

# **Evaluation of a New Authentication and Key Agreement Protocol for 5G Network**

**Zakaria Benfarhi**

Final International University  
February 2024  
Girne, TRNC

# **Evaluation of a New Authentication and Key Agreement Protocol for 5G Network**

by

**Zakaria Benfarhi**

A thesis submitted to the Institute of Graduate Studies  
in partial fulfillment of the requirements for the Degree of  
Master of Science  
in  
Software Engineering

Final International University  
February 2024  
Girne, TRNC



**FINAL INTERNATIONAL UNIVERSITY  
INSTITUTE OF GRADUATE STUDIES**

**APPROVAL**

Title: Evaluation of a New Authentication and Key Agreement Protocol for 5G Network

We certify that we approve this thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Software Engineering.

Approval of the Examining Committee:

Prof. Dr. Orhan GEMIKONAKLI  
(Supervisor)

Prof. Dr. Enver EVER

Assist. Prof. Dr. Hüseyin LORT

Assist. Prof. Dr. Mostafa Ayoubi  
MOBARHAN  
(Co-supervisor)

Assist. Prof. Dr. Ibrahim ADESHOLA

Approval of the Institute of Graduate Studies:

Prof. Dr. Nilgün SARP  
Director

Zakaria Benfarhi

Zakaria.benfarhi@final.edu.tr

ORCID iD: 0009-0000-5559-8810

© Zakaria Benfarhi 2024

## DEDICATION

*To my beloved parents and brothers, Dr. Said and Ms. Raja, whose unwavering support, guidance, and belief in me have been the bedrock of my journey, this work is for you.*

*You have taught me the value of hard work and perseverance, and for that, I am eternally grateful. To my brothers Amr, Marouane, and Mohammed. Your constant encouragement and faith in me have been invaluable and priceless.*

*I would also like to express my profound appreciation to my esteemed supervisors, Prof. Dr. Orhan Gemikonakli and Assist. Prof. Dr. Mostafa Ayoubi Mobarhan as well as to all of my lecturers. Your guidance, time, patience, mentorship, and expertise have been instrumental in shaping this study, and my academic, professional, and personal paths.*

*Lastly, I wish to acknowledge all the members of the university community. Their dedication to learning and growth has truly enriched my academic experience.*

*This thesis stands as a testament to the collective effort, wisdom, and spirit of all who have touched my academic journey.*

*With this in mind, I dedicate this thesis to you all. Thank you for playing a part in this significant chapter of my life.*

## **ETHICAL DECLARATION**

I, Zakaria Benfarhi, hereby, declare that I am the sole author of this thesis and it is my original work. I declare that I have followed ethical standards in collecting and analyzing the data and accurately reported the findings in this thesis. I have also properly credited and cited all the sources included in this work.

Zakaria Benfarhi

# ABSTRACT

In recent decades, wireless communication systems have undergone significant development, leading to the emergence of the transformative 5G network. Acknowledged for its high-speed download rates, minimized end-to-end delay, and seamless integration of cutting-edge network solutions, the 5G system stands as a cornerstone for real-time applications like IoT and M2M communications. However, like its predecessors 4G-LTE and 3G, the 5G network faces persistent security challenges, encompassing authentication mechanisms, privacy concerns, and potential threats such as DoS and DDoS attacks, MitM attacks, and eavesdropping.

This research delves into and better understands the intricate security challenges inherent in the 5<sup>th</sup> generation, focusing on designing and implementing the Efficient and Strong AKA (ES-AKA) protocol. The selection of 5G as the research focal point is motivated not only by the need to comprehensively explore and address security concerns but also by the multifaceted opportunities it presents. The ubiquitous integration of 5G in diverse sectors, such as the IoT and critical infrastructure, amplifies the urgency of a robust security framework. Moreover, the transformative potential of 5G in fostering technological innovation, economic growth, and societal advancements underscores the importance of fortifying its security architecture. The ES-AKA protocol, meticulously crafted for robustness and effectiveness, undergoes comprehensive implementation, leveraging the advanced capabilities of AVISPA Tools. Findings from the testing phase, conducted using state-of-the-art Offline Model-Checker (OFMC) and CL-based Attack Searcher (CL-AtSe) back ends, are compared with extensive literature reviews for performance evaluation such as resilient to all known attacks, including ToRPEDO, Jamming, Bogus Serving Node, and Reply attacks, etc., metrics such as communication overhead, computational overhead, and signalling messages and security properties, including confidentiality, integrity, mutual authentication, key exchange, and optimized handover, etc. Furthermore, this dissertation aims to enhance the security of 5G networks by thoroughly examining and proactively addressing potential security issues. The goal is to contribute not only to the protection of digital communications but also to foster a sustainable and secure evolution of the interconnected world. The proposed ES-AKA

model specifically addresses security challenges M2M communications as well. Additionally, a key finding of this research is that, upon studying various proposed protocols/methods, none of them demonstrates resilience against known attacks, including DoS/DDoS, MitM, eavesdropping, impersonation, etc. While maintaining practicality.

In essence, this research embarks on an expedition into the realm of secure communication protocols – the standardized AKA and EAP-AKA protocols vulnerable to the mentioned attacks, navigating through the design and implementation of the ES-AKA protocol. With AVISPA Tools serving as a guiding compass, the ES-AKA protocol is not only meticulously crafted but also subjected to rigorous testing using the advanced capabilities of AVISPA, particularly through the OFMC and CL-AtSe back ends. This comprehensive approach ensures the development and thorough evaluation of the protocol, addressing the challenges presented by the 5G network. However, it is crucial to acknowledge that this solution, while effective against current threats, may face challenges in the near future. The ever-evolving landscape of cybersecurity and attack techniques necessitates ongoing refinement. The complexity of the solution and the diverse array of involved parties may pose challenges in adapting to upcoming threats. Continuous vigilance and adaptation will be essential to ensure the enduring efficacy of the proposed solution.

**Keywords:** 5G Network, 5G-AKA, vulnerabilities, security, authentication, protocol, DoS attacks, MitM attacks, eavesdropping, AVISPA.



## ÖZ

Son yıllarda kablosuz iletişim sistemlerinde, iletişim teknolojilerini dönüştüren 5G ağının ortaya çıkmasına yol açan önemli gelişmeler yaşandı. Yüksek veri indirme hızları, asgari düzeylere indirilmiş uçtan uca gecikme ve son teknoloji ağ çözümlerinin kusursuz entegrasyonu ile 5G sistemi, Nesnelerin İnterneti (IoT) ve cihazlar/makineler arası (M2M) iletişim gibi gerçek zamanlı uygulamalar için bir temel oluşturmuştur. Ancak, öncülleri 4G-LTE ve 3G teknolojileri gibi 5G ağı da kimlik doğrulama mekanizmaları, gizlilik kaygıları ve potansiyel DoS ve DDoS saldırıları, MitM saldırıları ve gizlice dinleme gibi güvenlik tehditleri ile karşı karşıyadır.

