handover is made, and handover confirmation is done.

Initially a commonly used authentication procedure such as [145] will be used to authenticate the device to the network. It is also assumed that the *eNB* involved in the handover procedure have been authenticated and added to the SDN network. Authentication process will be running as a service at the management layer of SDN network. We

will call it Virtual authentication service (*VAS*) and it will be programmable through the management layer API. *VAS* has a master public-private key (K, K^{-1}) , where K is known to all AP's. *VAS* will periodically authenticate AP during the off-peak hours and will distribute the certificates to the device. The revocation process becomes easily manageable with *VAS* acting as an authority. SDN controller will have a dedicated cache available to store the cryptographic hash of the authentication information. For additional security, a traditional salt mechanism will be used to store the hash values. By reserving a dedicated cache at the controller level, the authentication process will speed up, and the delay to access the remote authentication server is avoided. During the initial authentication, the controller will cache the relevant information. The idea of using cache in SDN has been investigated in few studies [146] [147], we enhance the concept to leverage its use for authentication purposes thus aiding in latency reduction. The problem of privacy, non-tractability and non-link ability are solved by using a pseudonym for the entities involved in the procedure.

Following initial assumptions are made regarding the state of the network.

- $\text{State}(eNB_a, UE)$: Authenticated, UE is in an active session with eNB_a .
- $\text{State}(eNB_b, UE)$: Not Authenticated.
- $\text{State}(eNB_a, VAS)$: AP is authenticated to the network.
- $\text{State}(eNB_b, VAS)$: AP is authenticated to the network .
- $\text{State}(eNB_a, eNB_b)$: Not Authenticated.

It is assumed that UE is currently in an active session with the eNB_a . The mobility path in the scenario is from eNB_a to eNB_b and moving into the range of eNB_c . UE will update its security context information with eNB_a . The information used as physical attributes (PA) is already available at the AP. PA are channel attributes such as channel quality index (CQI), frequency channel and modulation rate. This information is already shared info between UE and eNB_a through the resource blocks (RB). UE will generate a nonce which will be used for freshness verification. K_{ua} is a symmetric session key established

Table 4.1: Notation Used

Symbol	Description
pid_i	Pseudo-identity for the device i
bid_j	Base station pseudo id j
LC	Current location of the device
D	Direction of movement of UE
R	Round trip time with the base station
N_x	Nonce for a principal x
PA	Physical attributes of the device
AP	Access point
UE	User equipment
BS	Base station
$h(\cdot)$	A secure one-way hash function
$M_1 M_2$	The concatenation operation on M_1 and M_2 data
N_x	Nonce for principal x
$E_k(M)$	Encryption of message M
K_{xy}	Symmetric key between principles x and y
K_x^{-1}	Private key for principal x
$\{M\}_{K_{xy}}$	Message M is encrypted with symmetric key K_{xy}
$\{M\}_{K_x^{-1}}$	Message M is signed with private key K_x^{-1}
T_a	Time period for the validity of the certificate for a

during authentication between the eNB_a and UE . The first message will be passing of the relevant security parameters to the eNB_a .

$$\mathbf{M1} : UE \rightarrow eNB_a : \{pid_i || bid_a || PA_i || LC_i || D_i || R_i\}_{K_{ua}} \quad (4.1)$$

eNB_a will update the UE authentication parameters with the VAS . N_a is freshly generated, freshness implies that the value has not been used before. It will also send a signed hashed value of the message so as to preserve the integrity of the message. Once VAS receives the message it will verify the information.

$$\begin{aligned} \mathbf{M2} : eNB_a \rightarrow VAS : \{ &VAS || bid_a || pid_i || PA_i || LC_i || D_i || R_i || N_a || \\ &\{h(VAS || bid_a || pid_i || PA_i || LC_i || D_i || R_i || N_a)\}_{K_a^{-1}}\}_{K_{av}} \end{aligned} \quad (4.2)$$

Where K_{av} is the session key between VAS and eNB_a . Once VAS receives the authentication information from eNB_a , it will decrypt the message and verify the certificate. Once the authenticity, validity and integrity of the message is verified, VAS will update authentication vector of the user. VAS will generate the session key K_{ab} and forward the message to eNB_b . $AUTH$ will be calculated at VAS as $h(N_{si}, N_a, CK, IK)$. Where N_{si} is the security context information sent by eNB_a , CK and IK are the ciphering and

integrity key which were generated during the initial authentication of the device to the network.

$$\begin{aligned} \mathbf{M3} : VAS \rightarrow eNB_b : \{ & bid_a || bid_b || pid_i || Ind_i || PA_i || LC_i || D_i || R_i || N_a || AUTH || K_{ab} || \\ & \{ h(bid_b || pid_i || PA_i || LC_i || D_i || R_i || N_a || K_{ab} || AUTH) || (A, K_a, T_a) \}_{K_{VAS}^{-1}} \}_{K_{bv}} \end{aligned} \quad (4.3)$$

VAS will determine the mobility path and will register the authentication information with next access point. *VAS* has information to communicate securely between the source and destination base stations. If the session key is not established it can be done with public key available at *VAS*. Ind_i is the index of access point being updated. This information can be used in the admission control process to determine the priority of incoming requests. It gives the SDN controller a mechanism to expedite priority handover requests. *VAS* will create session key for eNB_a to eNB_b link. The management of session keys between access point has been offloaded to SDN controller service due to the centralized nature of the network. *VAS* will generate the session keys for the entities involved in the session.

In 5G HetNet, an explicit secure channel does not exist between the handover entities. A secure channel between the *eNB* and SDN controller will be leveraged for authentication process. If the session key between *VAS* and eNB_b is expired or not established yet, then *VAS* will encrypt the message with symmetric session key and encrypt the session key with PK which was established during the network entry. The authentication credentials are sent along with the signed hash of the message to next access point along the mobility path. Furthermore, SDN controller will be able to dynamically deploy routing mechanism for efficiently forwarding messages between the underlying routing devices between eNB_a and eNB_b .

$$\begin{aligned} \mathbf{M4} : VAS \rightarrow eNB_a : \{ & pid_i || bid_b || K_{ab} || N_s || N_a || \{ h(pid_i || bid_b || K_{ab} || \\ & K_{ac} || N_s) || (B, K_b, T_b) \}_{K_{VAS}^{-1}} \}_{K_{av}} \end{aligned} \quad (4.4)$$

Once eNB_a receives the message from *VAS*, it will decrypt the message and verify the signature. Authenticity, origin and integrity of the message is established through the

verification process. *VAS* message contains session keys of the next *eNB* along the mobility path. N_a is used to verify the freshness of the message. N_s will be saved to verify the freshness of the incoming handover requests.

$$\mathbf{M5} : eNB_B \rightarrow eNB_A : \{HandOffReq||bid_b||pid_i||N_a||N_b||\{h(HandOffReq||bid_b||pid_i||N_a||N_b)\}_{K_B^{-1}}\}_{K_{ab}} \quad (4.5)$$

The handover process starts when *UE* moves into the range of the next access point. When *eNB_b* detects the *UE* inside of its range, it will send over a request for handover. The message will be decrypted using the session key provided by *VAS*. Signature verification will be done on the hashed value. After the integrity of the message is confirmed, *eNB_a* will verify the handover request freshness. The hash of the result is computed and compared with the value sent in the message. *eNB_a* will reply with acknowledgment.

$$\mathbf{M6} : eNB_A \rightarrow eNB_B : \{HandOffAck||pid_i||N_b||\{h(HandOffAck||N_b)\}_{K_A^{-1}}\}_{K_{ab}} \quad (4.6)$$

Once *eNB_b* receives the handoff acknowledgment, it will retrieve the nonce. If the nonce matches the expected value, then it will verify the signature and hash of the message.

$$\mathbf{M7} : eNB_A \rightarrow U : \{HandOffCmd||N_a||N_b\}_{K_{ua}} \quad (4.7)$$

eNB_a will pass the handoff command encrypted with the session key established with the *UE*. The command will inform the *UE* of the upcoming handoff message. It will pass nonce of *eNB_b* so that the *UE* can calculate the next session key K_{eNB_b} for next access point.

$$\mathbf{M8} : eNB_B \rightarrow U : \{UpdateReq\}_{K_{eNB_b}} \quad (4.8)$$

eNB_b will request for an update of the security parameters N_{si} , where the initial K_{eNB_b} is computed as $KDF(N_a, N_{si}, CK||IK)$. $CK||IK$ are calculated at the *UE* during authentication to the network.

$$\mathbf{M9} : U \rightarrow eNB_B : \{UpdateACK(SCI)\}_{K_{eNB_b}'} \quad (4.9)$$

UE will update the security context information encrypted with the newly derived session key. The new key will be derived as $K_{eNB_b}' = KDF(h(N_{si}, N_b), K_{eNB_b})$. The transferred information is verified to be more recent than previously shared one. VAS then shares the secure information to next cell APs according to the location and direction information in new SCI. $M1 - M4$ consists of pre-authentication procedure whereas step $M5 - M9$ are part of the handover procedure.

4.3 Security Analysis

We perform security analysis SAH using three methods. First, proof of logic correctness will be presented using BAN logic. Next, we show a formal proof of security for the scheme. Lastly, we present an informal proof of security.

BAN logic [148] is a logic developed for reasoning about protocols based on some assumptions and rules. It is one of the most popular formal methods to analyze and verify authentication protocols. The logical analysis helps to perform security analysis on protocols. In BAN logic the agents involved in the protocol are called Principals. It is assumed that principals are honest. Some of the general definitions in BAN logic are explained here. Principals are those agents involved in the protocol (usually people or programs). P, Q, R are all possible symbols for the principals in the rules definition. U_i, eNB_a, eNB_b, VAS are principals used. Symmetric keys are used to encrypt messages in sessions. Public keys are used in pairs, one of which is known to all. (K_b, K_b^{-1}) is example of key pair. Nonces are message parts that are not meant to be repeated. N_a, N_b, N_{si} are nonces used in proposed algorithm. Timestamps are similar to the nonces in that they are unlikely to be repeated. However, they reflect the current time of the person creating them e.g. T_a, T_b are timestamps.

For analyzing a protocol using BAN logic, we will idealize the protocol first and then list the assumptions and goals. Application of natural induction rules on idealized messages should lead to the security proof thus achieving the stated goals. BAN logic notation are summarized in table 4.2.

4.3.1 BAN Logic Analysis

Some of the inference rules from BAN logic are summarized below. The rules will be used to perform logical reasoning to achieve the stated goals. If P and Q have a shared key K and if P sees a message or formula signed with the key, then it believes that Q once said X . This is called *message meaning* rule. A similar rule applies to the private key.

Table 4.2: BAN Logic Notation

$P \models X$	P believes in X . This means that P trust formula X .
$P \triangleleft X$	P see X . This means that P has received X in a formula or sub formula
$\#(X)$	X is fresh. X is a nonce and freshness implies that it has not occurred before.
$P \models\triangleright X$	P has jurisdiction over X . It is used when reasoning over certificate authorities.
$P \sim X$	P once said X . Principal P has once sent a message containing X . It is not known how long ago the message was sent.
$P \stackrel{k}{\leftrightarrow} Q$	P and Q use a shared key K . Key is good and only known to P and Q
$\stackrel{k}{\rightarrow} P$	P has a public key K and a corresponding private key K^{-1} . The private key is only know to P or the principal trusted by P .
$P \stackrel{k}{\rightleftharpoons} Q$	X is a secret known only to P and Q .
$\{X\}_k$	Encryption of X with key K .
$\{X\}_{k^{-1}}$	X has been signed with private key K^{-1}

$$\frac{P \models Q \stackrel{K}{\leftrightarrow} P, P \triangleleft \{X\}_K}{P \models Q \sim X}, \frac{P \models \stackrel{K}{\rightarrow} Q, P \triangleleft \{X\}_{K^{-1}}}{P \models Q \sim X} \quad (4.10)$$

If P believes that X is fresh and Q once said X , then P believes that Q still believes in X . This rule is called *nonce verification* rule.

$$\frac{P \models \#(X), P \models Q \sim X}{P \models Q \models X} \quad (4.11)$$

If principal P believes that principal Q has jurisdiction over X and Q believes in X , then P will also believe in X . This rule is called *jurisdiction rule*.

$$\frac{P \models Q \models\triangleright X, P \models Q \models X}{P \models X} \quad (4.12)$$

Introduction rule applies to multi part messages, where if P believes in the components, then it will also believe in the aggregate and similar rule will apply to decomposition of a multi-part message. These rules will be referred as *decomposition rule*.

$$\frac{P \triangleleft (X, Y)}{P \triangleleft X}, \frac{P \models X, P \models Y}{P \models (X, Y)}, \frac{P \models (X, Y)}{P \models X} \quad (4.13)$$

The belief of the rule can be extended. If P believe that Q see/believe in aggregate message then P believe that Q believe the component of the message.

$$\frac{P \models Q \sim (X, Y), P \models Q \models (X, Y)}{P \models Q \sim X}, \frac{P \models Q \models (X, Y)}{P \models Q \models X} \quad (4.14)$$

If P believe that component X of a message is fresh then P believe in the key. The is called *key introduction* rule.

$$\frac{P \models \#(k), P \models Q \models X}{P \models P \overset{K}{\leftrightarrow} Q} \quad (4.15)$$

where X is the necessary element for a key. If P can verify that X has been signed by Q , then it can see the contents of the message X by using it's public keys. Then P believe that the aggregate message is also fresh. This rule will be called *freshness promotion* rule.

$$\frac{P \models \#(X)}{P \models \#(X, Y)} \quad (4.16)$$

In addition to these general BAN rules, we will use an extension of public key crypto system (PKCS) for BAN proposed in [149]. Following terms are used in PKCS.

- $\mathcal{PK}(K, A)$: Principal A has a good public key K associated with it. There exist a private key corresponding to the public key.
- $\Pi(A)$: A has a good private key known to it only.
- $\sigma(X, A)$: Formula or message X has been signed with private key belonging to A .
- $(\Theta(t1, t2), X)$: Means that X holds in the interval $(t1, t2)$
- $\Delta(t1, t2)$: $t1, t2$ denote a good time interval
- $\mathcal{R}(P, X)$: P is the intended recipient of the message X .

