



*AIN SHAMS UNIVERSITY  
FACULTY OF ENGINEERING  
CAIRO - EGYPT*

*Electronics and Communication Engineering  
Department*

**Cryptographic Authentication Protocol for Handover  
in 5G Mobile Network**

Dissertation submitted to the faculty of Engineering – Ain-Shams  
University in partial fulfilled of the requirements for the degree of  
Master of Science in Electrical Engineering

*Submitted By*

**Eng. Mohamed Said Abdelhady Ibrahim**  
*Electronics and Communication Eng. Department  
Faculty of Engineering - Ain-Shams University*

*Supervised By*

**Prof. Dr. Wagdy Anis**

Professor in Electronics and Communication Eng. Department  
Faculty of Engineering – Ain-Shams University (ASU)  
Cairo – Egypt

**Ass. Prof. Dr. Ahmed Ali Abdel-hafez**

Communications Department  
Military Technical Collage (MTC)  
Cairo – Egypt

**Dr. Haitham Mohamed El-demerdash**

Communications Department  
Military Technical Collage (MTC)  
Cairo – Egypt



*AIN SHAMS UNIVERSTY  
FACULTY OF ENGINEERING  
CAIRO - EGYPT*

*Examiners Committee*

*Name : Mohamed Saïd Abdelhady Ibrahim*

**Thesis** : Cryptographic Authentication Protocol For  
Handover in 5G Mobile Network

**Degree:** Master of Science

*Name, Title, and Affiliate    Signature*

1. *Prof. Dr. Talat Abdellatif Ibrahim Elgarf*  
*..... Professor of Communication in Higher*  
*Technological Institute (HTI)*
2. *Prof. Dr. Ismail Mohamed hafz*  
*..... professor in Electronics and*  
*Communication Eng. Department (ASU)*
3. *Prof. Dr. Wagdy Refaat Anis*                    *.....*  
*Professor in Electronics and Communication*  
*Eng. Department (ASU)*

*Date: 22 / 8 / 2020*

## *STATEMENT*

*This dissertation is submitted to Ain Shams University in partial fulfillment of the degree of Master of Philosophy in Electrical Engineering.*

*The work included in this dissertation was out by the author in the department of electronics and Communication Engineering, Ain Shams University.*

*No part of this dissertation has been submitted for a degree or qualification at other university or institution.*

*Name: Mohamed Saïd Abdelhady Ibrahim*

*Signature: .....*

*Date : 22 / 8 / 2020*

## *Abstract*

The massive increasing of the exchanging data, number of users, new applications, and the shortage of the current usable spectrum (several hundred megahertz and a few gigahertz) in the existing 4G mobile network led to think in exploiting millimeter wave (mm-Wave) spectrum for the next generation 5G mobile networks.

MM-Wave spectrum occupies the band from 30~300 GHz and this will require new architecture in 5G network with dense small scale cells provided with Base Stations (BS) equipped with Massive Multiple Input Multiple Output (Massive-MIMO) antennas due to the short propagation range and the needing for line-of-sight paths for mm-waves.

This new architecture achieves some advantages like better spectral allocations, increasing no. of users and no. of connected devices, expanding the application of Internet of Things (IoT) technology but also brings new difficult tasks in security provisioning, new stringent latency requirements and potential risk of some security attacks.

Impersonation and Man-in-the-Middle (MitM) attacks are examples of security attacks which will threaten security in 5G network due to the probable frequent handovers and authentication processes between User Equipment (UE) and base stations in dense small scale cells architecture.

So we propose a comprehensive solution for key generation and user handover authentication protocol for 5G mobile networks to mitigate these attacks by merging between non-cryptographic and cryptographic security techniques.

The key generation and handover authentication protocol depends on exploiting physical layer attributes Angle of Arrival (AoA) by using Multiple Signal Classification (MUSIC) algorithm to estimate (AoA).

The assessment and simulation for our protocol prove its strength and immunity against (MitM) attack using (AVISPA) tool and impersonation attack using (MATLAB) tool, with no extra communications overheads, with tolerable delay of estimation process.

## *Acknowledgement*

First and Foremost I would like to thank ALLAH — the Ever-Living and the Sustainer of all existence, the One that neither begets nor is born and nor is there to Him any equivalent.

I feel honored to record my deepest sense of gratitude and thanks to my supervisors:

**Prof. Dr. Wagdy Anis (ASU)**

**Prig. Ass. Prof. Ahmed Ali Abdel-Hafez (Egyptian Armed Forces)**

**Dr. Haitham Mohamed El-demerdash (Egyptian Armed Forces)**

Thanks for their supervision, guidance, generous advice, criticism, and continuous encouragement throughout this research.

Many thanks go to my commander general. Ass. Prof. Ahmed Aly Abd El-Hafez for his advice, for the open door policy and for many useful feedbacks during the writing of this dissertation. I believe that your supervision has allowed me to grow up as a researcher.