Bu araştırma, 5. kuşağın doğasında olan karmaşık güvenlik sorunlarını derinlemesine inceleyip daha iyi anlayarak, verimli ve güçlü AKA (ES-AKA) protokolünü tasarlayıp geliştirmeyi temel alıyor. Araştırmanın odak noktası olarak 5G'nin seçilmesi yalnızca güvenliği kapsamlı bir şekilde inceleme ve ele alma ihtiyacından kaynaklanmaz, 5G'nin sunduğu çok yönlü fırsatlar da bir motivasyon kaynağıdır. Hayatın her alanında yerini alan 5G'nin IoT ve kritik altyapı gibi çeşitli sektörlere entegrasyonu, sağlam bir güvenlik çerçevesini de acil kılmaktadır. Üstelik, 5G'nin teknolojik yeniliği, ekonomik büyümeyi ve toplumsal ilerlemeyi teşvik etmedeki dönüştürücü potansiyeli dikkate alındığında, 5G güvenlik mimarisini güçlendirmenin önemi daha da belirginleşiyor. ES-AKA protokolü, sağlamlık ve etkililik için titizlikle hazırlanmış olup AVISPA Araçlarının gelişmiş özelliklerinden yararlanarak kapsamlı testlerden geçirilir. Son teknoloji ürünü Offline Model-Checker (OFMC) kullanılarak gerçekleştirilen test aşaması ve CL tabanlı Saldırı Arayıcılarca (CL-AtSe) ağ sınırlarından elde edilen bulgular, iletişim yükü, hesaplama yükü ve sinyal mesajları, güvenlik ve gizlilik, bütünlük, karşılıklı kimlik doğrulama, anahtar değişimi ve optimize edilmiş alıcı-vericiler arası sinyal aktarımı vb. gibi metrikleri içeren kapsamlı bir literatür taramasıyla, ToRPEDO, Jamming, Bogus Serving Node ve Reply saldırıları vb. dahil olmak üzere bilinen tüm saldırılara karşı dayanıklılık gibi performans değerlendirmesi açısından kıyaslanmıştır. Ayrıca, bu çalışma, potansiyel güvenlik sorunlarını kapsamlı bir şekilde inceleyip proaktif bir şekilde ele alarak 5G ağlarının güvenliğini geliştirmeyi amaçlar. Amaç yalnızca dijital iletişimin korunmasına katkıda bulunmak değil, aynı zamanda

birbirine bağılı dünyanın sürdürülebilir ve güvenli bir evrimini teşvik etmektir. Önerilen ES-AKA modeli M2M iletişimde güvenlik sorunlarını da özellikle ele alıyor. Bu araştırmanın en önemli bulgusu şudur: Önerilen çeşitli protokoller/yöntemler araştırılıp incelendiği zaman, bunların hiçbirinin, pratik kullanımdan taviz vermeden, bilinen DoS/DDoS, MitM, gizlice dinleme, kimliğe bürünme vb. saldırılara karşı dayanıklılık göstermediği görülüyor.

Özünde, bu araştırma güvenli iletişim protokollerine doğru bir keşif gezisidir – yukarıda sözü edilen saldırılara karşı savunmasız, standartlaştırılmış AKA ve EAP-AKA protokolleri, ES-AKA protokolünün tasarımı ve uygulanmasında bir yolculuktur. AVISPA Araçlarının yol gösterici bir pusula görevi görmesi ile ES-AKA Protokolü yalnızca titizlikle oluşturulmaz, aynı zamanda AVISPA'nın özellikle OFMC ve CL-AtSe desteği aracılığıyla gelişmiş yetenekleri kullanılarak sıkı testlere de tabi tutulur. Bu kapsamlı yaklaşım, protokolün, 5G ağının sergilediği zorlukların kapsamlı bir şekilde değerlendirilmesini de sağlar. Ancak, bu çözümün mevcut tehditlere karşı etkili olmasına rağmen, yakın gelecekte zorluklarla karşılaşabileceğinin bilinmesi de önemlidir. Sürekli gelişen siber güvenlik ortamı ve saldırı teknikleri çözümlerde de sürekli iyileştirme gerektirir. Çözümün karmaşıklığı ve ilgili tarafların çeşitliliği, yaklaşmakta olan tehditlere uyum sağlamada zorluklar yaratabilir. Önerilen çözümün etkinliğinin kalıcı olabilmesi için sürekli dikkat ve adaptasyon gerekli olacaktır.

**Anahtar Kelimeler:** 5G Ağı, 5G-AKA, güvenlik açıkları, güvenlik, kimlik doğrulama, protokol, DoS saldırıları, MitM saldırıları, gizlice dinleme, AVISPA.

# TABLE OF CONTENTS

DEDICATION .....	v
ETHICAL DECLARATION .....	vi
ABSTRACT .....	vii
ÖZ .....	ix
LIST OF TABLES .....	xiii
LIST OF FIGURES .....	xiv
LIST OF APPENDICES .....	xv
LIST OF ABBREVIATIONS .....	xvi
CHAPTER 1 .....	1
INTRODUCTION .....	1
1.1 Problem Statement .....	2
1.2 Purpose of the Study .....	4
1.3 Significance of the Study .....	5
1.4 Research Questions and Hypotheses .....	6
1.5 Assumptions .....	7
1.6 Limitations .....	8
1.7 Definition of Key Terminology .....	9
1.7.1 Basic Key Terms .....	9
1.7.2 The 5G Architecture Components .....	11
1.7.3 The 5G-AKA Architecture Components .....	11
1.7.4 Security Threats in the 5G-AKA Protocol .....	12
CHAPTER 2 .....	15
LITERATURE REVIEW .....	15
2.1 Related Works .....	15
2.2 Verification Tools .....	29
CHAPTER 3 .....	35
ARCHITECTURE OF MACHINE-TO-MACHINE WITHIN 5G NETWORKS .....	35
CHAPTER 4 .....	41
5G NETWORK, AKA PROTOCOL, AND SECURITY CONCERNS .....	41

4.1 The 5G Architecture .....	41
4.2 The 5G-AKA and EAP-AKA Protocol Architectures.....	46
4.2.1 The 5G-AKA Protocol.....	50
4.2.2 EAP-AKA Protocol.....	50
4.3 5G Network Security: Loopholes and Services.....	52
CHAPTER 5 .....	60
PROPOSED PROTOCOL: ES-AKA METHOD .....	60
5.1 Full Description of the Proposed Protocol.....	61
5.2 A Detailed Description of the 10 Steps Involved Within the .....	63
Authentication Process .....	63
CHAPTER 6 .....	67
PROOF OF SECURITY REQUIREMENTS .....	67
CHAPTER 7 .....	79
PERFORMANCE EVALUATION OF THE ES-AKA PROTOCOL.....	79
7.1 Communication Overhead.....	79
7.2 Signaling Messages .....	80
CONCLUSION.....	82
REFERENCES .....	85
APPENDICES .....	92

## LIST OF TABLES

Table 1 A Comprehensive Analysis: Exploring Security and Performance Enhancements in 5G-AKA Protocols .....	24
Table 2 Tools being either used to Implement or Evaluate the Proposed Protocols.....	34
Table 3 Parameters of the ES-AKA Protocol .....	62
Table 4 Evaluation of the Resilience of Each Approach to various Forms of Attacks....	70
Table 5 Evaluation of a Security Approach According to Specified Characteristics .....	71