If Q has a good public and a private key and X is signed with Q private key, then it will lead to belief that Q once said X . This rule is called *signature verification* rule.

$$\frac{P \models \mathcal{PK}(K, Q), P \models \Pi(Q), P \triangleleft \sigma(X, Q)}{P \models Q \sim X} \quad (4.17)$$

Next rule explains that content of a signed message are visible.

$$\frac{P \triangleleft \sigma(X, Q)}{P \triangleleft X} \quad (4.18)$$

The rule for duration stamped messages can be given as

$$\frac{P \models Q \models \Delta(t_1, t_2), P \models Q \vdash (\Theta(t_1, t_2), X)}{P \models Q \models X} \quad (4.19)$$

Certificates for P can be described in the idealized form as

$$\sigma((\Theta(\delta_p), \mathcal{PK}(P_p, P)), C) \quad (4.20)$$

where $\delta_p = (t_1, t_2)$ is the duration of C_p

4.3.2 Initial Assumptions

Some assumptions are done for the initial state of the system. The protocol will be analyzed under these assumptions

- Assumptions for eNB_a are

$$\begin{array}{ll} eNB_a \models \mathcal{PK}(K_{VAS}, VAS) & eNB_a \models \Pi(VAS) \\ eNB_a \models eNB_a \xleftrightarrow{K_{as}} VAS & eNB_a \models \#(eNB_a \xleftrightarrow{K_{as}} VAS) \\ eNB_a \models N_a & eNB_a \models \Delta(\delta_{VAS}) \\ eNB_a \models eNB_a \xleftrightarrow{K_{ua}} U & eNB_a \models \#(eNB_a \xleftrightarrow{K_{ua}} U) \\ eNB_a \models VAS \models \mathcal{PK}(K_b, eNB_b) & eNB_a \models HandOver_{ack} \end{array}$$

- Assumptions for VAS are

$$\begin{array}{ll} VAS \models \mathcal{PK}(K_a, eNB_a) & VAS \models \mathcal{PK}(K_b, eNB_b) \\ VAS \models \Delta(\delta_{eNB_a}) & VAS \models \Delta(\delta_{eNB_b}) \\ VAS \xleftrightarrow{IK, CK} U & VAS \models eNB_a \xleftrightarrow{K_{as}} VAS \\ VAS \models \#(eNB_a \xleftrightarrow{K_{as}} VAS) & VAS \models eNB_b \xleftrightarrow{K_{bs}} VAS \\ VAS \models \#(eNB_b \xleftrightarrow{K_{bs}} VAS) & VAS \models AUTH \end{array}$$

- Assumptions for eNB_b are

$$\begin{array}{ll}
 eNB_b \models \mathcal{PK}(K_{VAS}, VAS) & eNB_b \models \Pi(VAS) \\
 eNB_a \models eNB_b \xleftrightarrow{K_{bs}} VAS & eNB_a \models \#(eNB_b \xleftrightarrow{K_{bs}} VAS) \\
 eNB_b \models N_b & eNB_b \models \Delta(\delta_{VAS}) \\
 eNB_b \models VAS \models \mathcal{PK}(K_a, eNB_a) & eNB_b \models HandOver_{req}
 \end{array}$$

- Assumptions for UE are

$$\begin{array}{ll}
 U \models U \xleftrightarrow{K_{ua}} eNB_a & eNB_a \models \#(eNB_a \xleftrightarrow{K_{ua}} U) \\
 U \xrightarrow{\text{IK,CK}} VAS & U \models N_{si} \\
 U \models (VAS \models eNB_b \models AUTH) &
 \end{array}$$

These assumptions establish control over nonces, authority of VAS and belief that it will create good keys. $HandOver_{req}$ and $HandOver_{ack}$ can be treated as nonce for the purpose of analysis.

4.3.3 Goal

Mutual authentication between UE and eNB_b are the main goals for handover. Furthermore both should believe in the established shared session key.

$$U \models U \xleftrightarrow{K_{ub}} B \quad (4.21)$$

$$B \models U \xleftrightarrow{K_{ub}} B \quad (4.22)$$

$$U \models B \models U \xleftrightarrow{K_{ub}} B \quad (4.23)$$

$$B \models U \models U \xleftrightarrow{K_{ub}} B \quad (4.24)$$

Another goal would be to establish the handover request is fresh and the corresponding party believes in the request and the acknowledgement.

$$A \models \#(HandOverReq) \quad (4.25)$$

$$B \models \#(HandOverAck) \quad (4.26)$$

$$A \models B \models (HandOverReq) \quad (4.27)$$

$$B \models A \models (HandOverAck) \quad (4.28)$$

$$U \models \#(HandOver_{cmd}) \quad (4.29)$$

Non-repudiation of the handover request and acknowledgement is also one of the goal of this scheme.

$$A \models \mathcal{R}(A, HandOverReq) \quad (4.30)$$

$$B \models \mathcal{R}(B, HandOverAck) \quad (4.31)$$

4.3.4 Idealized Form

In idealized form, parts of the message which do not contribute to the belief will be removed. To simplify the notations for analysis purpose, we will denote the principals UE, eNB_a, eNB_b, eNB_c as U, A, B, C and their corresponding public, private key pairs as $(K_a, K_a^{-1}), (K_b, K_b^{-1}), (K_c, K_c^{-1})$. Similarly, the session keys will use a simplified form as K_{xy} where X, Y denotes the principals sharing the key.

$$Message\ 1 : U \rightarrow A : \{N_{si}\}_{K_{ua}} \quad (4.32)$$

For simplicity we will use N_{si} to denote the security parameters used for authentication such as PA_i, LC_i, D_i, R_i . Most of the information in first message can be described as a nonce for analysis purpose.

$$Message\ 2 : A \rightarrow VAS : \{N_a, N_{si}, \sigma((N_a, N_{si}), K_A^{-1}), \mathcal{R}(VAS, (N_a, N_{si}))\}_{K_{av}} \quad (4.33)$$

$$Message\ 3 : VAS \rightarrow B : \{N_a, N_{si}, AUTH, (A \xleftrightarrow{K_{ab}} B) \# (A \xleftrightarrow{K_{ab}} B), \sigma(M_{vb}, K_{VAS}^{-1}, VAS), \mathcal{R}(B, M_{vb}), C_a\}_{K_{bv}} \quad (4.34)$$

Where M_{vb} denotes the message component $\{AUTH, N_a, N_{si}, K_{ab}\}$ and C_a denotes $\sigma(\Theta(\delta_a), \mathcal{PK}(K_a, A), VAS)$.

$$Message\ 4 : VAS \rightarrow A : \{N_a, N_{si}, (A \xleftrightarrow{K_{ab}} B) \# (A \xleftrightarrow{K_{ab}} B), \sigma(M_{va}, K_{VAS}^{-1}, VAS), \mathcal{R}(A, M_{va}), C_b\}_{K_{av}} \quad (4.35)$$

Where M_{va} denotes $\{N_a, N_{si}, K_{ab}\}$, C_b denotes $\sigma(\Theta(\delta_b), \mathcal{PK}(K_b, B), VAS)$.

$$\begin{aligned} \text{Message 5 : } B \rightarrow A : \{ & HandOver_{req}, M_{ba}, \sigma(HandOver_{req} || M_{ba}, K_B^{-1}, VAS), \\ & \mathcal{R}(A, HandOver_{req}) \}_{K_{ab}} \end{aligned} \quad (4.36)$$

Where M_{ba} denotes $\{N_b, N_a, N_{si}\}$.

$$\begin{aligned} \text{Message 6 : } A \rightarrow B : \{ & HandOver_{ack}, N_b, \sigma(HandOver_{ack}, N_b, K_A^{-1}, VAS), \\ & \mathcal{R}(B, HandOver_{ack}) \}_{K_{ab}} \end{aligned} \quad (4.37)$$

$$\text{Message 7 : } A \rightarrow U : \{ HandOver_{cmd}, N_a, N_b \}_{K_{ua}} \quad (4.38)$$

$$\text{Message 8 : } B \rightarrow U : \{ HandOver_{upd} \}_{K_{ub}} \quad (4.39)$$

$$\text{Message 9 : } U \rightarrow B : \{ N_{si'} \}_{K_{ub'}} \quad (4.40)$$

4.3.5 Analysis and Proof

The first main goal of the security analysis is to verify the mutual authentication between the user device and destination AP. The second main goal is to verify that shared session key established during handover is secure. Initial assumptions and goals have been laid down earlier, in this section we will do the analysis on the idealized form of the protocol. Each message of the idealized form will be analyzed using the BAN logic rules. The process starts with U collecting security information and sending it over to A . From the first message in (5.9) we get

$$A \triangleleft \{N_{si}\}_{K_{ua}}$$

Applying *message meaning* rule we get

$$A \models U \sim N_{si}$$

Using initial assumption for U and applying *jurisdiction rule* we get

$$A \models U \models N_{si} \text{ and } A \models U \models \#(N_{si})$$

A chooses a random N_a based on the initial assumption that it has control over the nonce. An entity creating a nonce will believe in it's value and freshness.

$$A \models N_a$$

$$A \models \#(N_a)$$

From Message 2 in eq. (5.10) we get

$$VAS \triangleleft \{N_a, N_{si}, \sigma((N_a, N_{si}), K_a^{-1}), \mathcal{R}(VAS, (N_a, N_{si}))\}_{K_{as}}$$

Applying *signature verification* and *message meaning* rule we get

$$VAS \models A \sim \{N_a, N_{si}, \sigma((N_a, N_{si}), K_a^{-1}), \mathcal{R}(VAS, (N_a, N_{si}))\}$$

Using *decomposition rule* we can conclude that.

$$VAS \models A \sim \{N_{si}\}$$

$$VAS \models A \sim \{N_a\}$$

VAS will verify the security context information, then applying *freshness promotion* rule it follows as

$$VAS \models \#(N_{si}) \text{ and } VAS \models \#(N_a)$$

Similarly it can be applied to rest of the message, if part of formula is fresh then entire formula is fresh

$$VAS \models \#(\{N_a, N_{si}, \sigma((N_a, N_{si}), K_a^{-1}), \mathcal{R}(VAS, (N_a, N_{si}))\})$$

Applying *nonce verification* rule we get

$$VAS \models A \models \{N_a, N_{si}, \sigma((N_a, N_{si}), K_a^{-1}), \mathcal{R}(VAS, (N_a, N_{si}))\}$$

Applying the *signature verification*, *jurisdiction* and *decomposition* rules it can be logically inferred that

$$VAS \models \mathcal{R}(VAS, (N_a, N_{si}))$$

Applying initial assumptions for VAS , we will calculate $AUTH$ as $h(N_{si}, N_a, CK, IK)$, implicit conclusion from the initial assumption can be reached that

$$VAS \models AUTH \text{ and } VAS \models \#(AUTH)$$

From message 3 in eq. (4.34) we get

$$B \triangleleft \{N_a, N_{si}, (A \xleftrightarrow{K_{ab}} B), \#(A \xleftrightarrow{K_{ab}} B), \sigma(M_{vb}, K_{VAS}^{-1}, VAS), \mathcal{R}(B, M_{vb}), C_a\}_{K_{bv}}$$

Using *message meaning* and *signature verification* rule here, we get

$$B \equiv VAS \sim \{N_a, N_{si}, AUTH, (A \xleftrightarrow{K_{ab}} B), \#(A \xleftrightarrow{K_{ab}} B), \sigma(M_{vb}, K_{VAS}^{-1}, VAS), \mathcal{R}(B, M_{vb}), C_a\}$$

It is important to clarify one of the initial assumption here. We conclude that we cannot reach a conclusion on the freshness of this message from logical analysis without employing further assumptions. Such a conclusion can be reached if we add a timestamp to message from VAS or do an additional handshake with VAS . However, that will add an overhead to the communication. If this message is an old replayed message, then the authentication will not proceed in next step because of nonce verification at eNB_a . We conclude that establishing freshness of this message is not necessary. Using the signature rule we can verify the public keys. From the message we get C_a is $\sigma((\Theta(\delta_a), \mathcal{PK}(K_a, A)), VAS))$. Using the initial assumption that VAS will generate valid keys only.

$$B \equiv VAS \equiv \sigma((\Theta(\delta_a), \mathcal{PK}(K_a, A)), VAS)) \quad (4.41)$$

Applying *jurisdiction* rule we get

$$B \equiv \sigma((\Theta(\delta_a), \mathcal{PK}(K_a, A)), VAS)) \quad (4.42)$$

Based on *signature* rule and the initial assumption that VAS will not issue invalid certificate. The assumption ($eNB_b \equiv VAS \equiv \Delta\delta_a$) is derived implicitly from the assumption ($eNB_b \equiv VAS \Rightarrow \mathcal{PK}(K_a, A)$) Applying *jurisdiction* rule we get

$$B \equiv \mathcal{PK}(K_a, A) \quad (\text{Goal})$$

From message 4 in (4.35) we get

$$A \triangleleft \{N_a, N_{si}, (A \xleftrightarrow{K_{ab}} B) \# (A \xleftrightarrow{K_{ab}} B), \sigma(M_{va}, K_{VAS}^{-1}, VAS), \mathcal{R}(B, M_{va}), C_b\}_{K_{av}}$$

From *message meaning* rule we get

$$A \models VAS \sim \{N_a, N_{si}, (A \xleftrightarrow{K_{ab}} B), \#(A \xleftrightarrow{K_{ab}} B), \sigma(M_{va}, K_{VAS}^{-1}, VAS), \mathcal{R}(A, M_{va}), C_b\}$$

A will verify the freshness of the nonce N_a . Applying *freshness promotion* rule we get

$$A \models \#(\{N_a, N_{si}, (A \xleftrightarrow{K_{ab}} B), \#(A \xleftrightarrow{K_{ab}} B), \sigma(M_{va}, K_{VAS}^{-1}, VAS), \mathcal{R}(B, M_{va}), C_b\})$$

Using *nonce verification* rule we get

$$A \models VAS \models \{N_a, N_{si}, (A \xleftrightarrow{K_{ab}} B) \# (A \xleftrightarrow{K_{ab}} B), \sigma(M_{va}, K_{VAS}^{-1}, VAS), \mathcal{R}(B, M_{va}), C_b\}$$

All participants believe that every entity will keep their private keys private so non-repudiation is established here for the signed message.

$$A \models VAS \models \mathcal{R}(A, M_{va})$$

As already established that A believes in the freshness of message and that the freshness can be applied to all components of the message, using *decomposition* and *nonce verification* rules we get

$$A \models \mathcal{R}(A, M_{va})$$

C_b is $\sigma((\Theta(\delta_b), \mathcal{PK}(K_b, A)), VAS))$. Using tag verification conclusion derived above, *decomposition* rule and *nonce verification* rule we get

$$A \models VAS \models \sigma((\Theta(\delta_b), \mathcal{PK}(K_b, B)), VAS)) \quad (4.43)$$

Applying *jurisdiction* rule we get

$$A \models \sigma((\Theta(\delta_b), \mathcal{PK}(K_b, B)), VAS)) \quad (4.44)$$

Based on *signature* rule and the initial assumption that VAS will not issue invalid certificate. The assumption $(eNB_a \models VAS \models \Delta\delta_b)$ is derived implicitly from the assumption $(eNB_a \models VAS \models \mathcal{PK}(K_b, B))$ Applying *jurisdiction* rule we get

$$A \models \mathcal{PK}(K_b, B) \quad (\text{Goal})$$

From message 5 in eq. (4.36) we get

$$A \triangleleft \{HandOver_{req}, M_{ba}, \sigma(HandOver_{req} || M_{ba}, K_B^{-1}, VAS), \mathcal{R}(A, HandOver_{req})\}_{K_{ab}}$$

Using *message meaning* and *signature verification* rule we get

$$A \models B \sim \{HandOver_{req}, M_{ba}, \sigma(HandOver_{req} || M_{ba}, K_B^{-1}, VAS), \mathcal{R}(A, HandOver_{req})\}$$

A will verify N_a , if the nonce is verified to be correct then the freshness of nonce will be established as well ($A \models \#(N_a)$). Using *freshness promotion* rule it can be established that

$$A \models \#(\{HandOver_{req}, M_{ba}, \sigma(HandOver_{req} || M_{ba}, K_B^{-1}, VAS), \mathcal{R}(A, HandOver_{req})\})$$

From *decomposition* rule we conclude

$$A \models \#(HandOver_{req}) \quad (\text{Goal})$$

Applying *nonce verification* rule we get

$$A \models B \models \{HandOver_{req}, M_{ba}, \sigma(HandOver_{req} || M_{ba}, K_B^{-1}, VAS), \mathcal{R}(A, HandOver_{req})\}$$

From *decomposition* rule and *jurisdiction rule* we conclude

$$A \models B \models HandOver_{req} \quad (\text{Goal})$$

$$A \models \mathcal{R}(A, HandOver_{req}) \quad (\text{Goal})$$

From message 6 in eq.(4.37) we get

$$B \triangleleft \{HandOver_{ack}, N_b, \sigma(HandOver_{ack}, N_b, K_A^{-1}, VAS), \mathcal{R}(B, HandOver_{ack})\}_{K_{ab}}$$

From *message meaning* rule we get

$$B \models A \sim \{HandOver_{ack}, N_b, \sigma(HandOver_{ack}, N_b, K_A^{-1}, VAS), \mathcal{R}(B, HandOver_{ack})\}$$

