AIN SHAMS UNIVERSTY
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 Said 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 Said 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 threat 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^{TH} 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
Θ_{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 Multiplexing
LOS	Line Of Sight
DOA	Direction Of Arrival
MUSIC	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
≤	Less Than Or Equal
∈	Belongs to
∀	For all
†	Conjugate Transpose
tr	Matrix Trace Operator
E[.]	Expectation Operator

Table of Contents

List of Figures

Fig. No. Title Page No.