# LIST OF FIGURES

Figure 1 SPAN Interface.....	29
Figure 2 The Four Backends of AVISPA .....	30
Figure 3 Scyther Verification System .....	31
Figure 4 Architecture of the M2M Communication .....	36
Figure 5 Architecture of the 5G Network .....	42
Figure 6 Network Architecture.....	45
Figure 7 Subscriber Mobility Communication Architecture .....	46
Figure 8 The 5G Units in the Authentication Mechanism.....	48
Figure 9 The 5G-AKA Protocol's Timeline Diagram .....	49
Figure 10 The EAP-AKA Protocol's Timeline Diagram .....	51
Figure 11 Traditional Authentication Architecture.....	51
Figure 12 Attacks in 5G Networks.....	57
Figure 13 Timeline Diagram of the Proposed Protocol .....	60
Figure 14 OFMC Back-end's Outcome.....	74
Figure 15 CL-AtSe Back-end's Outcome .....	76
Figure 16 Attack Simulation's Outcome .....	77
Figure 17 Signaling Message Comparison .....	80

# LIST OF APPENDICES

APPENDIX A UE's Role in the ES-AKA Protocol.....	93
APPENDIX B Session Role of the Proposed Protocol .....	95
APPENDIX C Environment Function .....	96
APPENDIX D Secrecy and Authentication Goals.....	96
APPENDIX E Definition of Secrecy and Authentication Goals .....	98
APPENDIX F Turinit Report .....	101

## LIST OF ABBREVIATIONS

3G, 4G, 5G	3 <sup>rd</sup> , 4 <sup>th</sup> , 5 <sup>th</sup> Generation(s)
3GPP	3 <sup>rd</sup> Generation Partnership Project
4G-LTE	4G Long-Term Evolution
5GC	5G Core
5G-VANET	Vehicular Ad Hoc Networks in the 5G context
AAA	Authentication, Authorization, and Accounting
AK	Anonymity Key
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
API	Application Programming Interface
ARPF	Access and Mobility Management Policy Control Function
AUSF	Authentication Server Function
AUTN	Authentication Token
AV	Authentication Vector
AVISPA	Automated Validation of Internet Security Protocols and Applications
BAN Logic	Burrows-Abadi-Needham
CAS	Combinatorial Analysis of Security Protocols
CCN	Cloud Computing Network
CCU	Central Control Unit
CK	Confidentiality Key
CL-AtSe	CL-based Attack Searcher
CIA	Confidentiality, Integrity, and Availability
CN	Core Network
COVID-19	Coronavirus Disease 2019
CP	Control Plane
CRC	Cyclic Redundancy Check
CPU	Central Processing Unit
D2D	Device-to-Device
DPM	Dependability Performance Measure
DL	Deep Learning
DNS	Domain Name System
DoS/DDoS	Denial-of-Service / Distributed DoS
DSP	Diameter Signal Protocol



DSSS	Direct Sequence Hopping Spread Spectrum
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
ECIES	Elliptic Curve Integrated Encryption Scheme
eMBB	Enhanced Mobile BroadBand
eNB	Evolved NodeB
ES-AKA	Efficient and Strong AKA
FBS	False Base Station
FHSS	Frequency Hopping Spread Spectrum
gNB	gNodeB
gNB-CU	Centralized Unit
gNB-DU	Distributed Unit
gNB-RU	Remote Unit
HCN	Heterogeneous Core Network
HLPSL	High Level Protocol Specification Language
HLR	Home Location Register
HN	Home Network
HSS	Home Subscriber Server
IK	Integrity Key
IKEV2	Internet Key Exchange version 2
IoT	Internet-of-Things
IT	Information Technology
LDA	Latent Dirichlet Allocation
M2M	Machine-to-Machine
MAC	Media Access Control
MD	Machine type Device
MEC	Multi-Entity Credential
MIMO	Multiple Input Multiple Output
MITM	Man-in-the-Middle
MSR-DoS	Modular Square Route DoS
N3IWF	Non-3GPP Interworking Function
NEF	Network Exposure Function
NLP	Natural Language Processing
NP	Neyman-Pearson
NG-RAN	New Generation Radio Access Network
NRF	Network Repository Function
OFMC	Offline Model Checker
ONOS	Open Network Operating System

PaaS	Platform as a Service
PCF	Policy Control Function
PCIF	Policy and Charging Information Function
PDN	Packet Data Network
PLS	Physical Layer Security
PS	Public Safety
QoS	Quality of Service
RAND	Random
SA	Stand Alone
SATMC	SAT-based Model-Checker
SBA	Service Based Architecture
SCA	Spectral Collision Avoidance
SEAF	Security Anchor Function
SEPP	Security Edge Protection Profile
SIDF	Subscription Identifier De-concealment Function
SIM	Subscriber Identity Module
SPAN	Security Protocol Analyzer
SPDL	Security Protocol Description Language
SQN	Sequence Number
SSL	Secure Sockets Layer
SUCI	Subscriber Concealed Identifier
SUPI	Subscriber Permanent Identifier
TA4SP	Timed Automata for Security Protocols
TCPS	Transportation Cyber-Physical Security
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UNI	Universal Network Interface
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communication
USIM	Universal / Subscriber Identity Module
WSN	Wireless Sensor Network
XRES	Expected Response

# CHAPTER 1

## INTRODUCTION

The evolution of mobile networks has seen a groundbreaking shift with the advent of the fifth generation, 5G, which was launched in South Korea in December 2018. Positioned to meet the escalating demand for high-speed data transmission and enhanced capacity, 5G introduces substantial improvements such as increased speed, lower latency, enhanced connectivity, energy efficiency, and robust support for massive Internet-of-Things (IoT) and machine-type communications (mMTCs). However, amidst these advantages, significant challenges arise, particularly in the realm of security ("A Generic Construction for Efficient and Secure AKA Protocol in 5G Network," 2018) (Braeken, 2019).

While 5G offers remarkable advancements, it simultaneously poses challenges in terms of security. These challenges encompass vulnerabilities in authentication mechanisms, privacy and integrity concerns, and susceptibility to various types of attacks. Among these, Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), Man-in-the-Middle (MitM), and eavesdropping attacks are noteworthy ("A Generic Construction for Efficient and Secure AKA Protocol in 5G Network," 2018).

The 5G architecture comprises three primary components:

1. 5G Access Network (AN): Also known as the Radio Access Network (RAN), it includes base stations and wireless connections to user devices, ranging from traditional macro-cells to small cells.
2. 5G Core Network (CN): Providing essential control functions such as network slicing, service quality management, session management, and mobility management.
3. User Equipment (UE): Devices like smartphones and IoT devices that connect to the 5G network.

A critical aspect of 5G's security architecture is the 5G Authentication and Key Agreement (5G-AKA) protocol, developed by the Third Generation Partnership Project

(3GPP). Despite its significance, this protocol has shown susceptibility to various attacks, indicating a need for further enhancement.

In the 5G-AKA protocol, three entities play pivotal roles: UE, Home Network (HN), and Serving Network (SN). The UE shares a master key exclusively with the HN, facilitating authentication and encryption key derivation when connecting to different SNs.