Freshness can be established by verifying N_b .

$$B \models \#(\{HandOver_{ack}, N_b, N_{si}, \sigma(HandOver_{ack}, N_b, N_{si}, K_A^{-1}, VAS), \mathcal{R}(B, HandOver_{ack})\})$$

From *decomposition* rule

$$B \models \#(HandOver_{ack}) \quad (\text{Goal})$$

Applying *nonce verification* we get

$$B \models A \models \{HandOver_{ack}, N_b, \sigma(HandOver_{ack}, N_b, K_A^{-1}, VAS), \mathcal{R}(B, HandOver_{ack})\}$$

Applying similar step of rules as in message 5 we can get to the conclusion

$$B \models A \models HandOver_{ack} \quad (\text{Goal})$$

$$B \models \mathcal{R}(B, HandOver_{ack}) \quad (\text{Goal})$$

From message 7 we get

$$U \triangleleft \{HandOver_{cmd}, N_{si}, N_b\}_{K_{ua}}$$

$$U \models A \vdash \{HandOver_{cmd}, N_{si}, N_b\}$$

U will verify the freshness of nonce N_{si} . Applying *promotion* and *decomposition* rule we get

$$U \models \#(HandOver_{cmd}) \quad (\text{Goal})$$

U will compute session key $K_{ub} = h(N_{si}, N_a, CK || IK)$, where freshness of this key is implicit from *freshness promotion* rule on N_{si} .

$$U \models \#(U \xleftrightarrow{K_{ub}} B)$$

From message 8,

$$U \triangleleft \{HandOver_{upd}, N_a, N_b\}_{K_{ub}}$$

Applying initial assumptions and *message meaning* rule we get

$$U \models B \vdash \{HandOver_{upd}, N_a, N_b\}$$

Applying *nonce verification* rule we get

$$U \models B \models U \xleftrightarrow{K_{ub}} B \quad (\text{Goal})$$

U will be able to verify the key with computed value which leads to the belief that $U \models B \models AUTH$, where $AUTH$ were component to derive the key. Applying the *key introduction* rule we get

$$U \models (U \xleftrightarrow{K_{ub}} B) \quad (\text{Goal})$$

From message 9 we get,

$$B \triangleleft \{N_{si}', N_b\}_{K_{ub'}}$$

where B will compute $K_{ub'} = h((N_{si}, N_b), K_{ub})$, based on initial assumption and *message meaning* rule we get

$$B \models U \sim \{N_{si}', N_b\}$$

B will verify the nonce N_b and applying *freshness promotion* rule we get

$$B \models \#(N_{si}', N_b)$$

Applying *nonce verification* rule and rule from eq. (4.14) we get

$$B \models U \models U \xleftrightarrow{K_{ub}} B \quad (\text{Goal})$$

Similarly from *freshness promotion* rule and *key introduction* rule it can be inferred

$$B \models U \xleftrightarrow{K_{ub}} B \quad (\text{Goal})$$

4.3.6 Formal Security Verification Using AVISPA Tool

In addition to the BAN analysis, we provide the simulation result for our proposed algorithm using the widely accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [150]. The tool provides a modular expressive language for specifying security protocols and their security properties. The tool performs automatic analysis using back-end models. Protocols to be studied in AVISPA tool have to be specified in HLPSL (High Level Protocols Specification Language). The goals used for simulation verification are secrecy of the session key K_{ab} , secrecy of session key K_{ub} and a strong authentication between UE and eNB_b . We have simulated the proposed algorithm using On-the-fly-Model-Checker (OFMC) and Constraint Logic based Attack

% OFMC	SUMMARY
% Version of 2006/02/13	SAFE
SUMMARY	DETAILS
SAFE	BOUNDED_NUMBER_OF_SESSIONS
DETAILS	TYPED_MODEL
BOUNDED_NUMBER_OF_SESSIONS	PROTOCOL
PROTOCOL	/home/span/span/testsuite/results/SDNAuthen.if
GOAL	GOAL
as_specified	As Specified
BACKEND	BACKEND
OFMC	CL-AtSe
COMMENTS	STATISTICS
STATISTICS	
parseTime: 0.00s	Analysed : 5133 states
searchTime: 0.31s	Reachable : 988 states
visitedNodes: 198 nodes	Translation: 0.04 seconds
depth: 13 plies	Computation: 0.04 seconds

Figure 4.1: AVISPA Simulation

Figure 4.2: Security Protocol Animator's Message Sequence Chart

Searcher (CL-AtSe) backend with a bounded number of session. Different iterations of the session have been verified where an honest agent's session runs in parallel with an intruder's session who is acting as one of the agents. The intruder is able to collect information with the honest session and use it for another session. The results in Figure (4.1) shows simulation results for two sessions where the intruder is acting as agent B in the second session. Using SPAN (Security Protocol Animator) [151] we were able to build message sequence charts (MSC) of the protocol execution for further verification. SPAN provides the ability to interactively inject messages as an intruder performing a specific attack. Mutual authentication and secrecy of keys K_{ab} and $K_{ub'}$ goals have been verified through simulation.

4.3.7 Security Analysis

In this section, an informal analysis against a variety of attack is shown.

4.3.7.1 Mutual Authentication and Key Agreement

During the handover procedure, mutual authentication and key agreement will be established between UE and eNB . This has been proved through BAN analysis earlier. AVISPA simulation results given below also prove this security property.

4.3.7.2 User Anonymity

We use pseudo identity for UE and base stations. A new pseudo id will be assigned for each new session so the identity of any UE cannot be associated with a particular base station without the explicit mapping knowledge.

4.3.7.3 Non-Repudiation of Handover Request/Ack

This has been proved through BAN analysis. Handover Request and acknowledgment (Ack) are signed with the private keys which give a strong confirmation on the origin of the message. Nonce verification confirms the freshness of handover request and Ack.

4.3.7.4 Parallel Session Attacks

Use of signature provides a verification on the origin of the message and its integrity. Nonce generated during session are unique and as integrity of the message is verified, ipso facto information from one session will not be of use in another session. This type of attack is also tested through AVISPA simulation.

4.3.7.5 Binding Attack

Binding attack happens when an intruder tries to convince one of the base station on a compromised public key. Let's suppose eNB_a wants to perform a handover procedure with eNB_b , then in such an attack intruder I will try to convince eNB_a that eNB_b 's public key is K_i . Certificate timestamps will ensure the validity period of the certificates. Forgery of a certificate is non-feasible due to the computational complexity.

4.3.7.6 Replay Attack

Our scheme can withstand any replay attacks. The scheme uses random nonce for freshness checking at the base stations and by authentication service. The nonce challenge will be rejected once a replayed message is returned.

4.3.7.7 Perfect Forward Secrecy

Perfect secrecy ensures that the adversary cannot compute the session keys even if the private keys of the participants are compromised. The session keys derivation uses a hash of security parameters such as physical link properties, current location, direction, channel quality indicator. The pseudo id's used are also per session based. Due to collision resistance property of the one way hash function, it will be computationally infeasible for an adversary to compute the session key.

4.3.7.8 Known Session Security Parameters

The proposed algorithm uses session security parameters for key derivations. Assuming a known adversary gets this information, he will still not be able to generate the key without knowledge of random nonce, ciphering and integrity keys.

4.3.7.9 Denial of Service Attack

DoS attacks can be handled through SDN based architecture. An intrusion detection service running at controller layer will detect if an unusual number of connections are requested during a time window through a specific network node. The system can react by isolating the source and stopping the spread of traffic to other parts of the network. Furthermore, initial checking of security parameters could be performed at the source *eNB* without involving *VAS* so such a attack could be thwarted in the starting phase.

4.3.7.10 Typing Attack

In this type of attack, an intruder replaces a protocol message field with another type. As we are sending hash of the message, any such change will result in a mismatch during hash verification. Furthermore the signatures will verify the integrity of messages. AVISPA simulation uses typed and un typed properties to verify such attacks.

4.3.7.11 Man-in-the-Middle Attack

The communication protocol uses signed messages and secret sharing. Without the secret, an intruder will not be able to impersonate.

4.4 Performance Analysis

5G networks are poised to support a transmission rate of upto 10 Gb/sec. At such high data rates, the bulk of the authenticated handover time will be taken by cryptographic operations rather than the transmission time. For performance analysis, we have looked into the time taken by cryptographic operations. The time used by handover execution has been measured using OpenSSL Library [152] [153]. This methodology of benchmarking has been used in several studies. For the SDN controller and *eNB*, we have performed the simulation on a system with Intel i7-6600U CPU @ 2.60Ghz. For the mobile device, we have used Motorola Droid XT910 which uses a Dual-core 1.2 GHz Cortex-A9. Two test configuration has been studied for comparison. In configuration 1, we have used RSA-2048 for digital signatures whereas the encryption is done using

Table 4.3: Time Costs of Cryptography Operations

(ms)	S_T	V_T	T_{PreA}	T_A	T_{Total}
Config 1	3.165	0.095	1.957	1.417	3.375
Config 2	0.200	0.416	0.307	0.424	0.7315

S_T : Total sign time, V_T : Total verify time, T_{PreA} : Total Pre-Authentication time, T_A : Authentication time, T_{Total} : Total time

AES-256-CBC and hashing uses SHA-256. In configuration 2 we have used ECDSA-256 which is equivalent to RSA-2048 in terms of key strength. Config 2 uses AES-256-CBC for encryption and SHA-256 for hashing.

To further compare our scheme against the existing method we will calculate computation time for some of the cryptographic operations. From [121], we find that $T_{PM} \approx 0.90 * T_{ME}$, $T_{TP} \approx 22.6 * T_{ME}$. Table 4.4 shows the cost of cryptographic operations on the eNB and UE. Based on the computational time presented in Table 4.4 we calculate

Table 4.4: Time Costs of Cryptography Operations

(ms)	T_E	T_H	T_{RV}	T_{PM}	T_{TP}
eNB	0.0337	0.00079	0.0190	0.030	0.7616
UE	0.225	0.0013	0.127	0.2025	2.87

T_E :modular exponentiation, T_{RV} :RSA Verification, T_M :point mul, T_P : Tate pairing, T_H : Hash (SHA-256)

the authentication time of different handover schemes as shown in Table 4.5. To calculate the authentication time we have assumed RSA 2048 or equivalent key strength in all the schemes. For IBC based scheme we have considered cost of three major operations as they will take the bulk computational time. The cost at user equipment and base station is measured as $T_{PM} + 2T_{TP} + 2T_H$. For Chameleon hash-based scheme the cost is estimated as $4T_E + 2T_{RV} + 3T_H$. For UNAEN based authentication the total computational cost is $5T_E + 2T_H$ at device and AP.

Next, we focus on the energy consumption. We calculate the power consumption

Table 4.5: Handover Authentication Time

(ms)	Authentication Time
IBC Scheme[110]	7.499
Chameleon Hash Scheme[154]	1.185
UNAEN Scheme [155]	1.433
Our Scheme	0.424

as $E = T \times W$, where T is the execution time for an operation and W is the CPU power. From Intel i5/i7 specification, we found the power to be 95W and calculated the energy consumption using the above formula. For energy consumption comparison, we are interested in the user device only. For the base station, the energy consumption is not a critical issue. For user device, it is a limited and valuable resource. A comparison of the energy consumption is shown in Table 4.6, Where $TA_{UE}(ms)$ is the total computational time at the user device for authentication process. $E_{UE}(mJ)$ is the energy consumed by the user device during the authentication procedure. The result shows that IBC scheme is the most expensive followed by UNAEN scheme then Chameleon hash scheme. Our scheme outperforms the other in terms of energy consumption. This is because symmetric encryption and hash operations are only used at the user device. As we are passing security context information, the main task involve are verification of the information which requires a hash operation only. The low-cost operation helps to reduce the overall cost whereas the alternative scheme is using public key based encryption hence the increased cost.

To study the performance of the proposed scheme under attack, we have assumed an unknown attack, such that it will be able to fail the authentication procedure. For the failed attempts, a new handover procedure will begin. Figure 4.3 shows how the authentication time will increase when under a successful unknown attack. The results are taken after 100,000 authentications were performed. The horizontal axis indicates the rate of failure that's if 10%, 20%...90% of the authentication attempts fail. The results

Table 4.6: Energy Consumption Comparison for UE

	$TA_{UE}(ms)$	$E_{UE}(mJ)$
IBC Scheme[110]	5.945	564.775
Chameleon Hash Scheme[154]	1.029	97.755
UNAEN Scheme [155]	1.1263	106.9985
Our Scheme	0.1152	10.944

show the delay impact under such an attack model. Config 2 will be able to meet the latency requirements of 5G even if 40% of the authentications fail due to an unknown attack. Results in table 4.3 show that the overall time taken by Config 2 is better than

Figure 4.3: Authentication Time Under Successful Unknown Attack

the time taken by Config 1. Time taken by the Config 2 will be able to meet the delay requirements of 5G.

4.5 Conclusion

In this chapter, we have introduced a new secure handover procedure for SDN-enabled 5G networks. The proposed procedure reduces the delay by taking advantage of SDN architecture. Distribution of the keys and single point of failure are the most common concern for a server-based solution which is resolved by using SDN. We have shown that our scheme is secure against known attacks. We have performed formal security analysis using BAN logic. We have further simulated the scheme using widely accepted AVISPA tool. Informal security analysis proves that the proposed scheme is secure against a variety of attacks. Performance analysis done shows that it will be able to meet the delay requirements of 5G networks.

Chapter 5

SDN-Enabled LTE-Advanced CoMP Authentication

5.1 Introduction

The evolution of LTE is helping the world to become more connected. An increase in the number of network-connected devices is proliferating LTE to more use cases. LTE enables users to achieve high data rates and low latency in 4G networks. LTE-Advanced plays a vital role in improving the latency, increasing data rates, providing ubiquitous connectivity, improving reliability, and strengthening security. LTE-Advanced Pro has taken another step forward towards the goal of 5G communication. It has laid down a roadmap of technologies that could help us to reach 5G. Carrier Aggregation, Dual Connectivity, and CoMP access are core technologies required in this roadmap. Dual Connectivity allows a user to receive data simultaneously from two base stations. With CoMP transmission and reception, multiple base stations can communicate with a user device. Carrier Aggregation (CA) allows the combination of multiple carriers to increase the transmission bandwidth. CA can be performed inter-band or intra-band. In 4G and 5G HetNet, combining these technologies will help to achieve low latency and high data rate goals. Security provisioning remains one of the critical aspects of 4G and 5G networks. DC and CoMP bring new challenges to security in the LTE-based networks. The device is required to communicate simultaneously with multiple base stations, and a secure channel is needed for such communications. 3GPP has laid down the specifications

for DC LTE security aspects. However, extending these methods to HetNet remains an open challenge. Furthermore, the security solution needs to meet the 5G network challenge of $1ms$ latency.

In this chapter, we will provide a mechanism for authentication and key establishment, in DC and CoMP 5G HetNet networks, which can meet the delay requirements of 5G. Our contribution to this problem is to provide an SDN-based authentication and key establishment solution for 5G LTE/LTE-Advanced networks. We devise a Merkle-tree-based scheme for fast authentication with multiple base stations. We extend the security context transfer concept to SDN-Enabled LTE-Advanced networks to achieve low latency. We provide a proof of logic correctness and a formal security proof using AVISPA. Performance analysis compares it with existing methods and proves that it can reduce the latency; moreover, it is more energy efficient for the user equipment. To the best of our knowledge, we are providing the first and best solution that provides a secure SDN authentication solution for CoMP, DC-based LTE 4G, and 5G HetNet.