Finally, I would like to thank my family to whom I owe a great deal. To **my father, my mother, my wife and my children, my sisters.**

I apologize for my wife and my children for all the long nights and weekends, and holidays which I missed. Thanks for your endless support, encouragement, understanding and helping me through all my work.

**Dear .... Thanks for all ....**

*Mohamed said Abdelhady*

## List of Acronyms

### *Abbreviation*

5G	5 <sup>TH</sup> Generation Mobile Network
LTE-A	Long Term Evolution-Advanced
CDMA	Code Division Multiple Access
MIMO	Multiple-Input, Multiple - Output
CoMP	Coordinated Multi-Point
CA	Carrier Aggregation
HetNet	Heterogeneous Network
MitM	Man-In-The-Middle Attack
AOA	Angle Of Arrival
TEK	Transmission Encryption Key
BS	Base Station
UE	User Equipment
$\Theta_{EXP}$	Expected Range
IMT	International Mobile Telecommunications
PCS	Personal Communications Service
GSM	Global Systems for Mobile communications
MMS	Multimedia Messages
IP	Internet Protocol
IOT	Internet of Things
MMTC	Massive Machine Type Communications

URLLC	Ultra-reliable and Low-latency Communications
mm- Wave	Millimeter Wave
QOS	Quality of Service
UDN	Ultra-Dense Network
DOS	Denial Of Service
DDOS	Distributed Denial Of Service
FHSS	Frequency Hopping Spread Spectrum
DSSS	Direct Sequence Spread Spectrum
WLANs	Wireless Local Area Networks
SHA	Secure Hash Algorithm
FS	Forward Secrecy
3GPP	3rd Generation Partnership Project
RSS	Received Signal Strength
EAP/AKA	Extensible Authentication Protocol-Authentication and Key Agreement
MD5	Message-Digest Algorithm
PLS	Physical Layer Security
MME	Mobility Management Entity
ULA	Uniform Linear Array
OFDM	Orthogonal Frequency-Division
LOS	Multiplexing
DOA	Line Of Sight
MUSIC	Direction Of Arrival
	Multiple Signal Classification
ACK	Acknowledgment

## List of Symbols

### Symbol

$n_s$	Symbol Index
$+$	Addition
$n_p$	Packet Number
$n_{sc}$	Subcarrier Index
$P$	Maximum Power
$\leq$	Less Than Or Equal
$\in$	Belongs to
$\forall$	For all
$\dagger$	Conjugate Transpose
$\text{tr}$	Matrix Trace Operator
$E[.]$	Expectation Operator

# Table of Contents

<b>STATEMENT</b> .....	<b>iv</b>
<b>Abstract</b> .....	<b>v-vi</b>
<b>Acknowledgement</b> .....	<b>vii</b>
<b>List of Acronyms</b> .....	<b>viii-ix</b>
<b>List of Symbols</b> .....	<b>x</b>
<b>Table of Contents</b> .....	<b>xi</b>
<b>List of Figures</b> .....	<b>xiv-xv</b>
<b>List of Tables</b> .....	<b>xvii</b>
<b>CHAPTER 1</b>	
<b>Introduction</b> .....	<b>1</b>
1.1 Overview.....	1
1.2 Problem Statement.....	3
1.3 Solution Overview.....	3
1.4 Related Work.....	4
1.5 Publications.....	7
1.6 Thesis Organization.....	8
<b>CHAPTER 2</b>	
<b>5<sup>TH</sup> generation mobile network</b> .....	<b>9</b>
<b>2.1 Introduction</b> .....	<b>9</b>
Evolution of Mobile Wireless Technologies.....	9
2.2.1 First Generation (1G).....	10
2.2.2 Second Generation (2G).....	11
2.2.3 Third Generation (3G).....	11
2.2.4 Fourth Generation (4G).....	11
2.3 (5G) Mobile Network.....	12
2.3.1 (5G) vs (4G) capabilities.....	14
2.3.2 Benefits of (5G).....	14
2.4 (5G) Network Architecture.....	15
2.5 Main Components for 5G Network.....	17
2.5.1 Millimeter Waves.....	17
2.5.2 Massive MIMO.....	18
2.5.3 <b>Heterogeneous Network (HetNet)</b> .....	<b>18</b>
Summary.....	19
<b>CHAPTER 3</b>	
<b>Wireless Network Security and Security Provisioning for 5G mobile network</b> .....	<b>20</b>