Notwithstanding its advancements, the 5G-AKA protocol exhibits vulnerabilities, including privacy leaks, replay, de-synchronization, DoS / DDoS, and potential weaknesses against MitM attacks (Sharma, 2019).

The high complexity of the 5G architecture and the 5G-AKA protocol may lead to misconfigurations, creating opportunities for security breaches. These vulnerabilities raise significant security concerns that demand immediate attention and mitigation measures (Sharma, 2019).

This study aims to address identified vulnerabilities, particularly within the 5G-AKA protocol, and proposes measures to enhance the overall security of 5G networks. The objective is to design a protocol that not only rectifies existing limitations such as security challenges, privacy concerns, and protocol overhead but also anticipates and withstands potential attacks, ensuring efficient authentication and preserving user privacy and safety within the 5G network.

## **1.1 Problem Statement**

The rapid evolution of 5G networks, while promising groundbreaking connectivity speeds and capabilities, has introduced a new set of security vulnerabilities. Despite industry efforts to bolster security measures, persistent vulnerabilities pose a threat to user data and network functionality.

Following the release of the standardized 5G-AKA protocol, the 3GPP outlined several updates to enhance security ("A Generic Construction for Efficient and Secure AKA Protocol in 5G Network," 2018). However, ongoing vulnerabilities - which will be discussed further in the upcoming sections - highlight the need for robust solutions. The structure of the 5G network includes two main components: The 5G-Core (5GC) and the New Generation Radio Access Network (NG-RAN).

The 5GC operates as the central hub of 5G technology, overseeing data and plane operations, data traffic consolidation, and multiple security layers provision. It employs a Service-Based Architecture (SBA) that is cloud-compatible to bolster security, authentication, and session management. The 5GC SBA consists of twelve integral components, including UE, User Plane Function (UPF), Data Network (DN), Access and Mobility Management Function (AMF), Authentication Server (AUSF), Session Management Function (SMF), Network Slice Selection Function (NSSF), Network Exposure Function (NEF), Network Repository Function (NRF), Policy Control Function (PCF), Unified Data Management (UDM), and Application Function (AF) (“5G Security Recommendations Package #1”, 2016) (Ouaissa, 2020).

Security risks in the 5G network can be segmented into three parts based on the CIA triad:

- Confidentiality: Safeguarding information from unwarranted access or exposure.
- Integrity: Preserving the authenticity and reliability of data.
- Availability: Ensuring systems, networks, and services are available and functional as required.

The AKA protocol serves as a secure method for exchanging information among various entities through symmetric key cryptography (Chen et al., 2016). This research aims to craft a superior authentication protocol that not only addresses the limitations of the standardized 5G-AKA protocol but also significantly enhances the security of the 5G network.

The protocol is designed to counter potential attacks, including DoS / DDoS, MitM, spoofing, replay, DNS, location discovery, and AKA attacks. The research methodology concentrates on creating a protocol that accentuates user privacy and security while ensuring efficient and secure authentication within the 5G network. The study aims to demonstrate efficacy across two different back ends in AVISPA (OFMC and CL-AtSe) as well as various metrics, including computational and communication overheads, and signaling messages.

## 1.2 Purpose of the Study

The primary aim of this research is to strengthen the security mechanisms of the 5G network by implementing an advanced authentication protocol. This protocol is specifically tailored to address vulnerabilities in the existing 5G-AKA protocol, including Eavesdropping, DoS, DDoS, MITM, Replay, Spoofing, DNS attacks, Location Discovery, and AKA attacks, despite continuous updates by the 3GPP. Acknowledging the persistent susceptibility of the 5G network to various security threats, the overarching goal is to create a robust protocol capable of defending against the mentioned spectrum of attacks.

The chosen approach places strong emphasis on user privacy and security while simultaneously optimizing authentication efficiency within the 5G network. To be more specific, the study aims to achieve its goals by introducing an authentication protocol that not only enhances the confidentiality, integrity, and availability of data within this network but also addresses theoretical insights into the design of secure authentication protocols as well.

The significance of this study is underscored by its potential to make a substantial contribution to the enhancement of both 5G network security and the specific challenges posed by M2M communication. This is particularly crucial in light of the expanding role of these networks in today's interconnected world. The anticipated outcomes are expected to provide practical solutions not only to identified security vulnerabilities within the 5G infrastructure but also to the intricate security demands of M2M scenarios, offering valuable guidance for future research and policy decisions in the realm of connected networks.

To accomplish the study objectives, the research presents a unique solution developed independently, guided by insights gained from an extensive literature review and substantiated through subsequent performance comparison.

However, here is an overview of the next phase of the research methodology, the desired authentication protocol named as Efficient and Strong AKA (ES-AKA) will be translated into the High-Level Protocol Specification Language (HLPSL). This step is crucial for formal verification, assessing the protocol's security properties rigorously. The HLPSL format provides a standardized representation that can be processed by formal verification tools. Following the translation / coding in HLPSL, two powerful backend

tools, namely OFMC and CL-AtSe will be used to simulate virtual real-world conditions, enabling a thorough evaluation of the protocol's robustness against known security threats. The distinctive methodology will be comprehensively delineated in the study's proposed protocol, security analysis and performance evaluation sections.

### **1.3 Significance of the Study**

The significance of this research stems from its potential to contribute substantially to the ongoing efforts to strengthen the security infrastructure of the 5G network, a pivotal enabler of numerous emerging technologies. The reasons for its paramount importance are as follows:

1. **Enhanced Security for Users:** Designing a robust authentication protocol addresses the inherent limitations of the standardized 5G-AKA protocol, aiming to enhance security for millions of users globally, fostering greater trust and confidence in 5G technologies.
2. **Impact on Standards and Policies:** Outcomes could influence the development and modification of future security protocols or standards for 5G networks, ensuring a more secure and reliable communication framework.
3. **Societal Benefits:** A secure 5G network is crucial for the safe growth of IoT, secure transmission of sensitive data, including: biometric data, authentication credentials, financial and health information, etc. And increasing user trust in 5G technology. By contributing to a more secure network, this study indirectly supports the further advancement and adoption of technologies reliant on 5G, such as autonomous vehicles, smart cities, and remote healthcare, to name a few.
4. **Contribution to Knowledge:** This research will provide a novel perspective on how to address the security issues in the 5G-AKA protocol, contributing to the pool of knowledge in the field of 5G security. The study's findings could provide a fresh insight into the theoretical and practical aspects of secure 5G network design and operation.
5. **Solution to Real-World Problem:** The study aims to design a protocol that could be applied practically to enhance the security real-world problem, namely the security vulnerabilities in the current 5G networks, leading to safer, more reliable telecommunications.