5.2 Background

5.2.1 LTE-Advanced Dual Connectivity and CoMP

With DC and CA, LTE-based networks can connect to two base stations. The ability to simultaneously communicate with both base stations allows for an increased data rate and provides a mechanism to improve the QoS. However, it presents a challenge regarding coordination between the two base stations. From a security perspective, the device needs to have a secure channel with both base stations, and the base stations also need a secure channel with each other. The support of dense HetNet will be a cornerstone in 5G, making secure handovers in high mobility dense HetNet scenarios remains challenging. With DC support there is an additional requirement to authenticate the base station with the latency requirements of $1ms$, making most of the current methods ineligible in 5G. 3GPP has laid down the specification for secure authentication and handover in DC LTE. The two deployment strategies are described below:

5.2.1.1 Separate Bearer

In this method, both *MeNB* and *SeNB* will have separate bearers as shown in Fig. (5.1). *SeNB* needs to create separate keys for encryption with the user. This method requires a secure channel between *MeNB* and *SeNB*. It also requires a secure channel between *SeNB* and *UE*. The X2 interface is used for signaling purposes.

Figure 5.1: Separate Bearer Scenario

5.2.1.2 Split Bearer

In this method, encryption will be done at *MeNB*. The packets will then be forwarded to *SeNB*, which will proceed to forward it to the device as shown in Fig. (5.2). This deployment method requires no security related changes and can work based on a legacy system. The Split Bearer method has few shortcomings as it overloads the X2-interface, which is predominantly used for signaling purpose only. Forwarding multiple streams to

Figure 5.2: Split Bearer Scenario

multiple users this way will create congestion on X2 interface. The transmission delay and latency are lower on the S1 interface compared to the X2 interface.

3GPP do not specify these strategies for CoMP explicitly. Due to the similarities between the two, the procedures can be applied to CoMP as well.

5.2.2 Open Issues

There are some gaps in the LTE DC and CoMP specifications that require investigation. Firstly, in many scenarios a direct connection between eNB and HeNB is not possible. Densification of the 5G network will create a lot of HeNB within a Macro cell. To deal with the scalability of the network, X2 proxy server or X2 gateways have been proposed. In some use cases, HeNB gateways are also widely used to communicate the eNB. Secondly, X2 interface security settings are optional, and implementation depends on the individual vendors. The specification assumes a direct, secure link between *MeNB*

and $SeNB$. An investigation is required for security implementation when a direct link is not secure, or a direct connection is not possible.

Figure 5.3: HeNB Scalability

Another issue is the key establishment. $SeNB$ keys are derived from the K_{eNB} session key. In some scenarios, the SCC counter is reset to zero. For example, when a K_{eNB} is refreshed through a vertical handover. It has been shown in [156] that LTE session key is not perfectly forward/backward secure. Due to the resetting of the counter, $SeNB$ keys have the same weakness.

5.2.3 Merkle-tree-based Authentication

A Merkle Tree is a complete binary tree where the internal nodes are computed by taking the hash of the leaf nodes. Usually, the leaf nodes are kept secret whereas the root is made public. It is computationally infeasible to compute the leaf nodes from the root node. Fig (5.4) shows an example Merkle Tree. In the example, if node B wants to perform authentication with node A. It will pass H_B and H_{CD} . Based on these two values A can compute the root and authenticate it as B. There has been prior work done which uses a Merkle tree for authentication [157] in smart grids.

Figure 5.4: Merkle-Tree

5.3 Proposed Scheme

In Chapter 4, we have proposed an SDN-based model for 5G networks. We will use the same model here.

5.3.1 Authentication and Key Establishment

Authentication, confidentiality, integrity, privacy and non-repudiation are the main security properties required for any communication. Secure transfer of confidential information requires the creation of a secure channel. This process involves authentication and key establishment. In this section, we propose an authentication and key establishment scheme for a CoMP/DC LTE 5G HetNet. The problem is broken down into sub-problems. Firstly, the base station needs to authenticate CoMP candidates. During this step, the candidate base station will inform the *MeNB* about its security features. Secondly, key establishment takes place between CoMP candidates and the master base station. A negotiation of the security features to use with the device is done using the established keys. Lastly, the user device authenticates and establish keys with selected CoMP candidates. In the pre-authentication phase, we will pass the security information to the CoMP candidate and establish the session keys. The authentication phase will be

fast this way and can meet the 5G delay requirements.

5.3.1.1 Phase 1

Initially a commonly used authentication procedure such as [145] will be used to authenticate the device to the network. It is assumed that the UE is currently in an active session with the $MeNB_a$. It is within the range of few APs. AP_b , AP_c , AP_d , AP_e are possible candidates for a CoMP session. UE is sharing its security context information with the base station $MeNB_a$ and SDN controller. SDN's CoMP Authentication Module (CAM) will have this information with it. For the sake of completeness, we will show the context information transfer between eNB_a and SDN controller. Security context information consists of physical attributes such as channel quality index (CQI), frequency channel and modulation rate, and other attributes such as direction, distance, round trip time, pseudo identities of the base station and user equipment. UE will generate a nonce which will be used for freshness verification. K_{ua} is a symmetric session key established during authentication between the $MeNB_a$ and the UE . The first message will be passing of the relevant security parameters to the $MeNB_a$.

$$UE_i \rightarrow MeNB_a : \{pid_i || bid_a || sc_i\}_{K_{ua}} \quad (5.1)$$

Where the security context information is $sc = \{PA_i || LC_i || D_i || R_i\}$. $MeNB_a$ will update the UE authentication parameters with the CAM . N_a is freshly generated.

$$MeNB_a \rightarrow CAM : \{bid_a || bid_b || bid_c || bid_d || bid_e || pid_i || sc_i || N_a\}_{K_{as}} \quad (5.2)$$

Where K_{as} is the session key between CAM and $MeNB_a$. Once CAM receives the authentication information from $MeNB_a$, it will decrypt the message and update the authentication vector of the user. sk is the secret shared between $MeNB_a$ and SDN controller. $AUTH_j$ will be calculated at CAM using a Merkle-Tree approach.

Based on Merkle tree, the authentication vector for CoMP AP will be calculated as

$$AUTH_b = \{\mathcal{PK}_a, Hash1, Hash23, root\}$$

$$AUTH_c = \{\mathcal{PK}_a, Hash0, Hash23, root\}$$

Table 5.1: Notation Used

Symbol	Description
pid_i	Pseudo-identity for the device i
bid_j	Base station pseudo id j
sc	Security context information of the device
LC	Current location of the device
D	Direction of movement of UE
R	Round trip time with the base station
N_s	Nonce for a principal CAM
PA	Physical attributes of the device
AP	Access point
$MeNB_a$	Master eNodeB
UE	User equipment
BS	Base station
$h(.)$	A secure one-way hash function
$M_1 M_2$	The concatenation operation on $M1$ and $M2$ data
N_a	Nonce for principal a
$E_k(M)$	Encryption of message M
K_{ua}	Symmetric key between principles $MeNB_a$ and the UE
K_x^{-1}	Private key for principal x
$\{M\}_{K_{xy}}$	Message M is encrypted with symmetric key K_{xy}
$\{M\}_{K_x^{-1}}$	Message M is signed with private key K_x^{-1}
$\mathcal{PK}_b$	Public key of Access Point B

Figure 5.5: Merkle-Tree-Authentication

$$AUTH_d = \{\mathcal{PK}_a, Hash3, Hash01, root\}$$

$$AUTH_e = \{\mathcal{PK}_a, Hash2, Hash01, root\}$$

CAM will send the pre-authentication security context to the CoMP AP.

$$CAM \rightarrow AP_b : \{bid_a, K_{ab}, N_a, N_s, AUTH_b\}_{K_{bs}}$$

$$CAM \rightarrow AP_c : \{bid_a, K_{ac}, N_a, N_s, AUTH_c\}_{K_{cs}}$$

$$CAM \rightarrow AP_d : \{bid_a, K_{ad}, N_a, N_s, AUTH_d\}_{K_{ds}}$$

$$CAM \rightarrow AP_e : \{bid_a, K_{ae}, N_a, N_s, AUTH_e\}_{K_{es}}$$

$$CAM \rightarrow MeNB_a : \{N_a, N_s, K_{ax}, root\}_{K_{as}}$$

Where K_{ax} is derived from session key $K_{ax} = KDF(K_{xs}, rand)$, where x denotes any CoMP destination AP. The nonce is added to verify the freshness of the message. Our assumption is that the session key is already established between the destination CoMP and *CAM*. This is based on the architecture of SDN and will be done during the registration phase. Once a device enters the network it will establish a secure connection with the SDN controller. Furthermore, SDN controller will be able to dynamically deploy routing mechanism for efficiently forwarding the messages on the underlying routing devices between *MeNB_a* and CoMP devices. The AP will inform about its security capabilities such as encryption algorithm it supports as *alg*.

$$AP_b \rightarrow MeNB_a : \{\mathcal{PK}_b, \{N_b', N_a, N_s, Hash1, Hash23, root, alg\}_{K_a}\}_{K_{ab}}$$

Where $N_b' = N_a \oplus N_b$, once *MeNB_a* receives the message it will start the authentication process. Firstly, the root is verified to check that it matches the stored value. Secondly, the verification of the Merkle-tree will start. *MeNB_a* will calculate Hash0 based on the $\mathcal{PK}_b$ sent by *AP_b*. It will use the Hash1 and calculate Hash01. Then it will use the result and Hash23 to verify the root matches. It can be seen that a total of three hash calculation will be performed to achieve the authentication. Merkle-Tree based authentication helps to achieve authentication and guarantees the validity and freshness of the message. We also establish that $\mathcal{PK}_b$ is a good key without performing any expensive signature

distribution and verification procedures. The procedure has protection against denial of service attacks as the root comparison will fail for an invalid request. Similarly, other CoMP candidates will perform the same steps.

$$AP_c \rightarrow MeNB_a : \{\mathcal{PK}_c, \{N'_c, N_a, N_s, Hash0, Hash23, root, alg\}_{K_a}\}_{K_{ac}}$$

$$AP_d \rightarrow MeNB_a : \{\mathcal{PK}_d, \{N'_d, N_a, N_s, Hash3, Hash01, root, alg\}_{K_a}\}_{K_{ad}}$$

$$AP_e \rightarrow MeNB_a : \{\mathcal{PK}_e, \{N'_e, N_a, N_s, Hash2, Hash01, root, alg\}_{K_a}\}_{K_{ae}}$$

Once a secure channel has been established between the base stations. $MeNB_a$ will respond back to the challenge.

$$MeNB_a \rightarrow AP_b : \{bid_b, N_a, N_b, alg, \{H(bid_a, bid_b, N_a, N'_b, alg)\}_{K_b}\}_{K_{ab}}$$

Similarly, to the other APs.

$$MeNB_a \rightarrow AP_c : \{bid_c, N_a, N_c, alg, \{H(bid_a, bid_c, N_a, N'_c, alg)\}_{K_c}\}_{K_{ac}}$$

$$MeNB_a \rightarrow AP_d : \{bid_d, N_a, N_d, alg, \{H(bid_a, bid_d, N_a, N'_d, alg)\}_{K_d}\}_{K_{ad}}$$

$$MeNB_a \rightarrow AP_e : \{bid_e, N_a, N_e, alg, \{H(bid_a, bid_e, N_a, N'_e, alg)\}_{K_e}\}_{K_{ae}}$$

This concludes the security context transfer phase. A secure channel has been established between the $MeNB$ and candidate CoMP APs.

5.3.1.2 Phase 2

In the second phase the device authentication takes place and bearer offload is done. Once $MeNB$ decides to offload some of the bearers to CoMP APs it will begin the process. Key establishment will be similar to the LTE specs $CK_{eNB-B} = KDF(K_{eNB}, SCC_1, N_b)$ with the addition of a nonce.

$$Message\ 1 : MeNB_a \rightarrow AP_b : \{CK_{eNB}, DRB\}_{K_{ab}} \quad (5.3)$$

$$Message\ 2 : MeNB_a \rightarrow UE : \{SCC, DRB, N_b, alg\}_{K_{ua}} \quad (5.4)$$

A similar sequence of steps will take place for other CoMP candidates. Due to the context transfer we have reduced the actual authentication to a two-step procedure. According to the *3GPP* specifications SCC will be updated for each of the new connection, similarly during handover it will be reset.

$$MeNB_a \rightarrow AP_c : \{CK_{eNB-C}, DRB2\}_{K_{ac}} \quad (5.5)$$

$$MeNB_a \rightarrow UE : \{SCC, DRB2, N_c, alg\}_{K_{ua}} \quad (5.6)$$

$$MeNB_a \rightarrow AP_d : \{CK_{eNB-D}, DRB3\}_{K_{ad}} \quad (5.7)$$

$$MeNB_a \rightarrow UE : \{SCC, DRB3, N_d, alg\}_{K_{ua}} \quad (5.8)$$

$$MeNB_a \rightarrow AP_e : \{CK_{eNB-E}, DRB3\}_{K_{ab}} \quad (5.9)$$

$$MeNB_a \rightarrow UE : \{SCC, DRB3, N_e, alg\}_{K_{ua}} \quad (5.10)$$

Where

$$CK_{eNB-C} = KDF(K_{eNB}, SCC_2, N_c)$$

$$CK_{eNB-D} = KDF(K_{eNB}, SCC_3, N_d)$$

$$CK_{eNB-E} = KDF(K_{eNB}, SCC_4, N_e)$$

5.4 Security Evaluation

Security evaluation will be carried out in three ways. Firstly, formal proof of logic correctness will be established through BAN analysis. Secondly, formal security verification will be done using simulation. Lastly, an informal analysis is done for the popular type of attacks.

5.4.1 Proof of Logic Correctness

BAN logic [148] is a logic developed for reasoning about protocols based on some assumptions and rules. It is one of the most popular formal methods to analyze and verify authentication protocols. For analyzing a protocol using BAN logic, we will idealize the protocol first and then list the assumptions and goals. Application of natural induction rules on idealized messages should lead to the security proof thus achieving the stated goals. We will analyze a subset of the problem i.e. pre-authentication of one AP using BAN. However, the results can be extended to other APs. We have used an extension of BAN logic for public keys [149]. This will help in analysis of messages employing public keys.