3.1	Introduction.....	20
3.2	Security attacks.....	20
3.2.1	Common Security attacks.....	21
3.3	Some attacks in 5G Mobile Network.....	22
3.4	Network Security Aspects.....	28
3.4.1	Access control.....	28
3.4.2	Authentication.....	29
3.4.3	Confidentiality.....	30
3.4.4	Data integrity.....	30
3.4.5	Non-Repudiation.....	31
3.4.6	Availability.....	31
3.4.7	Security Mechanisms.....	31
3.4.8	Key Management.....	32
3.5	Security Challenges in 5G Mobile Network.....	34
3.6	Security Provisioning in Handover Process in 5G Mobile Network .....	35
3.7	Cryptographic Techniques.....	37
3.7.1	Types of Cryptographic Techniques.....	37
3.7.2	Common Cryptographic Pitfalls.....	37
3.8	Non-Cryptographic Techniques (Physical Layer Security (PLS)).....	43
3.9	Summary.....	45

## **CHAPTER 4**

	<b>Proposed Protocol for Secure Handover Authentication for (5G) Mobile Network.....</b>	<b>46</b>
4.1	Introduction.....	46
4.2	New Technology, Structure and Requirements for 5G Network.....	46
4.3	Proposed Protocol Goal.....	47
4.4	System Model.....	50
4.4.1	System Model Description.....	50
4.4.2	AOA Estimation.....	53
4.4.3	MUSIC Algorithm to Estimate Angle of Arrival.....	54
4.4.4	Examples of Pseudo Spectrum Calculation with different values of SNR and Different Directions Using MUSIC Algorithm.....	56
4.6	Proposed Protocol Description.....	58

Summary.....	61
<b>CHAPTER 5</b>	
<b>SECURITY ASSESMENT OF THE POSEDPROTOCO.....</b>	<b>62</b>
5.1 Introduction.....	62
5.2 Attack Model.....	63
5.3 Security Assessment to the proposed Protocol.....	62
5.3.1 Security Assessment to the Proposed Protocol against MITM Attack Using AVISPA.....	63
5.3.2 Security Assessment to the proposed Protocol against Impersonation Attack Using MATLAB.....	73
5.4 Summary.....	81
<b>CHAPTER 6</b>	
<b>Conclusion and Future Work.....</b>	<b>82</b>
6.1 Conclusions.....	82
6.2 Future Work.....	82
<b>References.....</b>	<b>84</b>

## List of Figures

<b>Fig. No.</b>	<b>Title</b>	<b>Page No.</b>
Figure 1.1	Mutual Authentication during Handover with participation of AAA server.....	5
Figure 1.2.	Mutual Authentication during Handover with participation .....	5
Figure 1.3	Handover Authentication using security context based schemes.....	6
Figure 1.4	cross-layer handover authentication mechanism.....	7
Figure 2.1	Evolution of Wireless Technologies.....;	10
Figure 2.2	Penetration of MM-wave.....	14
Figure 2.3	General (5G) Mobile Network Architecture .....	16
Figure 2.4	mm-wave spectrum.....,	17
Figure 2.5	Overview System for (5G) Network.....	18
Figure 2.6	Network architecture combining and MMIMO and mm-Wave.....	19
Figure 3.1	Common Security Attacks on Networks .....	22
Figure 3.2	Attacks in 5G wireless networks (a). Eavesdropping (b). Jamming (c). DDoS (d). MITM.....	23
Figure 3.3	Impersonation Attack.....	27
Figure 3.4	Mutual Authentication during Handover between the User and a New Network (procedure 1) and Within the Same Network (procedure 2).....	37

Figure 3.5 Symmetric Encryption .....	39
Figure 3.6 Asymmetric Encryption.....	40
Figure 3.7 Steganography.....	41
Figure 3.8 Hashing.....	42
Figure 4.1 System Model.....	50
Figure 4.2 Structure of an Antenna Array.....	54
Figure 4.3 Pseudo Spectrum at $\theta = 40^\circ$ and SNR = 5 dB.....	57
Figure 4.4 Pseudo Spectrum at $\theta = 60^\circ$ and SNR = 10 d.....	58
Figure 4.5 Proposed Protocol.....	60
Figure 5.1 AVISPA Tool Architecture.....	64
Figure 5.2 CAS Description for Proposed Scheme.....	68
Figure 5.3 OFMC Model Checker Result.....	70
Figure 5.4 CL-ATSE Attacks Searcher Result.....	70
Figure 5.5 Protocol Complete Run.....	71
Figure 5.6 Attack Trace.....	72
Figure 5.7 Attacker's Gained Information.....	73
Figure 5.8 PD as a Function of SNR for UE Located at 20.....	75
Figure 5.9 PD as a function of SNR for UE located at $80^\circ$ .....	76
Figure 5.10 PF as a function of SNR for an attacker located at 19.5° .....	77
Figure 5.11 PF as a function of SNR for an attacker located at 81° .....	78
Figure. 5.12. Chart Represents the percentage of 1000 beacon messages that have been declared as authorized or unauthorized for different transmit directions.....	80