6. **Cost-Efficiency:** By considering metrics such as computational and communication overheads, handover latency, storage costs, transaction and execution costs, the study aims to develop a solution that is not only secure but also cost-efficient. This could have significant implications for network providers looking to balance the cost and security of their services.
7. **Increased User Privacy:** One of the main goals of this research is to enhance user privacy within the 5G network. By doing so, it could have a significant impact on the personal security of millions of individuals who use 5G networks in their daily lives.
8. **Facilitation of Future Technological Innovations:** With 5G networks playing an increasingly central role in enabling technological innovations in fields as diverse as autonomous vehicles and telemedicine, enhancing the security of these networks is of utmost importance. The success of this research could, therefore, indirectly facilitate future technological innovations by providing a more secure foundation for their development.
9. **Future Research:** Serving as a foundation for future research in 5G security, the insights and findings may guide researchers, propelling advancements in the field.

Overall, this research aims to have a broad impact, not only in academic and research circles, but also for industry practitioners, policy-makers, etc.

## **1.4 Research Questions and Hypotheses**

The fundamental research question for this study could be formulated as follows:

In what ways can the authentication protocol of the 5G network be refined to boost security measures and fend off a variety of attacks?

To delve into this primary research question comprehensively, the ensuing sub-questions will be scrutinized:

1. What are the current shortcomings and susceptibilities of the authentication protocol presently in use in the 5G Network?
2. What potential hazards and threats emerge from various attacks aimed at the 5G authentication protocol?
3. How can the employment of reciprocal authentication mechanisms effectively deter masquerading attacks and illicit access?



4. What type of secure key creation algorithms should be employed to set up robust and secure communication paths, thus diminishing compromised encryption and decryption procedures?

## **1.5 Assumptions**

In embarking on this research, it is crucial to acknowledge several foundational assumptions. While untested, they are deemed reasonably valid within the context of this study, shaping the structure and boundaries of the research. However, their applicability may vary across different contexts or within other 5G networks.

The following are the five fundamental assumptions for this study:

1. The existing 5G-AKA authentication protocol contains certain vulnerabilities that can be exploited through a variety of attacks: This assumption is based on the idea that the current authentication protocol has certain inherent flaws or weak points, identified through previous research and security reports. These vulnerabilities could potentially be targeted by malicious actors to breach the network's security.
2. Enhancing the authentication protocol can effectively mitigate these vulnerabilities: It is presumed that the creation of a robust authentication protocol can address and rectify the known vulnerabilities in the current 5G-AKA protocol. This enhanced protocol would provide stronger safeguards against potential attacks.
3. All other factors affecting the security of the 5G network, apart from the authentication protocol, will remain constant during this study: This assumption indicates that variables like the network's infrastructure, hardware, software, and user behavior, among others, will not change or modified during the period of the study, ensuring that any changes observed can be attributed to the modified authentication protocol.
4. The chosen methods of testing and evaluating the proposed authentication protocol will provide reliable and valid results: This is an essential assumption that presumes the research methodology, testing strategies, and evaluation metrics chosen for this study will be able to accurately measure the effectiveness and security of the proposed authentication protocol.

5. The security risks and vulnerabilities identified in the 5G-AKA protocol are representative of similar vulnerabilities that may exist in other comparable 5G technologies: This assumption is based on the premise that the vulnerabilities found in the 5G-AKA protocol are not unique to this specific protocol, but rather indicative of broader security risks present in similar 5G technologies. This means that the findings of this study could potentially be applicable to other 5G networks and systems as well.

While these assumptions provide a foundational basis for this research, it is worth noting that their applicability could vary across different circumstances or 5G networks. The insights gained from this study, however, could potentially offer broader applications and inform future security enhancements within the field of 5G technologies.

## **1.6 Limitations**

In the pursuit of this dissertation, it is essential to recognize and address certain limitations that may affect the implementation and scalability of the proposed authentication protocol. While the protocol will undergo rigorous evaluation and testing in a controlled environment, its real-world application may introduce additional challenges that need to be carefully considered.

One significant limitation lies in the transition from a controlled environment to a practical, large-scale deployment. Factors such as the diversity of network infrastructures, varying hardware and software configurations, and the sheer size of a live network can introduce complexities that were not present in the controlled testing phase. Therefore, it is essential to acknowledge these real-world challenges could impact the protocol's performance and effectiveness, making it crucial to thoroughly evaluate the protocol's resilience in different deployment scenarios.

Another limitation pertains to the varying security practices adopted by telecom vendors and operators. While the designed protocol demonstrates robustness and efficiency in the controlled environment, its full potential can only be realized when it is implemented and configured correctly in live networks. Adherence to recommended security practices, proper implementation, and configuration are imperative to ensure that the protocol can stand up to the challenges posed by potential attackers and offer the highest level of security.

Additionally, as technology continually evolves, so do the tactics employed by cyber attackers. Although the proposed protocol is expected to bolster security significantly, it may encounter new threats or vulnerabilities in the future. Thus, it becomes essential to maintain ongoing research and collaboration with industry stakeholders to stay abreast of emerging security challenges and continuously improve the protocol's capabilities.

Despite these limitations, the research anticipates that the designed authentication protocol will maintain its robustness and efficiency, effectively addressing the known weaknesses. Indeed, the proposed solution is expected to bolster the overall security of the 5G network. The outcomes of this research aim to lay a solid foundation for future security enhancements in 5G networks and analogous emerging technologies.

The success of the proposed protocol's real-world implementation depends on the collective efforts of academia, industry stakeholders, and policy-makers. Collaboration among these entities can lead to refinements in the protocol, ensuring its practical viability and adaptability to diverse network environments. Through such concerted efforts, the research aims to contribute significantly to strengthening the security infrastructure of the 5G network and bolstering its role as a key enabler for numerous emerging technologies.

## **1.7 Definition of Key Terminology**

In the course of this study, a variety of specialized terms and acronyms will be used that are specific to the field of telecommunications and 5G network security. To ensure clarity and facilitate understanding, the following key terms have been defined:

### **1.7.1 Basic Key Terms**

- **5G Network:** This term refers to the fifth generation of wireless technology, designed to deliver faster speeds, lower latency, and more reliable connectivity than its predecessors (e.g.: 3G, 4G, and LTE) (Braeken, 2019).
- **Authentication Protocol:** An authentication protocol is a type of security protocol that verifies the identity of a user, system, or device, typically before granting access to resources in an information system.
- **5G-AKA:** This is the AKA used in 5G networks. Developed by the 3GPP, it is designed to provide secure communication between a user and the network.

- 3GPP: A collaboration between groups of telecommunications associations, known as the Organizational Partners, aimed at developing globally applicable specifications for mobile systems.
- 5GC: This refers to the core network of the 5G architecture, which is responsible for key functions such as user authentication, session management, and mobility management.
- NG-RAN: It includes the network's base stations and antennas that connect mobile users and wireless devices to the main core network.
- Service-Based Architecture (SBA): An architectural design pattern that structures applications as a collection of loosely coupled services. In the context of 5G, SBA refers to the architecture where network functions within the 5GC expose their functionalities as services, allowing other authorized network functions to access these services. This results in a highly flexible and modular network design that is more scalable, secure, and easier to manage compared to traditional network architectures.
- Cryptography: It is a method of protecting data and information (plain-text) by transforming it into an unreadable format (cipher-text). Only those who possess a special key can decrypt the information back into a readable format. Cryptography is a fundamental component of secure communication, ensuring data confidentiality, data integrity, authentication, and non-repudiation.
- Asymmetric Encryption: Also known as Public Key encryption, it is a type of encryption where two different keys are used for encryption and decryption. These are the public key, which can be shared openly, and the private key, which is kept secret by the user. The public key is used to encrypt the message, and only the corresponding private key can be used to decrypt it. This method is often used in secure communications over the internet, such as in secure email and SSL/TLS for web traffic.
- Symmetric Encryption: Is a type of encryption where the same key is used for both encryption and decryption. This method is faster and simpler than asymmetric encryption but requires that the key be kept secret from all except

the sender and receiver. This can make it less practical for large-scale or public communications. Symmetric encryption is often used for bulk data encryption and for encrypting data at rest.