5.4.1.1 Initial Assumptions

Some assumptions are made for the initial state of the system. The protocol will be analyzed under these assumptions. Assumptions for $MeNB_a$ will establish a belief in CAM and the fact that it will issue good keys.

$$MeNB_a \models \mathcal{PK}(K_{CAM}, CAM)$$

$$MeNB_a \models A \xleftrightarrow{K_{as}} CAM$$

$$MeNB_a \models \#(A \xleftrightarrow{K_{as}} CAM)$$

$$MeNB_a \models \Pi(CAM)$$

$$MeNB_a \models N_a$$

$$MeNB_a \models CAM \models \Delta(\delta_{AP_b})$$

$$MeNB_a \models \Delta(\delta_{CAM})$$

$$MeNB_a \xRightarrow{sk} CAM$$

Assumptions for CAM will be The assumptions are that SDN controller module will give out valid public keys.

$$CAM \models \mathcal{PK}(K_a, A)$$

$$CAM \models \mathcal{PK}(K_b, B)$$

$$CAM \models \Pi(A)$$

$$CAM \models \Pi(B)$$

$$CAM \models \Delta(\delta_{MeNB_a})$$

$$CAM \models \Delta(\delta_{AP_b})$$

Assumptions for a DC/CoMP candidate AP_b will be

$$AP_b \models \mathcal{PK}(K_{VAS}, VAS)$$

$$AP_b \models \Pi(VAS)$$

$$AP_b \models N_b$$

$$AP_b \models AP_b \xleftrightarrow{K_{bs}} CAM$$

$$AP_b \models \#(AP_b \xleftrightarrow{K_{bs}} CAM)$$

Assumptions for UE will be

$$UE \models UE \xleftrightarrow{K_{ua}} MeNB_a$$

$$UE \models N_{sc}$$

5.4.1.2 Goal

Mutual authentication between $MeNB_a$ and AP_b are the main goals for Phase one. Furthermore, both should believe in the established shared session key.

$$MeNB_a \models N_a$$

$$AP_b \models N_b$$

$$MeNB_a \models AP_b \models N_a$$

$$AP_b \models MeNB_a \models N_a$$

$$\begin{aligned}
 AP_b &\models MeNB_a \models N_b \\
 MeNB_a &\models AP_b \models N_b \\
 AP_b &\models MeNB_a \xleftrightarrow{k} AP_b \\
 MeNB_a &\models AP_b \xleftrightarrow{k} MeNB_a
 \end{aligned}$$

5.4.1.3 Idealized Form

In an idealized form, parts of the message which do not contribute to the belief will be removed.

$$Message\ 1 : U \rightarrow MeNB_a : \{N_{sc}\}_{K_{ua}} \quad (5.11)$$

N_{sc} denotes the security context information used for authentication such as PA_i, LC_i, D_i, R_i . Most of the information in first message can be described as a nonce for analysis purpose.

$$Message\ 2 : MeNB_a \rightarrow CAM : \{bid_b, N_a, N_{sc}\}_{K_{as}} \quad (5.12)$$

$$Message\ 3 : CAM \rightarrow AP_b : \{K_{ab}, \#(K_{ab}), N_a, N_s, AUTH_b\}_{K_{bs}} \quad (5.13)$$

Where $AUTH_b = \{\mathcal{PK}_a, Hash1, Hash23, root\}$.

$$Message\ 4 : CAM \rightarrow MeNB_a : \{N_a, N_s, root, K_{ab}, \#(K_{ab})\}_{K_{as}} \quad (5.14)$$

$$\begin{aligned}
 Message\ 5 : AP_b \rightarrow MeNB_a : \{ \mathcal{PK}_b, \#(\mathcal{PK}_b), \{N_a, N_s, N_b, Hash1, \\
 Hash23, root, N_{alg}\}_{K_a} \}_{K_{ab}} \quad (5.15)
 \end{aligned}$$

$$\begin{aligned}
 Message\ 6 : MeNB_a \rightarrow AP_b : \{bid_b, N_a, N_b, N_{alg}, \{H(bid_a, bid_b, \\
 N_a, N_b)\}_{K_b}\}_{K_{ab}} \quad (5.16)
 \end{aligned}$$

5.4.1.4 Analysis and Proof

The first main goal of the security analysis is to verify the mutual authentication between $MeNB_a$ and AP_b . The second main goal is mutual belief in nonce from the corresponding party. Nonce verification would imply belief in freshness and origin of the nonce. Initial assumptions and goals have been laid down earlier, in this section we will do the analysis on the idealized form of the protocol. Each message of the idealized form will be analyzed using the BAN logic rules. The proof is done for only messages involved in authentication between $MeNB_a$ and AP_b , however it can be extended to AP_c , AP_d , AP_e . The process starts with UE collecting security information and sending it over to $MeNB_a$. From the first message in (5.11) we get

$$MeNB_a \triangleleft \{N_{sc}\}_{K_{ua}}$$

Applying rule from (4.10) we get

$$MeNB_a \models UE \sim N_{sc}$$

Using initial assumption for UE and applying rule (4.12) we get

$$MeNB_a \models UE \models N_{sc} \text{ and } MeNB_a \models UE \models \#(N_{sc})$$

$MeNB_a$ choose a random N_a and send to CAM . From Eq. (5.12) we get

$$CAM \triangleleft \{bid_b, N_a, N_{sc}\}_{K_{as}}$$

Applying rule from (4.10) we get

$$CAM \models MeNB_a \sim \{bid_b, N_a, N_{sc}\}$$

From Eq. (5.13) we get

$$AP_b \triangleleft \{K_{ab}, \#(K_{ab}), N_a, N_s, AUTH_b\}_{K_{bs}}$$

Applying Eq. (4.12)

$$AP_b \models CAM \sim \{K_{ab}, \#(K_{ab}), N_a, N_s, AUTH_b\}$$

Using session key assumptions and applying (4.12) it can be concluded that

$$AP_b \models CAM \models \{AUTH_b\} \text{ and } AP_b \models CAM \models \#(AUTH_b)$$

Furthermore, applying promotion rule then jurisdiction rule (4.12) it can inferred that

$$AP_b \models K_{ab}$$

From Eq. (5.14) we get

$$MeNB_a \triangleleft \{N_a, N_s, root, K_{ab}, \#(K_{ab})\}_{K_{as}}$$

Using (4.10) we get

$$MeNB_a \models CAM \sim \{N_a, N_s, root, K_{ab}, \#(K_{ab})\}$$

$MeNB_a$ will verify N_a . If the nonce value matches then its freshness is established ($MeNB_a \models \#(N_a)$). Applying the Eq. (4.16) rule we can conclude that

$$MeNB_a \models \#(N_a, N_s, root, K_{ab}, \#(K_{ab}))$$

Applying Eq. (4.12) and promotion rule

$$MeNB_a \models K_{ab}$$

$$MeNB_a \models root$$

From Eq. (5.15) we get the authentication request

$$MeNB_a \triangleleft \{\mathcal{PK}_b, \#(\mathcal{PK}_b), \{N_a, N_s, N_b, Hash1, Hash23, root\}_{K_a}\}_{K_{ab}}$$

Applying rule from Eq. (4.10)

$$MeNB_a \models AP_b \sim \{\mathcal{PK}_b, \#(\mathcal{PK}_b), N_a, N_s, N_b, Hash1, Hash23, root\}$$

Freshness of the message is established by verifying the nonce ($MeNB_a \models \#(N_a)$) and applying the freshness promotion rule we get

$$MeNB_a \models \#(\{N_a, N_s, N_b, Hash1, Hash23, root\})$$

Applying nonce verification rule Eq. (4.11)

$$MeNB_a \models AP_b \models \{N_a, N_s, N_b, Hash1, Hash23, root\} \quad (\text{Goal})$$

Applying Eq. (4.12) and promotion rule

$$MeNB_a \models \{N_a, N_s, N_b, Hash1, Hash23, root\} \quad (\text{Goal})$$

$MeNB_a$ will carry out Merkle-tree based Authentication of AP_b and also establish that $\mathcal{PK}_b$ is good. Then it will send message in Eq. (5.16)

$$AP_b \triangleleft \{bid_b, N_a, N_b, N_{alg}, \{H(bid_a, bid_b, N_a, N_b)\}_{K_b}\}_{K_{ab}}$$

Applying rule from Eq. (4.10)

$$AP_b \models MeNB_a \sim \{bid_b, N_a, N_b, N_{alg}, \{H(bid_a, bid_b, N_a, N_b)\}_{K_b}\}$$

After establishing the freshness of the message from nonce N_b and applying rule Eq. (4.11)

$$AP_b \models MeNB_a \models \{bid_b, N_a, N_b, N_{alg}, \{H(bid_a, bid_b, N_a, N_b)\}_{K_b}\} \quad (\text{Goal})$$

Applying Eq. (4.12), Eq. (4.10) and decomposition rule

$$AP_b \models \{bid_b, N_a, N_b, N_{alg}, \{H(bid_a, bid_b, N_a, N_b)\}_{K_b}\} \quad (\text{Goal})$$

This concludes the pre-authentication phase.

5.4.2 Formal Security Proof

We perform formal security verification of the proposed algorithm through the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [150]. Protocols are written in High-Level Protocol Specification Language (HLPSL). The backend used for model verification are On-the-Fly-Model-Checker (OFMC) [158] and Constraint-Logic-based model checker. We have used Dolev-Yao attack model [143]. The adversary can intercept, modify and replay any message. He can start a parallel session and use current session information in another session. AVISPA supports two types of goals in

HLPSL specifications i.e. secrecy and authentication. To verify the security of our scheme we have used strong mutual authentication and secrecy of session keys as a goal. The main roles defined in our scheme are the role of SDN controller service *CAM*, *MeNB_a* and *SeNB*. HLPSL specifications for creating the Merkle tree and verification of the Merkle tree is given below.

Code for CAM role

```

role role_CAM( MeNBa,SeNBb,CAM:agent,
               Sk:symmetric_key,
               KPa,KPb,KPs:public_key,
               H: function,
               Kas,Kbs:symmetric_key,
               SND,RCV:channel(dy)
           )
played_by CAM
def=
  local
    State:nat,
    Na,Nsc,Ns:text,
    H0,Hash0,Hash01,Root:message, Hash1,Hash23:text,
    Kab:symmetric_key
  init
    State := 0
  transition
    2. State=0 /\ RCV({SeNBb.Na'.Nsc'}_Kas) =|>
      State':=1 /\ Ns':=new()
                  /\ H0' := H(SeNBb,Nsc',Sk,Na')
                  /\ Hash0' := H(H0',KPb)
                  /\ Hash1' := new()
                  /\ Hash01' := H(Hash0',Hash1')
                  /\ Hash23' := new()
                  /\ Kab' :=new()
                  /\ Root' := H(Hash01',Hash23')
                  /\ SND({Kab'.Na'.Ns'.KPa.Hash0'.Hash1'
                        .Hash23'.Root'}_Kbs)
                  /\ secret(Kab',sec_1,{MeNBa,CAM,SeNBb})
                  /\ SND({Kab'.Na'.Ns'.Root'}_Kas)

end role

```

Code for MeNBa role

```

role role_MeNBa( MeNBa,SeNBb,CAM:agent,
                 KPa,KPs:public_key,
                 Sk,Kas:symmetric_key,
                 H: function,
                 SND,RCV:channel(dy)
               )
played_by MeNBa
def=
  local
    State:nat,
    Nsc,NbOld,Na,Ns:text,
    H0,Hash0,Root,Nb:message,
    Hash1,Hash23:text,Kab:symmetric_key,
    KPb:public_key
  init
    State := 0
  transition
    1. State=0    /\ RCV(start) =|>
      State':=1  /\ Nsc':=new()
                  /\ Na':=new()
                  /\ witness(MeNBa,SeNBb,auth_3,Na')
                  /\ SND({SeNBb.Na'.Nsc'}_Kas)
    4. State=1    /\ RCV({Kab'.Na.Ns'.Root'}_Kas) =|>
      State':=2  /\ Hash1':= new()
                  /\ Hash23':= new()
                  /\ H0' := H(SeNBb,Nsc,Sk,Na)
    6. State=2    /\ RCV( {KPb'.{Na.Ns.Nb'.H(H0',KPb')}.
                        Hash1'.Hash23'.Root'}_KPa}_Kab)=|>
      State':=3  /\ SND({SeNBb.Na.Nb'.{H(MeNBa.SeNBb.
                        Na.Nb')}_inv(KPa)}_Kab)
                  /\ NbOld' := xor(Nb',Na)
                  /\ request(MeNBa,SeNBb,auth_4,NbOld')
end role

```

To verify the HLPSL specification correctness we have used SPAN (Security Protocol Animator) [151]. The tool can create a message sequence chart based on the HLPSL specifications. It provides a proof of execution. SPAN tools also provide an interactive intruder model where we can actively inject attack messages as an intruder during the

protocol execution. Figure 5.6 shows that the protocol animation is complete from the specifications. Thus it allows to carry out some manual attacks for verification purposes. Automatic verification of our scheme using AVISPA shows that it is safe. Results are

Figure 5.6: Security Protocol Animator's Message Sequence Chart

shown below. First we create a single session.

```
session(kbs,kas,h,kPs,kPb,kPa,MeNB_a,SeNB_b,CAM,sk)
```

OFMC results of a single session is shown below

```

% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/Merkle.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.01s
  visitedNodes: 6 nodes
  
```

Similarly using ATSE backend we get

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/Merkle.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed    : 7 states
  Reachable   : 2 states
  Translation: 0.00 seconds
```

To verify that the proposed scheme is safe against replay attacks we simulate multiple sessions. Two more sessions are created where intruder is acting as a *MeNB* and *SeNB*.

```
session(kbs,kas,h,kPs,kPb,kPa,MeNB_a,SeNB_b,CAM,sk)
/\ session(kbs,kas,h,kPs,kPb,kPa,MeNB_a,SeNB_b,CAM,sk)
/\ session(kbs,kai,h,kPs,kPb,kPi,i,SeNB_b,CAM,sk)
/\ session(kbi,kas,h,kPs,kPi,kPa,MeNB_a,i,CAM,sk)
```

Simulation results using OFMC and ATSE backend of multiple sessions is shown below.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/Merkle.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 39.03s
  visitedNodes: 14916 nodes
```