### **1.7.2 The 5G Architecture Components**

- User Equipment (UE): Refers to a device, such as smartphones or IoT device, used directly by an end-user to communicate on the network.
- User Plane Function (UPF): Responsible for packet routing and forwarding, packet inspection, and user plane part of mobility management in the 5G network.
- Data Network (DN): The network that provides data connectivity to the UE. It could be the internet or an operator's services network.
- Access and Mobility Management Function (AMF): Handles UE's access to the core network and manages its mobility.
- Authentication Server Function (AUSF): Verifies the UE's credentials during the authentication process.
- Session Management Function (SMF): Manages the UE's data sessions.
- Network Slice Selection Function (NSSF): Responsible for the selection of Network Slice instances to serve the UE.
- Network Exposure Function (NEF): Exposes the services and capabilities provided by the 3GPP network functions to application functions.
- NF Repository Function (NRF): Handles service discovery in an SBA.
- Policy Control Function (PCF): Establishes and manages policies within the network.
- Unified Data Management (UDM): Manages user data in the 5G network.
- Application Function (AF): Influences traffic routing and provides application-level information for policy control.

### **1.7.3 The 5G-AKA Architecture Components**

- Subscriber Permanent Identifier (SUPI): A permanent identity used in 5G systems to identify a subscriber.
- Serving Network Name (SNname): The identifier of the serving network in an authentication credential.

- Authentication Token (AUTN): A token sent from the network to the UE as part of the authentication process. It serves to prove the network's authenticity to the UE, assist in authenticating the UE to the network, and provide resistance against replay attacks.
- Expected Response (XRES): is a crucial component in the challenge-response mechanism used in mobile communications for authentication. Technically, it is a value calculated by the network and the UE during the authentication process to verify mutual authenticity. Furthermore, it ensures that the UE is genuine and is in possession of the correct secret key, thereby establishing a trusted connection between the network and the UE.
- Confidentiality Key (CK), Integrity Key (IK), and Anonymity Key (AK): All these keys are derived from the same authentication and key agreement procedure but are used for different security purposes. Typically, derived using the Milenage algorithm in UMTS, with the UE and the network's Authentication Centre (AuC) both possessing the necessary secret key ( $K_i$ ) to derive them.
- Authentication Centre (AuC): is crucial for network security, responsible for user authentication and identity protection. It produces cryptographic keys for authentication, relying on a secret key specific to each subscriber. The AuC also creates temporary identities for communication privacy and securely holds subscriber authentication keys. In tandem with the Home Location Register (HLR), the AuC maintains the network's confidentiality.
- Home Network Public Key and Home Network Private Key (Hpublic-key and Hprivate-key): A pair of cryptographic keys used by the HN for the Elliptic Curve Integrated Encryption Scheme (ECIES) encryption and decryption processes.

#### **1.7.4 Security Threats in the 5G-AKA Protocol**

- Man-in-the-Middle (MitM) Attacks: A MitM attack could involve an attacker intercepting and potentially altering communication between two parties during the authentication process, without either party realizing the

communication has been tampered with. For example, the intruder could alter messages between the user's device and the network to gain unauthorized access or intercept sensitive information.

- Eavesdropping: This could involve an attacker secretly listening to the communication during the authentication process to gather sensitive information such as user credentials, session keys, or other personal data.
- Denial-of-Service (DoS) Attacks: This attack could attempt to overwhelm the network's authentication mechanisms, rendering the network unavailable to legitimate users. For instance, an attacker could repeatedly attempt to authenticate with false credentials, causing the system to expend resources processing these attempts and leaving insufficient resources for legitimate user requests.
- Distributed Denial-of-Service (DDoS) Attacks: A DDoS attack might involve overwhelming the network's authentication mechanisms from multiple sources. This could make the network unavailable to legitimate users and may be harder to mitigate due to the distributed nature of the attack.
- Replay Attack: A replay attack could involve an attacker intercepting a valid authentication request and later retransmitting it. The network would treat the replayed request as valid, potentially allowing the attacker to gain unauthorized access.
- Impersonation Attack: This attack could involve an intruder posing as a legitimate network user or entity to gain unauthorized access. For instance, by obtaining valid authentication credentials through eavesdropping or other means, the intruder could trick the network into believing they are a legitimate user.

To conduct, this research presents the design and implementation of a novel AKA protocol named ES-AKA. This innovative protocol is developed to effectively mitigate all mentioned attacks, providing a robust security solution. Furthermore, to assess its practical viability, ES-AKA is subjected to a comparative analysis with ten other AKA methods identified through an extensive literature review. The evaluation encompasses

various aspects such as their resilience to known attacks and security properties, ensuring the selection of a practical and secure solution. Additionally, the proposed model undergoes a thorough virtual testing phase using two distinct backends, namely OFMC and CL-AtSe, to validate its effectiveness and resilience in simulated environments.



## **CHAPTER 2**

### **LITERATURE REVIEW**

A vast array of scholarly inquiries and detailed analyses have been aimed at probing the intricacies of security within 5G Networks, especially focusing on the unique authentication protocol termed as 5G-AKA. Experts and researchers in this domain have invested their skills and knowledge in a thorough exploration of the potential security loopholes and risks intrinsic to the network. Their collective efforts encompass a detailed scrutiny and evaluation of the effectiveness of the 5G-AKA protocol in ensuring safe and secure communications while resisting a wide spectrum of cyber threats and intrusive attacks. These in-depth studies serve not only to assess the protocol's robustness and potential vulnerabilities but also to inspire improvements that will bolster the overall security resilience of 5G Networks and pave the way for future enhancements in this critical field of network security.

#### **2.1 Related Works**

Arkko et al. (2015) put forth an advanced version of the 5G-AKA which substitutes SQNs with arbitrary values, aiming to accomplish two additional security objectives. Despite being in their nascent stages, blockchain-based solutions exhibit immense promise in addressing 5G technological hurdles such as decentralization, transparency, interoperability, and privacy and security concerns. The innate properties of blockchain, such as transparency, data encryption, auditability, immutability, and a distributed framework, enable it to offer viable solutions for data privacy, authentication, integrity protection, and access control. Various technologies, including Software-Defined Networking (SDN), Network Function Virtualization (NFV), machine learning, and cloud computing, are employed within 5G networks to augment service efficiency. However, these also introduce a set of challenges.

The development of the protocol was informed by a set of fundamental principles. These included the utilization of Blockchain as an interface to facilitate roaming capabilities between HNs and alternative operators. It was mandated that all authentication requests bear the digital signature of the initiating agent, and that both HN

and SN should possess valid certificates to authenticate data origin. To prevent exposure of sensitive user data, message exchanges between HN and SN were encrypted. A stringent access management system was implemented, permitting only the HN to register a response to an authentication request transaction. The involvement of the HN's random number in session key generation was ensured to incorporate it into the key derivation algorithm. To authenticate freshness and counter replay attacks, every authentication request was assigned a unique identifier. A message sequence was deployed to achieve enhanced performance. Emphasis was laid on the necessity of secure communication between the UE and the gNB-Distributed Unit (DU) to prevent security threats that could burden the gNB-Centralized Unit (CU) with processing requests. Moreover, potential security threats during inter-gNB-DU handover were identified, which could result in traffic bottlenecks. In the NG-RAN architecture, functional splitting was employed to segregate gNB functions into gNB-CU, gNB-DU, and gNB-Remote Unit (RU), each having its own interfaces to the 5G core. The F1 interface was used to facilitate communication between the different components of the gNB-CU and gNB-DU (Nowak, 2021) (Shin, 2020).

Huang et al., (2019) explore the use of analytical modelling methods for assessing the reliability of the 5G-AKA authentication service. They propose two availability models, along with methodologies to compute the Dependability Performance Measure (DPM) and the time required for the service to recover from its first failure. The Total Cost of Ownership (TCO) is also discussed, taking into account a variety of aspects including infrastructure costs, energy consumption, and operational expenses. The study operates on the assumption that all time intervals follow an exponential distribution.

Khan et al. (2021) proposed a novel AKA mechanism that tackles the vulnerabilities identified within the standard 5G-AKA. The recommended solution is secure, efficient, and not resource-intensive. It underwent testing through Security Protocol ANalyzer (SPAN) software verification, demonstrating its resilience against various forms of attacks and its ability to maintain data integrity while reducing latency. Furthermore, it exhibits greater robustness in comparison to the recently standardized 5G-AKA.

Kim et al. (2021) delve into the challenges associated with creating a handover protocol for 5G-WLAN Wireless Local Area Networks, which is not only secure but also

efficient. The Extensible Authentication Protocol (EAP) authentication method utilized in LTE and 3G networks might include significant authentication lags in 5G networks, especially when handover authentications occur frequently. To address this issue, the research proposes the adoption of the MECs authentication mechanism, which has the potential to decrease the average Auth delay while simultaneously enhancing security. The suggested approach involves using a MEC server for re-authentication instead of conducting authentication with Authentication Authorization and Accounting (AAA) protocol each time. This process reduces the distance for the exchange of authentication information and future diminishes authentication latency.

Han et al. (2019) delve into the exploration of methodologies for assessing the reliability of the 5G-AKA authentication service. Their work outlines the models for availability, methods for computing DPM and the first time of service restoration, in addition to discussing TCO. Their assumption is based on exponential distributions, but they have plans for future research to incorporate semi-Markov processes. The authors express intent to factor in recovery policy within their model and expand it to account for failures of multiple entries. A numerical analysis is conducted to display the influence of varying parameters on DPM, the first restoration time, and TCO.

Jiang et al. (2020) propose an improved method of 5G-AKA that bolsters both privacy and the efficiency of authentication. They achieve this by implementing an identity pool and Bloom filter. The presented approach allows UE to modify their temporary identifier and proceed with authentication, negating the need for synchronization of the Sequence Number (SQN). The method builds upon the existing 5G-AKA mechanism and proves its viability for practical applications.

Conti et al. (2016) conducted a thorough analysis of the security characteristics inherent in the 5G-AKA protocol. This was done by creating a formal model in accordance with the revised 5G standards. Through this security assessment, it was revealed that the protocol becomes susceptible to replay and passive monitoring attacks when the channel condition changes from secure to insecure. This vulnerability arises from the inability of diameter sessions to safeguard the channels. As such, the study recommends against assuming that communication channels are secure, considering the growing sophistication of cyber threats.

Hojjati et al. (2020) introduce the GSL-AKA method as a viable solution for M2M communication with both LTE and 5G networks. This approach aims to fulfill security objectives, maintain privacy, and address the single key issues experienced in previous group-based AKA protocols. Additionally, it successfully circumvents recognized attacks and demonstrates superior computational and communication overheads in performance evaluations.

Al-Shareeda et al. (2022) suggest an authentication scheme tailored for mission-critical Internet of Vehicles (IoV) applications. The scheme is lightweight and designed for optimal space efficiency. The mechanism leverages the use of cuckoo filter for efficient authentication in densely populated vehicular scenarios and is juxtaposed with the standardized 5G-AKA process for comparison. The proposed scheme exhibits better performance in terms of end-to-end latency and protocol overhead. The authors plan to focus future research efforts on further enhancing the mechanism by using roadside units to verify messages via broadcast messages in nearby vehicles.

De Ree et al. (2019) present an innovative AKA mechanism for Device-to-Device (D2D) communication within the realm of 5G networks. Their method employs Physical Layer Security (PLS) alongside public key cryptography for authentication purposes. It generates a symmetric session key, which is then combined with a parameter based on the communication channel to create a dynamic key. This key is then used for encrypting data and ensuring data integrity. Their proposed method has been demonstrated to be resilient against MitM and impersonation attacks. The research paper's analysis and the results from simulations validate the effectiveness of their method in achieving authentication and privacy.

Ouaissa et al. (2020) put forth an authentication method that is both efficient and preserves privacy in the context of 5G communication networks. The focus of their proposed mechanism is to ensure the safeguarding of the shared key and the identity of the device. The AVISPA tool is used to verify the protocol, and it has been found to meet all security objectives and to resist attacks effectively. The mechanism proposed considerably elevates privacy and security with only a minimal overhead. According to the authors, this is the first approach in existing literature that successfully preserves the device identity and the shared key between entities in communication.

Houmer et al. (2020) put forward a novel AKA mechanism designed for 3GPP 5G networks, incorporating extended Chebyshev chaotic maps. This mechanism presents two secure yet lightweight authentication protocols suitable for UE and substantial Machine-type Devices (MDs). It simplifies the authentication process, decreases communication and signalling expenditures, and has computational and storage costs akin to standard AKA protocols. Both security and performance analysis indicate that the suggested protocols outshine the standard mechanism and other comparable protocols.

Modiri et al. (2018) pinpoint two concerns associated with the 5G-AKA mechanism, specifically related to generating random numbers and managing sessions. To address these issues, they suggest modifications which comprise a straightforward session binding solution that consistently generates a random key, thereby bolstering security and defending against activity tracking attacks.

Bahja et al. (2020) point out certain vulnerabilities in existing 4G network authentication methods that are prone to attacks, and note that some of these vulnerabilities persist in 5G, despite the introduction of new authentication procedures. With the development of new 5G applications, there is the potential for additional security risks to arise. The study emphasizes the necessity of innovative AAA mechanisms that are tailored to 5G's unique demands, such as IoT devices, heterogenous network access, and network slicing. The relevance of their research is underscored by its implications for ensuring the security of both network operators and users.