Similarly using ATSE backend we get

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/Merkle.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed    : 1421 states
  Reachable   : 333 states
  Translation: 0.02 seconds
```

5.4.3 Security Analysis

We perform an informal analysis against a variety of attacks.

5.4.3.1 Confidentiality

We use pseudo identities for UE , $MeNB_a$, $SeNB_b$ and CAM . A new pseudo ID is provided for each new session, so the identity of any entity is not traceable to a particular base station without the explicit mapping knowledge.

5.4.3.2 Replay Attack

Our scheme can withstand any replay attacks. The scheme uses random nonce for freshness checking at the base stations and by the authentication service.

5.4.3.3 Parallel Session Attacks

Nonce generated during the session are unique and as the integrity of the message is verified, ipso-facto information from one session will not be of use in another session. This type of attack is also tested through AVISPA simulation by modeling intruder in parallel sessions.

5.4.3.4 Perfect Forward Secrecy

Perfect secrecy ensures that the adversary cannot compute the session keys even if the private keys of the participants are compromised. The session keys derivation uses a random number per session; therefore, it is computationally infeasible to get the session keys without knowledge of the random number.

5.4.3.5 Denial of Service Attack

Merkle root is passed in the authentication request. If a wrong value is passed here then no further computation is done; moreover, such an attack will be thwarted in the starting phase.

5.4.3.6 Typing Attack

In this type of attack, an intruder replaces a protocol message field with another type. If there is any change to the messages, then the Merkle-tree path verification will fail. The tree verification guarantees the integrity of the keys. AVISPA simulation uses typed and untyped properties to verify such attacks.

5.4.3.7 Man-in-the-Middle Attack

This attack is not possible without knowledge of private/public keys. An adversary cannot falsify the public keys without changing the Merkle root. Due to the computational complexity, it is infeasible for an adversary to get a private key from the public key.

5.5 Performance Analysis

We use three main criteria to compare the performance of the proposed algorithm. Authentication delay is analyzed to see if the proposed scheme can meet the delay requirements of 5G LTE-A based network. Communication overhead is compared with some of the fast authentication schemes available today. Due to the importance of energy consumption in the mobile devices, an analysis is carried out for comparing.

5.5.1 Communication Overhead

To compute the communication overhead of the algorithms, we calculate the cost as a sum of the delays of the messages. The cost of communication between the device and authentication server is assumed to be at a maximum, so it's considered as one unit. The cost between *UE* and *eNB* is assumed to be in δ units. This is less than the cost of communication between a device and an authentication server ($0 < \delta < 1$). The cost of communication between the *eNBs* is assumed as ϵ units. The cost between two MMEs is considered to be η units. To calculate the total cost, we add up the cost of individual messages. A comparison of well-known authentication schemes in LTE is presented below. From Table (5.2), we can see that the communication overhead during

Table 5.2: Computational Cost Comparison

Scheme	Communication cost
HeNB to eNB per 3GPP [159],[160]	$3\delta + 4$
Inter MME per 3GPP [159],[160]	$3\delta + 2\eta + 4$
HeNB to Open access HeNB per 3GPP [159],[160]	$3\delta + 2\epsilon$
CapAuth Scheme [161]	$2\delta + 3$
UAP Scheme [162]	3δ
UNAEN Scheme [155]	3δ
Chameleon Hash Scheme [154]	3δ
IDC Scheme[110]	3δ
3GPP LTE Dual	$\delta + 2\epsilon$
Our Scheme	$\delta + \epsilon$

the authentication phase is similar to LTE Dual scheme. However, LTE Dual Scheme only works for scenarios where a direct connection is available between the *eNBs*, whereas in other scenarios scheme in [159] and [160] is used. Our proposed method is applicable in all scenarios as the security context is transferred during the first phase. Other schemes such as identity-based encryption, chameleon hashing based and universal authentication schemes all have similar overhead as our scheme. From the communication overhead perspective, they all provide a low overhead as compared to the LTE schemes where a direct link is not present. In a CoMP scenario, a mobile device can connect to multiple

Figure 5.7: Communication Cost for CoMP

base stations. LTE-Advanced supports up to eight downlink streams. Fig. 5.7 shows how the communication cost will scale when a user device performs the authentication procedure with multiple base stations. The cost between a user device and base station is almost the same as the cost between two base stations. Hence, we assume $\epsilon = \delta = 0.4$. The cost between the MME is less than the cost between a base station and user device. As a result, we assume it to be half $\eta = 0.2$.

5.5.2 Computational Cost

For performance analysis calculations we have used OpenSSL[152] and [121] benchmarks to calculate time for cryptographic operations execution. Most of the earlier studies have used 1024-bit key as a benchmark; however, they do not meet the security requirements of today's networks. As of 2016, RSA 2048 or ECDSA with P-224 are considered to be a secure key length. Future 5G networks are expected to keep up with the strength of the key requirements. Modern devices are much more power efficient and can carry out faster computations. For comparison, we have assumed that all the schemes are using RSA 2048 or equivalent key strength based mechanism. For benchmarking we have used

Intel i7-6600U CPU @ 2.60Ghz as an eNB and used two cores on Intel i5-2500 @ 3.30GHz as a user device. eNB is running on a 64-bit machine, and UE is on a 32-bit machine. From [121], we find that $T_{PM} \approx 0.90 * T_{ME}$, $T_{TP} \approx 22.6 * T_{ME}$. Table 5.3 shows the cost of cryptographic operations on the eNB and UE. IBC-based scheme computational cost

Table 5.3: Time Costs of Cryptography Operations

(ms)	T_E	T_H	T_{RV}	T_{PM}	T_{TP}
eNB	0.0337	0.00079	0.0190	0.030	0.7616
UE	0.225	0.0013	0.127	0.2025	2.87

T_E :modular exponentiation, T_{RV} :RSA Verification, T_M :point mul, T_P : tate pairing, T_H : Hash (SHA-256)

at the user equipment and base station are measured as $T_{PM} + 2T_{TP} + 2T_H$. Chameleon hash-based scheme computational cost at *UE* and *AP* is measured as $4T_E + 2T_{RV} + 3T_H$. For UNAEN based authentication the cost at device and AP will be $5T_E + 2T_H$ each. For LTE-based schemes *UE* will do $4T_H$ and *eNB* will do $2T_H$. In our scheme, the total cost at UE will be $5T_H$ and at AP will be $3T_H$. The UE is doing five hash operations among which four are for key establishment with the four CoMP AP and one for updating sci to controller. AP will perform three hash operations to verify the Merkle root before it requests for authentication. Table 5.4 shows the total cost comparison between different schemes.

Fig. 5.8 shows how the computational cost will scale when a user device performs the authentication procedure with multiple base stations. IBC based scheme is most expensive due to the Tate pairing operation. Chameleon hash scheme and UNAEN scheme are of similar cost. Our proposed scheme is slightly expensive than the LTE-based scheme in [159],[160]. As explained earlier, LTE scheme will only work in the scenario where a direct secure link is available between the source and destination AP.

Figure 5.8: Computational Cost for CoMP

Table 5.4: Comparison of Computational Cost

(ms)	T_{UE}	T_{eNB}	T_{Authen}	T_{CoMP}
IBC Scheme[110]	5.945	1.553	7.499	29.996
Chameleon Hash Scheme[154]	1.029	0.1561	1.185	4.74
UNAEN Scheme [155]	1.1263	0.170	1.433	5.732
LTE Schemes [159],[160]	0.0052	0.00158	0.00678	0.02712
Our Scheme	0.0065	0.00237	0.00887	0.03548

5.5.3 Energy Comparison

Energy consumption is an important aspect of mobile communication. Due to limited energy resources, computations that take place in the user device need to be energy efficient. We perform energy comparisons of proposed algorithms with other schemes. Table 5.5 shows the energy consumed by various cryptographic operations. To calculate the energy we use $E = T \times W$, where T is the execution time, and W is the CPU power. For i7 specification, we found the power to be 95W and calculated the energy consumption.

Table 5.5: Energy Costs of Cryptography Operations

(mJ)	T_E	T_H	T_{RV}	T_{PM}	T_{TP}
UE	21.375	0.1235	12.065	19.2375	272.65

T_E :modular exponentiation, T_{RV} :RSA Verification, T_M :point mul, T_P : Tate pairing

From the comparison presented in Table 5.6, we can see that the proposed scheme has energy consumption comparable with the LTE-based schemes. Fig. 5.9 shows how the energy cost will scale when a user device performs the authentication procedure with multiple base stations. IBC based scheme is most expensive due to the Tate pairing operation, as the computational time of this scheme is higher, the device will consume more energy. Chameleon hash scheme and UNAEN scheme are of similar cost. Our

Figure 5.9: Energy Consumption for CoMP

Table 5.6: Comparison of Energy Cost

(mJ)	E_{UE}	$E_{UE-CoMP}$
IDC Scheme[110]	564.775	2259.08
Chameleon Hash Scheme [154]	97.755	391.02
UNAEN Scheme [155]	106.99	427.99
LTE Schemes [159],[160]	0.494	2.0
Our Scheme	0.6175	2.5

proposed scheme is of similar order as the LTE-based scheme in [159],[160] but works in a scenario where a direct secure link has not been established between the eNB.

5.5.4 Performance Under An Unknown Attack

To study the performance of the proposed scheme under attack, we have assumed an unknown attack, such that it will be able to fail the authentication procedure. For the failed attempts, a new authentication procedure will begin. The authentication time used includes both phase one and phase two of the scheme. We further assume that any failure in authentication phase will cause the pre-authentication to reoccur. Figure 5.10 shows how the authentication time will increase when under a successful unknown attack. The results are taken after 100,000 authentications were performed. The horizontal axis indicates the rate of failure that's if 10%, 20%...90% of the authentication attempts fail. The results show the delay impact under such an attack model.

Figure 5.10: Authentication Time Under Successful Unknown Attack

5.6 Conclusion

DC and CoMP are important LTE technologies that are required to achieve 5G network goals. New CoMP and DC connections need to be established in user mobility scenarios. Creating a secure connection in a 5G HetNet is challenging due to low latency requirements. Existing methods cannot achieve the desired latency goal due to computational or communication overhead. We have proposed a scheme which leverages the SDN-enabled network to transfer security context before authentication. We have presented a formal proof of logic correctness. Formal security verification is done by means of AVISPA and SPAN. An informal analysis of the scheme shows that it is secure against a variety of attacks. Performance analysis for communication overhead, computational cost and energy consumption demonstrate that our scheme can meet 5G network requirements.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

In this thesis, we have studied QoS and security provisioning in LTE-Advanced based 4G/5G networks. We have reviewed the existing QoS and security procedures in LTE-Advanced and proposed solutions which can improve QoS and provide security.

Firstly, we start with QoS provisioning in 5G networks. We focus on resource scheduling to improve the QoS. We model the scheduling problem as resource matching problem. We present a heuristic Matching Game solution for the optimization problem. Simulation results show that Matching Game can improve the average throughput and keep similar fairness among the users. We demonstrate proof of stability and uniqueness for the proposed solution. We also show that the matching achieved from Matching Game is Pareto optimal.

Secondly, we focus on security in LTE-Advanced networks. We have explored authentication and key establishment in 5G networks. More specifically we have proposed a new handover procedure in SDN-enabled 5G networks. We examine the existing SDN-based solution in 5G and find several gaps in the current solution. We then propose a new scheme which creates a secure channel between source and destination AP. To the best of our knowledge, this is the best SDN-based solution for secure handover in 5G networks. We leverage SDN architecture to pass security context information of the user device. The proposed solution can meet the requirements of 5G networks. We have shown that

our scheme is secure against known attacks. We have performed formal security analysis using BAN logic. We have further simulated the scheme using widely accepted AVISPA tool. Informal security analysis proves that the proposed scheme is secure against a variety of attacks. Performance analysis done shows that it will be able to meet the delay requirements of 5G networks.

Building on our work on SDN-enabled 5G LTE-Advanced network, we further explore DC/CoMP authentication and key establishment in 5G network. We find that the existing methods will not be able to meet the latency requirement of 5G network. We propose a Merkle-tree based pre-authentication solution which can meet the demands of a 5G network. We present a formal and informal security analysis and perform logic correctness check. Performance analysis shows that our scheme performs better compared to the alternative schemes.

6.2 Future Work

Our proposed Matching Game scheme uses QoS as the main criteria for scheduling decision. Further research can explore other parameters impact on the system performance. Use of parameters such as delay, latency, load, type of traffic and fairness could yield some interesting results. By fine tuning some optimization criteria different scenario can be investigated. We have focused the study on a single eNB scheduling. With the introduction of CoMP, the scheduling algorithm needs to take other base stations into account. Another area of interest would be a cooperative matching algorithm which pools the resources from multiple base station to perform matching. One of the limitations of the proposed scheme is that the side requesting in the first place will have an optimal solution. As such, the presented algorithm is optimal from the UE request perspective. However, its stable from both sides perspective. Future work can be done to investigate an RB optimal solution. Future work can also expand into finding out a fair solution where a balanced matching can be achieved which is optimal for both sets of agents.

From a security perspective, SDN-enabled network authentication solutions could be investigated in some other scenario such as high-speed rail network, vehicular technol-

ogy. Another interesting area would be to examine group authentications with the SDN architecture. As the number of devices is increasing a lot group authentication remains a challenge for Internet of Things (IoT) devices due to the latency challenge of 5G networks. The investigation can be carried out to expand the proposed SDN-based solution to such scenarios.

Publication

- M. J. Alam and M. Ma, “Resource Matching in Carrier Aggregation Enabling 5G Networks,” *Wireless Personal Communications*, pp. 1–20, 2016
- M. J. Alam and M. Ma, “Pareto Efficient Resource Matching for LTE-A System,” in *2015 10th International Conference on Information, Communications and Signal Processing (ICICS)*, pp. 1–5, Dec 2015
- M. J. Alam and M. Ma, “Radio Resource Management by Evolutionary Algorithms for 4G LTE-Advanced Networks,” in *Bio-Inspired Computation in Telecommunications*, pp. 141–162, Morgan Kaufmann, 2015

References

- [1] G. Yuan, X. Zhang, W. Wang, and Y. Yang, “Carrier aggregation for LTE-Advanced mobile communication systems,” *IEEE Communications Magazine*, vol. 48, pp. 88–93, February 2010.
- [2] H. Lee, S. Vahid, and K. Moessner, “A Survey of Radio Resource Management for Spectrum Aggregation in LTE-Advanced,” *IEEE Communications Surveys Tutorials*, vol. 16, pp. 745–760, Second 2014.
- [3] Z. Zhao, J. Wang, S. Redana, and B. Raaf, “Downlink Resource Allocation for LTE-Advanced Networks with Type-1 Relay Nodes,” in *2012 IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1–5, Sept 2012.
- [4] Q. Kong, R. Lu, S. Chen, and H. Zhu, “Achieve Secure Handover Session Key Management via Mobile Relay in LTE-Advanced Networks,” *IEEE Internet of Things Journal*, vol. 4, pp. 29–39, Feb 2017.
- [5] F. Liu, E. Bala, E. Erkip, M. C. Beluri, and R. Yang, “Small-Cell Traffic Balancing Over Licensed and Unlicensed Bands,” *IEEE Transactions on Vehicular Technology*, vol. 64, pp. 5850–5865, Dec 2015.
- [6] C. Niu, Y. Li, R. Q. Hu, and F. Ye, “Femtocell-enhanced multi-target spectrum allocation strategy in LTE-A HetNets,” *IET Communications*, vol. 11, no. 6, pp. 887–896, 2017.

- [7] S. Mosleh, L. Liu, and J. Zhang, "Proportional-Fair Resource Allocation for Coordinated Multi-point Transmission in LTE-Advanced," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 5355–5367, Aug 2016.
- [8] D. Marabissi, G. Bartoli, R. Fantacci, and M. Pucci, "An Optimized CoMP Transmission for a Heterogeneous Network Using eICIC Approach," *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 8230–8239, Oct 2016.
- [9] P. Semov, P. Koleva, K. Tonchev, V. Poulkov, and A. Mihovska, "Autonomous learning model for achieving multi cell load balancing capabilities in HetNet," in *2016 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 1–5, June 2016.
- [10] H. Y. Lateef, A. Imran, M. A. Imran, L. Giupponi, and M. Dohler, "LTE-advanced self-organizing network conflicts and coordination algorithms," *IEEE Wireless Communications*, vol. 22, pp. 108–117, June 2015.
- [11] M. Peng, D. Liang, Y. Wei, J. Li, and H. H. Chen, "Self-configuration and self-optimization in LTE-advanced heterogeneous networks," *IEEE Communications Magazine*, vol. 51, pp. 36–45, May 2013.
- [12] Z. Yuanping, L. Wenjia, and Y. Xin, "A Novel Downlink Adaption Scheme for TDD Type-II Relay Systems," in *2011 Third International Conference on Measuring Technology and Mechatronics Automation*, vol. 1, pp. 191–194, Jan 2011.
- [13] H. He, Y. Rui, Y. Luo, Y. Zhu, and M. Li, "Power Scaling Method for Uplink Power Control with Carrier Aggregation," in *2011 Third International Conference on Measuring Technology and Mechatronics Automation*, vol. 2, pp. 883–886, Jan 2011.
- [14] S. Schwarz, C. Mehlhrer, and M. Rupp, "Calculation of the spatial preprocessing and link adaption feedback for 3GPP UMTS/LTE," in *2010 Wireless Advanced 2010*, pp. 1–6, June 2010.

REFERENCES

- [15] M. Hu, S. Jin, and X. Gao, "A low-complexity adaptive transmission scheme based on the dual-codebook of 3GPP LTE-Advanced," in *2011 International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–5, Nov 2011.
- [16] T. Warabino, S. Kaneko, S. Nanba, and Y. Kishi, "Advanced load balancing in LTE/LTE-A cellular network," in *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*, pp. 530–535, Sept 2012.
- [17] Y. Wang, K. I. Pedersen, P. E. Mogensen, and T. B. Sørensen, "Carrier load balancing methods with bursty traffic for LTE-Advanced systems," in *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 22–26, Sept 2009.
- [18] L. Zhang, F. Liu, L. Huang, and W. Wang, "Traffic load balance methods in the LTE-Advanced system with carrier aggregation," in *2010 International Conference on Communications, Circuits and Systems (ICCCAS)*, pp. 63–67, July 2010.
- [19] K. Lee, S. Kim, S. Lee, and J. Ma, "Load balancing with transmission power control in femtocell networks," in *13th International Conference on Advanced Communication Technology (ICACT2011)*, pp. 519–522, Feb 2011.
- [20] Y. Wang, K. I. Pedersen, T. B. Sørensen, and P. E. Mogensen, "Carrier load balancing and packet scheduling for multi-carrier systems," *IEEE Transactions on Wireless Communications*, vol. 9, pp. 1780–1789, May 2010.
- [21] Z. Zou, C. Guo, Z. Zeng, and S. Shi, "A Dynamic Adjusting Carrier Coverage-Based Load Balancing Scheme in LTE-Advanced System Based on Carrier Aggregation," in *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–4, Sept 2011.
- [22] Y. Liu and P. Chen, "Joint scheduling for MU-CoMP in uplink LTE-advanced systems," in *2012 IEEE 14th International Conference on Communication Technology*, pp. 214–218, Nov 2012.

REFERENCES

- [23] H. Wang, C. Rosa, and K. Pedersen, "Performance of Uplink Carrier Aggregation in LTE-Advanced Systems," in *2010 IEEE 72nd Vehicular Technology Conference - Fall*, pp. 1–5, Sept 2010.
- [24] H. Wang, C. Rosa, and K. Pedersen, "Uplink Component Carrier Selection for LTE-Advanced Systems with Carrier Aggregation," in *2011 IEEE International Conference on Communications (ICC)*, pp. 1–5, June 2011.
- [25] R. Sivaraj, A. Pande, K. Zeng, K. Govindan, and P. Mohapatra, "Edge-prioritized channel- and traffic-aware uplink Carrier Aggregation in LTE-advanced systems," in *2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–9, June 2012.
- [26] H. Wang, H. Nguyen, C. Rosa, and K. Pedersen, "Uplink multi-cluster scheduling with MU-MIMO for LTE-Advanced with carrier aggregation," in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1202–1206, April 2012.
- [27] P. Shang, X. Zhu, L. Zhang, J. Wu, and J. Chen, "Delta Metric Scheduling for LTE-Advanced Uplink Multi-User MIMO Systems," in *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, May 2012.
- [28] N. Prasad, H. Zhang, H. Zhu, and S. Rangarajan, "Multi-user MIMO scheduling in the fourth generation cellular uplink," in *2013 Asilomar Conference on Signals, Systems and Computers*, pp. 1855–1859, Nov 2013.
- [29] F. Liu, K. Zheng, W. Xiang, and H. Zhao, "Design and Performance Analysis of An Energy-Efficient Uplink Carrier Aggregation Scheme," *IEEE Journal on Selected Areas in Communications*, vol. 32, pp. 197–207, February 2014.
- [30] M. A. Lema, M. Garcia-Lozano, S. Ruiz, and G. D. Gonzalez, "Introduction of MPDR information for enhanced multi-cluster scheduling in LTE-A uplink," in *6th Joint IFIP Wireless and Mobile Networking Conference (WMNC)*, pp. 1–7, April 2013.

REFERENCES

- [31] I. S. Coma, M. Aydin, S. Zhang, P. Kuonen, and J. F. Wagen, “Reinforcement learning based radio resource scheduling in LTE-advanced,” in *The 17th International Conference on Automation and Computing*, pp. 219–224, Sept 2011.
- [32] N. Lei, C. Guo, C. Feng, and Y. Chen, “A multi-user MIMO resource scheduling scheme for carrier aggregation scenario,” in *2011 International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–5, Nov 2011.
- [33] Y. L. Chung, L. J. Jang, and Z. Tsai, “An efficient downlink packet scheduling algorithm in LTE-Advanced systems with Carrier Aggregation,” in *2011 IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 632–636, Jan 2011.
- [34] Y. L. Chung and Z. Tsai, “A quantized water-filling packet scheduling scheme for downlink transmissions in LTE-advanced systems with Carrier Aggregation,” in *SoftCOM 2010, 18th International Conference on Software, Telecommunications and Computer Networks*, pp. 275–279, Sept 2010.
- [35] M. S. ElBamby and K. M. F. Elsayed, “A transportation problem based resource allocation scheme for an LTE-Advanced system with carrier aggregation,” in *2012 IFIP Wireless Days*, pp. 1–6, Nov 2012.
- [36] L. Zeng, J. Jin, Y. Wang, and D. Yang, “A coordinated multi-cell MU-MIMO scheme for the downlink LTE-Advanced system,” in *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 2117–2121, Sept 2009.
- [37] L. Liu, G. Miao, and J. Zhang, “Energy-efficient scheduling for downlink multi-user MIMO,” in *2012 IEEE International Conference on Communications (ICC)*, pp. 4394–4394, June 2012.
- [38] H. Chen, Y. Jiang, J. Xu, and H. Hu, “Energy-Efficient Coordinated Scheduling Mechanism for Cellular Communication Systems with Multiple Component Car-

- riers,” *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 959–968, May 2013.
- [39] G. Yue, N. Prasad, and S. Rangarajan, “Downlink multiuser MIMO scheduling in LTE-Advanced systems,” in *2012 IEEE International Conference on Communications (ICC)*, pp. 4484–4488, June 2012.
- [40] L. Zhang, S. Peter, and C. Wang, “Performance evaluation of layer adaptive multi-user scheduling in LTE-A downlink,” in *7th International Conference on Communications and Networking in China*, pp. 787–791, Aug 2012.
- [41] F. Vitiello, S. Redana, and J. Hmlinen, “Admission control for LTE-Advanced relay systems,” in *European Wireless 2012; 18th European Wireless Conference 2012*, pp. 1–8, April 2012.
- [42] F. Tesema, F. Granelli, F. Vitiello, and S. Redana, “Priority and Buffer Based Admission Control in Relay-enhanced LTE-A systems,” in *European Wireless 2013; 19th European Wireless Conference*, pp. 1–6, April 2013.
- [43] K. Dimou, M. Wang, Y. Yang, M. Kazmi, A. Larmo, J. Pettersson, W. Muller, and Y. Timmer, “Handover within 3GPP LTE: Design Principles and Performance,” in *2009 IEEE 70th Vehicular Technology Conference Fall*, pp. 1–5, Sept 2009.
- [44] O. Teyeb, V. V. Phan, B. Raaf, and S. Redana, “Handover Framework for Relay Enhanced LTE Networks,” in *2009 IEEE International Conference on Communications Workshops*, pp. 1–5, June 2009.
- [45] J. Chang, Y. Li, S. Feng, H. Wang, C. Sun, and P. Zhang, “A Fractional Soft Handover Scheme for 3GPP LTE-Advanced System,” in *2009 IEEE International Conference on Communications Workshops*, pp. 1–5, June 2009.
- [46] X. Cao, D. Xiao, and C. Xiu, “Handover performance of relaxing SCell measurement period in LTE-A with carrier aggregation,” in *2011 International Conference on Electric Information and Control Engineering*, pp. 438–441, April 2011.

REFERENCES

- [47] H. Zhang, X. Wen, B. Wang, W. Zheng, and Z. Lu, "A Novel Self-Optimizing Handover Mechanism for Multi-service Provisioning in LTE-Advanced," in *2009 International Conference on Research Challenges in Computer Science*, pp. 221–224, Dec 2009.
- [48] T. Jansen, I. Balan, J. Turk, I. Moerman, and T. Kurner, "Handover Parameter Optimization in LTE Self-Organizing Networks," in *2010 IEEE 72nd Vehicular Technology Conference - Fall*, pp. 1–5, Sept 2010.
- [49] A. Ulvan, R. Bestak, and M. Ulvan, "The study of handover procedure in LTE-based femtocell network," in *WMNC2010*, pp. 1–6, Oct 2010.
- [50] C. C. Lin, K. Sandrasegaran, X. Zhu, and Z. Xu, "Performance evaluation of capacity based CoMP handover algorithm for LTE-Advanced," in *The 15th International Symposium on Wireless Personal Multimedia Communications*, pp. 236–240, Sept 2012.
- [51] C.-C. Lin, K. Sandrasegaran, and S. Reeves, "Handover algorithm with joint processing in LTE-advanced," in *2012 9th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, pp. 1–4, May 2012.
- [52] H. M. Tu, J. S. Lin, T. S. Chang, and K. T. Feng, "Prediction-based handover schemes for relay-enhanced LTE-A systems," in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 2879–2884, April 2012.
- [53] B. Feng and G. Li, "A low-overhead handover scheme for LTE-Advanced OFDM cellular networks," in *2012 International Conference on Computer Science and Information Processing (CSIP)*, pp. 389–392, Aug 2012.
- [54] T. Beniero, S. Redana, J. Hamalainen, and B. Raaf, "Effect of Relaying on Coverage in 3GPP LTE-Advanced," in *VTC Spring 2009 - IEEE 69th Vehicular Technology Conference*, pp. 1–5, April 2009.

REFERENCES

- [55] J. Zheng, P. Sartori, and B. Wei, "Performance Analysis of Layer 1 Relays," in *2009 IEEE International Conference on Communications Workshops*, pp. 1–6, June 2009.
- [56] S. Nagata, Y. Yan, X. Gao, A. Li, H. Kayama, T. Abe, and T. Nakamura, "Investigation on System Performance of L1/L3 Relays in LTE-Advanced Downlink," in *2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*, pp. 1–5, May 2011.
- [57] Y. Wang, G. Feng, and Y. Zhang, "Cost-Efficient Deployment of Relays for LTE-Advanced Cellular Networks," in *2011 IEEE International Conference on Communications (ICC)*, pp. 1–5, June 2011.
- [58] R. H. Gohary and H. Yanikomeroglu, "An emerging concept for 4G+ wireless cellular networks: Terminal relaying," in *2011 Saudi International Electronics, Communications and Photonics Conference (SIECP)*, pp. 1–4, April 2011.
- [59] Y. Hu and L. Qiu, "A Novel Multiple Relay Selection Strategy for LTE-Advanced Relay Systems," in *2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*, pp. 1–5, May 2011.
- [60] A. Karaer, . Bulakci, S. Redana, B. Raaf, and J. Hmlinen, "Uplink performance optimization in relay enhanced LTE-Advanced networks," in *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 360–364, Sept 2009.
- [61] J. Liu, C. Hu, Z. Ma, K. Zheng, and W. Wang, "Semi-persistent scheduling for VoIP service in the LTE-Advanced relaying networks," in *2010 International Conference on Communications, Circuits and Systems (ICCCAS)*, pp. 54–58, July 2010.
- [62] M. Minelli, M. Coupechoux, J. M. Kelif, M. Ma, and P. Godlewski, "Relays-enhanced LTE-Advanced networks performance studies," in *34th IEEE Sarnoff Symposium*, pp. 1–5, May 2011.

REFERENCES

- [63] J. Kennedy and R. Eberhart, “Particle swarm optimization,” in *Neural Networks, 1995. Proceedings., IEEE International Conference on*, vol. 4, pp. 1942–1948 vol.4, Nov 1995.
- [64] M. Campos, E. Bonabeau, G. Theraulaz, and J.-L. Deneubourg, “Dynamic scheduling and division of labor in social insects,” *Adaptive Behavior*, vol. 8, no. 2, pp. 83–95, 2000.
- [65] M. Dorigo, M. Birattari, and T. Stutzle, “Ant colony optimization,” *IEEE computational intelligence magazine*, vol. 1, no. 4, pp. 28–39, 2006.
- [66] D. Karaboga and B. Akay, “A survey: algorithms simulating bee swarm intelligence,” *Artificial Intelligence Review*, vol. 31, no. 1-4, pp. 61–85, 2009.
- [67] N. Gordon, I. A. Wagner, and A. M. Bruckstein, “Discrete bee dance algorithm for pattern formation on a grid,” in *Intelligent Agent Technology, 2003. IAT 2003. IEEE/WIC International Conference on*, pp. 545–549, IEEE, 2003.
- [68] T. D. Seeley, A. S. Mikheyev, and G. J. Pagano, “Dancing bees tune both duration and rate of waggle-run production in relation to nectar-source profitability,” *Journal of Comparative Physiology A*, vol. 186, no. 9, pp. 813–819, 2000.
- [69] K. Diwold, M. Beekman, and M. Middendorf, *Honeybee Optimisation – An Overview and a New Bee Inspired Optimisation Scheme*, pp. 295–327. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.
- [70] N. Lemmens, S. De Jong, K. Tuyls, and A. Nowe, “A bee algorithm for multi-agent systems: recruitment and navigation combined,” in *In Proceedings of ALAG, an AAMAS workshop*, Citeseer, 2007.
- [71] D. M. Gordon, “The organization of work in social insect colonies,” *Nature*, vol. 380, no. 6570, p. 121, 1996.
- [72] H.-L. Hung, “Application firefly algorithm for peak-to-average power ratio reduction in OFDM systems,” *Telecommunication Systems*, pp. 1–8, 2016.

- [73] S. Kirkpatrick, C. D. Gelatt, M. P. Vecchi, *et al.*, “Optimization by simulated annealing,” *science*, vol. 220, no. 4598, pp. 671–680, 1983.
- [74] J. Handl, J. Knowles, and M. Dorigo, “Ant-based clustering and topographic mapping,” *Artificial life*, vol. 12, no. 1, pp. 35–62, 2006.
- [75] E. D. Lumer and B. Faieta, “Diversity and adaptation in populations of clustering ants,” in *Proceedings of the third international conference on Simulation of adaptive behavior: from animals to animats 3: from animals to animats 3*, pp. 501–508, MIT Press, 1994.
- [76] E. Zitzler and L. Thiele, “Multiobjective evolutionary algorithms: a comparative case study and the strength pareto approach,” *IEEE Transactions on Evolutionary Computation*, vol. 3, pp. 257–271, Nov 1999.
- [77] S. Mao, Y. Zu, W. Li, and Y. Jia, “Resource Allocation Based on Genetic Algorithm in the Multiuser Cooperative OFDM System,” in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on*, pp. 1–4, IEEE, 2012.
- [78] H. M. Ali, S. Ashrafinia, J. Liu, and D. C. Lee, “Wireless Mesh Network Planning Using Quantum Inspired Evolutionary Algorithm,” in *Vehicular Technology Conference (VTC Fall), 2011 IEEE*, pp. 1–5, IEEE, 2011.
- [79] F.-S. Chu and K.-C. Chen, “Iterative tracking the minimum of overall energy consumption in OFDMA systems,” in *2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 102–106, IEEE, 2011.
- [80] A. Thompson, D. Corne, and C.-X. Wang, “Optimization of LTE scheduling using multi-objective evolutionary algorithms,” in *2010 UK Workshop on Computational Intelligence (UKCI)*, pp. 1–6, IEEE, 2010.

REFERENCES

- [81] T. Jiang, X. Tan, X. Luan, X. Zhang, and J. Wu, "Evolutionary game based access class barring for machine-to-machine communications," in *16th International Conference on Advanced Communication Technology*, pp. 832–835, IEEE, 2014.
- [82] H. Tian, S. Gao, J. Zhu, and L. Chen, "Improved Component Carrier Selection Method for Non-Continuous Carrier Aggregation in LTE-Advanced Systems," in *2011 IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1–5, Sept 2011.
- [83] Y. Wang, K. I. Pedersen, P. E. Mogensen, and T. B. Srensen, "Resource allocation considerations for multi-carrier LTE-Advanced systems operating in backward compatible mode," in *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 370–374, Sept 2009.
- [84] L. Lei and K. Zheng, "Performance evaluation of carrier aggregation for elastic traffic in LTE-Advanced systems," *IEICE transactions on communications*, vol. 92, no. 11, pp. 3516–3519, 2009.
- [85] L. Zhang, F. Liu, L. Huang, and W. Wang, "Traffic load balance methods in the LTE-Advanced system with carrier aggregation," in *Communications, Circuits and Systems (ICCCAS), 2010 International Conference on*, pp. 63–67, IEEE, 2010.
- [86] L. Zhang, K. Zheng, W. Wang, and L. Huang, "Performance analysis on carrier scheduling schemes in the long-term evolution-advanced system with carrier aggregation," *IET Communications*, vol. 5, pp. 612–619, March 2011.
- [87] L. Chen, W. Chen, X. Zhang, and D. Yang, "Analysis and Simulation for Spectrum Aggregation in LTE-Advanced System," in *2009 IEEE 70th Vehicular Technology Conference Fall*, pp. 1–6, Sept 2009.
- [88] L. Zhang, Y. Wang, L. Huang, H. Wang, and W. Wang, "QoS performance analysis on carrier aggregation based LTE-A systems," in *Wireless Mobile and Computing (CCWMC 2009), IET International Communication Conference on*, pp. 253–256, Dec 2009.

REFERENCES

- [89] F. P. Kelly, A. K. Maulloo, and D. K. Tan, “Rate control for communication networks: shadow prices, proportional fairness and stability,” *Journal of the Operational Research society*, vol. 49, no. 3, pp. 237–252, 1998.
- [90] M. Andrews, K. Kumaran, K. Ramanan, A. Stolyar, P. Whiting, and R. Vijayakumar, “Providing quality of service over a shared wireless link,” *IEEE Communications Magazine*, vol. 39, pp. 150–154, Feb 2001.
- [91] S.-B. Lee, S. Choudhury, A. Khoshnevis, S. Xu, and S. Lu, “Downlink MIMO with Frequency-Domain Packet Scheduling for 3GPP LTE,” in *INFOCOM 2009, IEEE*, pp. 1269–1277, April 2009.
- [92] M. Feng, S. Mao, and T. Jiang, “Enhancing the performance of future wireless networks with software-defined networking,” *Frontiers of Information Technology & Electronic Engineering*, vol. 17, no. 7, pp. 606–619, 2016.
- [93] M. Dabbagh, B. Hamdaoui, M. Guizani, and A. Rayes, “Software-defined networking security: pros and cons,” *IEEE Communications Magazine*, vol. 53, pp. 73–79, June 2015.
- [94] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, “Software-defined mobile networks security,” *Mobile Networks and Applications*, vol. 21, no. 5, pp. 729–743, 2016.
- [95] D. Forsberg, H. Leping, K. Tsuyoshi, and S. Alanara, “Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface,” in *2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1–5, Sept 2007.
- [96] D. Yu and W. Wen, “Non-access-stratum request attack in E-UTRAN,” in *2012 Computing, Communications and Applications Conference*, pp. 48–53, Jan 2012.

REFERENCES

- [97] M. Purkhiabani and A. Salahi, “Enhanced authentication and key agreement procedure of next generation evolved mobile networks,” in *2011 IEEE 3rd International Conference on Communication Software and Networks*, pp. 557–563, May 2011.
- [98] H. Mun, K. Han, and K. Kim, “3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA,” in *2009 Wireless Telecommunications Symposium*, pp. 1–8, April 2009.
- [99] C. K. Han and H. K. Choi, “Security Analysis of Handover Key Management in 4G LTE/SAE Networks,” *IEEE Transactions on Mobile Computing*, vol. 13, pp. 457–468, Feb 2014.
- [100] J. Cao, M. Ma, and H. Li, “Unified handover authentication between heterogeneous access systems in LTE networks,” in *2012 IEEE Global Communications Conference (GLOBECOM)*, pp. 5308–5313, Dec 2012.
- [101] C. K. Han, H. K. Choi, and I. H. Kim, “Building Femtocell More Secure with Improved Proxy Signature,” in *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, pp. 1–6, Nov 2009.
- [102] A. Mishra, M. H. Shin, N. L. Petroni, T. C. Clancy, and W. A. Arbaugh, “Proactive key distribution using neighbor graphs,” *IEEE Wireless Communications*, vol. 11, pp. 26–36, Feb 2004.
- [103] I. E. Bouabidi, I. Daly, and F. Zarai, “Secure handoff protocol in 3GPP LTE networks,” in *Third International Conference on Communications and Networking*, pp. 1–6, March 2012.
- [104] A. Bohk, L. Butryn, and L. Dra, “An authentication scheme for fast handover between WiFi access points,” in *Proc. of ACM Wireless Internet Conference (WICON)*, 2007.
- [105] R. Rajavelsamy and S. Choi, “Security aspects of inter-access system mobility between 3GPP and non-3GPP networks,” in *Communication Systems Software and*

REFERENCES

- Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on*, pp. 209–213, Jan 2008.
- [106] H. Wang and A. R. Prasad, “Fast authentication for inter-domain handover,” in *International Conference on Telecommunications*, pp. 973–982, Springer, 2004.
- [107] C. Zhang, R. Lu, P.-H. Ho, and A. Chen, “A location privacy preserving authentication scheme in vehicular networks,” in *2008 IEEE Wireless Communications and Networking Conference*, pp. 2543–2548, IEEE, 2008.
- [108] J. Choi and S. Jung, “A secure and efficient handover authentication based on light-weight Diffie-Hellman on mobile node in FMIPv6,” *IEICE transactions on communications*, vol. 91, no. 2, pp. 605–608, 2008.
- [109] Y. Zheng, D. He, L. Xu, and X. Tang, “Security scheme for 4G wireless systems,” in *Proceedings. 2005 International Conference on Communications, Circuits and Systems, 2005.*, vol. 1, pp. 397–401 Vol. 1, May 2005.
- [110] Y. Kim, W. Ren, J. Y. Jo, M. Yang, Y. Jiang, and J. Zheng, “Sfric: A secure fast roaming scheme in wireless lan using id-based cryptography,” in *2007 IEEE International Conference on Communications*, pp. 1570–1575, June 2007.
- [111] Q. Han, Y. Zhang, X. Chen, H. Li, and J. Quan, “Efficient and robust identity-based handoff authentication in wireless networks,” in *International Conference on Network and System Security*, pp. 180–191, Springer, 2012.
- [112] A.-N. Shen, S. Guo, D. Zeng, and M. Guizani, “A lightweight privacy-preserving protocol using chameleon hashing for secure vehicular communications,” in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 2543–2548, IEEE, 2012.
- [113] J. Choi and S. Jung, “A handover authentication using credentials based on chameleon hashing,” *IEEE communications letters*, vol. 14, no. 1, pp. 54–56, 2010.

REFERENCES

- [114] M. K. KHAN, “Cryptanalysis of a handover authentication scheme using credentials based on chameleon hashing,” *IEICE TRANSACTIONS on Information and Systems*, vol. 93, no. 12, pp. 3400–3402, 2010.
- [115] D. He, C. Chen, S. Chan, and J. Bu, “Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions,” *IEEE Transactions on Wireless Communications*, vol. 11, pp. 48–53, January 2012.
- [116] D. He, C. Chen, S. Chan, J. Bu, and L. T. Yang, “Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks,” *IEEE Transactions on Industrial Electronics*, vol. 60, pp. 5348–5354, Nov 2013.
- [117] S. L. Yeo, W. S. Yap, J. K. Liu, and M. Henricksen, “Comments on ”Analysis and Improvement of a Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions”,” *IEEE Communications Letters*, vol. 17, pp. 1521–1523, August 2013.
- [118] H.-s. ROH and S.-h. JUNG, “RSA-based proxy signature for media independent handover,” *()*, vol. 4, p. 012, 2010.
- [119] Q. Jing, Y. Zhang, A. Fu, and X. Liu, “A privacy preserving handover authentication scheme for EAP-based wireless networks,” in *Global Telecommunications Conference (GLOBECOM 2011)*, 2011 IEEE, pp. 1–6, IEEE, 2011.
- [120] C. Jin, L. Hui, *et al.*, “Handover authentication between different types of eNBs in LTE networks,” *The Journal of China Universities of Posts and Telecommunications*, vol. 20, no. 2, pp. 106–112, 2013.
- [121] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, “A simple and robust handover authentication between HeNB and eNB in LTE networks,” *Computer Networks*, vol. 56, no. 8, pp. 2119–2131, 2012.

REFERENCES

- [122] N. Krichene and N. Boudriga, “Securing Roaming and Vertical Handover in Fourth Generation Networks,” in *2009 Third International Conference on Network and System Security*, pp. 225–231, Oct 2009.
- [123] H. Song, X. Fang, and L. Yan, “Handover Scheme for 5G C/U Plane Split Heterogeneous Network in High-Speed Railway,” *IEEE Transactions on Vehicular Technology*, vol. 63, pp. 4633–4646, Nov 2014.
- [124] M. Boujelben, S. B. Rejeb, and S. Tabbane, “A novel green handover self-optimization algorithm for LTE-A / 5G HetNets,” in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 413–418, Aug 2015.
- [125] M. Boujelben, S. B. Rejeb, and S. Tabbane, “A novel mobility-based CoMP handover algorithm for LTE-A / 5G HetNets,” in *Software, Telecommunications and Computer Networks (SoftCOM), 2015 23rd International Conference on*, pp. 143–147, Sept 2015.
- [126] A. C. Morales, A. Aijaz, and T. Mahmoodi, “Taming Mobility Management Functions in 5G: Handover Functionality as a Service (FaaS),” in *2015 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–4, Dec 2015.
- [127] D. Kreutz, F. M. V. Ramos, P. E. Verssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey,” *Proceedings of the IEEE*, vol. 103, pp. 14–76, Jan 2015.
- [128] X. Duan and X. Wang, “Authentication handover and privacy protection in 5G het-nets using software-defined networking,” *IEEE Communications Magazine*, vol. 53, pp. 28–35, April 2015.
- [129] D. Gale and L. S. Shapley, “College admissions and the stability of marriage,” *The American Mathematical Monthly*, vol. 69, no. 1, pp. 9–15, 1962.

REFERENCES

- [130] M. Feng, S. Mao, and T. Jiang, “Joint duplex mode selection, channel allocation, and power control for full-duplex cognitive femtocell networks,” *Digital Communications and Networks*, vol. 1, no. 1, pp. 30–44, 2015.
- [131] A. Abdulkadiroglu and T. Sönmez, “Matching markets: Theory and practice,” *Advances in Economics and Econometrics*, vol. 1, pp. 3–47, 2013.
- [132] A. E. Roth, “Deferred acceptance algorithms: History, theory, practice, and open questions,” *International Journal of Game Theory*, vol. 36, no. 3-4, pp. 537–569, 2008.
- [133] H. Kim, K. Kim, Y. Han, and S. Yun, “A proportional fair scheduling for multicarrier transmission systems,” in *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, vol. 1, pp. 409–413, IEEE, 2004.
- [134] J. M. Holtzman, “Asymptotic analysis of proportional fair algorithm,” in *12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. PIMRC 2001. Proceedings (Cat. No.01TH8598)*, vol. 2, pp. F–33–F–37 vol.2, Sep 2001.
- [135] S. B. Lee, I. Pefkianakis, A. Meyerson, S. Xu, and S. Lu, “Proportional Fair Frequency-Domain Packet Scheduling for 3GPP LTE Uplink,” in *IEEE INFOCOM 2009*, pp. 2611–2615, April 2009.
- [136] R. Jain, D. Chiu, and W. Hawe, “A Quantitative Measure of Fairness And Discrimination For Resource Allocation In Shared Computer Systems,” *arXiv preprint cs/9809099*, 1998.
- [137] C. V. N. Index, “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper,” tech. rep., Tech. rep. Cisco, 2016. url: <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html>.

REFERENCES

- [138] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, “What will 5G be?,” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, 2014.
- [139] M. K. Arjmandi, “5G Overview: Key Technologies,” *Opportunities in 5G Networks: A Research and Development Perspective*, p. 19, 2016.
- [140] D. Center, “Samsung Electronics Co,” *Ltd.[2015] 5G vision, 16s. URL: <http://www.samsung.com/global/businessimages/insights/2015/Samsung-5G-Vision-0.pdf>*, 2015.
- [141] “5G Vision:The 5G Infrastructure Public Private Partnership:the next generation of communication networks and services., White Paper,” tech. rep., The 5G Infrastructure Public Private Partnership. url: <https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf>.
- [142] N. Panwar, S. Sharma, and A. K. Singh, “A survey on 5G: The next generation of mobile communication,” *Physical Communication*, vol. 18, pp. 64–84, 2016.
- [143] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.
- [144] D. R. Stinson, “Some Observations on the Theory of Cryptographic Hash Functions,” *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 259–277, 2006.
- [145] E. U. T. R. A. Network, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (gprs) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access,” 2011.
- [146] A. Ruia, C. J. Casey, S. Saha, and A. Sprintson, “Flowcache: A cache-based approach for improving SDN scalability,” in *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 610–615, April 2016.

REFERENCES

- [147] X. Wang, M. Chen, T. Taleb, A. Ksentini, and V. C. M. Leung, “Cache in the air: exploiting content caching and delivery techniques for 5G systems,” *IEEE Communications Magazine*, vol. 52, pp. 131–139, February 2014.
- [148] M. Burrows, M. Abadi, and R. M. Needham, “A logic of authentication,” in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 426, pp. 233–271, The Royal Society, 1989.
- [149] K. Gaarder and E. Sneekenes, “Applying a formal analysis technique to the CCITT X. 509 strong two-way authentication protocol,” *Journal of cryptology*, vol. 3, no. 2, pp. 81–98, 1991.
- [150] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, *et al.*, “The AVISPA tool for the automated validation of internet security protocols and applications,” in *International Conference on Computer Aided Verification*, pp. 281–285, Springer, 2005.
- [151] Y. Glouche, T. Genet, O. Heen, and O. Courtay, “A security protocol animator tool for AVISPA,” in *ARTIST2 workshop on security specification and verification of embedded systems, Pisa*, p. 12, 2006.
- [152] E. A. Young, T. J. Hudson, and R. Engelschall, “Openssl: The open source toolkit for ssl/tls,” 2011.
- [153] F. Fainelli, “The Openwrt embedded development framework,” in *Proceedings of the Free and Open Source Software Developers European Meeting*, 2008.
- [154] J. Choi and S. Jung, “A handover authentication using credentials based on chameleon hashing,” *IEEE Communications Letters*, vol. 14, pp. 54–56, January 2010.

REFERENCES

- [155] J. Cao, M. Ma, and H. Li, “An Uniform Handover Authentication between E-UTRAN and Non-3GPP Access Networks,” *IEEE Transactions on Wireless Communications*, vol. 11, pp. 3644–3650, October 2012.
- [156] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, “A Survey on Security Aspects for LTE and LTE-A Networks,” *IEEE Communications Surveys Tutorials*, vol. 16, pp. 283–302, First 2014.
- [157] M. C. Muoz, M. Moh, and T. S. Moh, “Improving smart grid authentication using Merkle Trees,” in *2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS)*, pp. 793–798, Dec 2014.
- [158] D. Basin, S. Mödersheim, and L. Vigano, “An on-the-fly model-checker for security protocol analysis,” in *European Symposium on Research in Computer Security*, pp. 253–270, Springer, 2003.
- [159] “3GPP TS 33.401 V11.5.0 , Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Rel 11),” 2012.
- [160] “3GPP TS 36.300 V11.3.0, Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); overall description;(Rel 11),” 2012.
- [161] L. Cai, S. Machiraju, and H. Chen, “CapAuth: A Capability-based Handover Scheme,” in *2010 Proceedings IEEE INFOCOM*, pp. 1–5, March 2010.
- [162] G. Yang, Q. Huang, D. S. Wong, and X. Deng, “Universal authentication protocols for anonymous wireless communications,” *IEEE Transactions on Wireless Communications*, vol. 9, pp. 168–174, January 2010.
- [163] M. J. Alam and M. Ma, “Resource Matching in Carrier Aggregation Enabling 5G Networks,” *Wireless Personal Communications*, pp. 1–20, 2016.

REFERENCES

- [164] M. J. Alam and M. Ma, “Pareto Efficient Resource Matching for LTE-A System,” in *2015 10th International Conference on Information, Communications and Signal Processing (ICICS)*, pp. 1–5, Dec 2015.
- [165] M. J. Alam and M. Ma, “Radio Resource Management by Evolutionary Algorithms for 4G LTE-Advanced Networks,” in *Bio-Inspired Computation in Telecommunications*, pp. 141–162, Morgan Kaufmann, 2015.