Adem et al. (2015) employed Petri Net for an in-depth security analysis of the 5G-AKA protocol and unveiled three potential attack strategies. Among them, two attacks shed light on the existing security loopholes in the protocol, while the third highlighted the inadequate protective measures in place for the SN. To rectify these vulnerabilities, the authors introduced a novel scheme incorporating UNI and a challenge-response mechanism. This study marks the first usage of Petri Net as a tool for delineating and verifying the security aspects of the 5G-AKA. The validity of the model was ascertained through an evaluation of the information that could be reached at each place and transition.

Pari et al. (2019) pinpoint deficiencies and potential risk areas in the authentication and access control system proposed by Adavoudi-Jolfaie et al. As an improvement, they put forward a novel architecture specifically tailored for Wireless Sensor Networks

(WSNs) incorporated within 5G-enhanced IoT. The researchers conducted an analysis of their proposed three-factor authentication, authorization, and key agreement scheme, which is grounded in ECC. Their findings indicated that the new scheme provides superior security functionalities without significantly escalating the communication overhead. Consequently, they plan to dedicate their future research to optimizing their proposed solution based on the insights derived from these experimental outcomes.

Park et al. (2022) introduce an innovative Puzzle-based Co-Authentication scheme, referred to as PCA, aimed at overcoming the limitations observed in existing pseudonymous authentication strategies for Vehicular Ad Hoc Networks in the 5G context (5G-VANET). The PCA scheme curbs the capability of adversaries to generate counterfeit certificates, while simultaneously amplifying the proficiency of certificate validation. The scheme effectiveness is substantiated through both theoretical analysis and empirical results, showcasing its prowess in combating DoS attacks and mitigating the burden of pseudonymous authentication. As a part of their future work, the researchers aspire to discover more sophisticated computational puzzles to further streamline the process of pseudonymous authentication.

Shin et al. (2020) propose a novel communication security methodology named Modular Square Root (MSR-DoS) for 5G vehicular networks, which incorporates modular square root. This scheme ensures privacy, security, and reciprocal authentication, and meets an array of security criteria. Furthermore, it has been designed to keep communication and computational costs to a minimum. Looking ahead, the authors plan to extend their research by integrating fog computing, accommodating batch verification processes, and carrying out simulation experiments.

Basudan et al. (2020) investigate the implementation of network coding-enabled mobile small cells to fulfill the demanding throughput and ultra-reliability specifications of 5G networks. Given the security considerations, traditional integrity systems may prove inadequate in the context of network coding. The authors propose homomorphic schemes as possible solutions. They discuss two potential strategies, one hinging on a central controller and other employing a distributed ledger akin to blockchain, which could offer improved performance in the coordinated small cell system. Nevertheless, additional validation is necessary to guarantee their practical application.

Nowak et al. (2021) introduce a novel technique to identify spoofing assaults in 5G mmWave massive MIMO communication systems, leveraging channel virtual representation. They employ Neyman-Pearson NP testing for consistent radio settings and adopt a machine learning-based strategy for fluctuating radio environments. The method proposed outperforms conventional methods in terms of detection rates and precision. Furthermore, it is deemed more efficient and accurate compared to currently available one-class classifiers.

Vasudevan et al. (2022) assess the implications of adversarial example generation assaults on machine learning models that are deployed for various functions in 5G networks. The research delineates the methodologies involved in data creation, model training, and evaluation procedures, and gauges the impact of different attacks on the targeted models. Despite acknowledging the potential for substantial efforts from these attacks, the authors argue that it's improbable for adversaries to gain access to the model's input or output labels. Looking forward, they suggest the development of algorithms designed for input-agnostic adversarial disruptions.

Baker et al. (2011) present an exhaustive review of progress made in 5G wireless security and suggest a unique security architecture for 5G wireless systems. The security aspects of emerging technologies including Heterogeneous Network (HetNet), D2D communication, massive MIMO, SDN, and the IoT are discussed in detail. The paper delves into the benefits of the proposed architecture in terms of identity management and adaptable authentication, and it investigates a specific handover procedure along with its performance.

Li, W. et al. (2021) underline the critical importance of secure wireless communication within 5G networks that are deployed for critical communication systems, which have stringent requirements for privacy and data integrity. They provide a critical analysis of the initial set of 5G security specifications, suggesting a comprehensive security framework designed to prevent insecure operational models and potential vulnerabilities. They advocate for collaborative efforts across different organizations for the design and implementation of secure 5G systems, incorporating new technologies such as the 5G RAN. Furthermore, they propose conducting additional security research to

tackle vulnerabilities present in emergent and future mobile communication and control systems.

Duan et al. (2016) present an AI-based approach designed to detect DoS/DDoS attacks on computer networks. The solution proposed is rooted in a flexible, modular architecture built-on SDN, which can be tailored to identify a broad spectrum of attacks. Various Deep Learning (DL) and Machine Learning (ML) models were evaluated in the study. It was found that DL models outperformed their ML counterparts in identifying both slow-rate and high-volume attacks, achieving high detection rates. The proposed solution was assessed using a simulated testbed, and open tools such as Open Network Operating System (ONOS) controller facilitate its implementation in real-world environments. Future developments include augmenting the solution's scalability and devising an optimized mitigation strategy.

Cheng et al. (2022) is designed to tackle existing issues in LTE while fulfilling the requirements of 5G and crucial Public Safety (PS) systems. This includes safeguarded processes for authentication and re-authentication, resulting in decreased access latency and a lighter workload on the Home Subscriber Server (HSS). Furthermore, the system addresses security vulnerabilities. The safety of this system has been confirmed, providing privacy protection and secure communication not only for LTE but also for future-generation PS networks.

Li, Y. et al. (2020) evaluate the influence of MEC technology on 5G MEC-centric services across twelve different sectors. The investigation primarily targets the required parameters, vulnerabilities, and typical attack networks, recommending corresponding security strategies. The study also explores the possible application of AI to enhance decision-making in resource allocation and boost network efficiency. In conclusion, while MEC technology introduces new security hurdles that necessitate in-depth scrutiny, it also presents considerable potential benefits for a variety of sectors.

Bahja et al. (2020) elaborate on the utilization of Natural Language Processing (NLP) techniques for scrutinizing social media data, enabling a more comprehensive understanding of how misinformation proliferates. Specifically, they concentrate on the examination of tweets relating to COVID-19, wherein the pandemic is associated with 5G. This is achieved through the deployment of diverse models like sentiment analysis,



Latent Dirichlet Allocation (LDA), and social network analysis. The study of the occurrence and interrelations of various subjects in these tweets facilitates the detection of misinformation patterns, thereby providing guidance to policymakers for devising appropriate countermeasures. The authors propose augmenting their research by implementing a more detailed and long-term analysis.

Li, Y. et al. (2020) strive to enhance the allocation of resources for eMMB and URLLC slices in the 5G RAN, ensuring the prevention of Spectral Collision Avoidance (SCA). The proposed algorithm, known as SCA-RA, is designed to increase the quantity of accommodatable slices and lower the blocking ratios associated with slice requests. The outcomes from simulations demonstrate that this approach leads to a better utilization of resources and a decrease in the consumption of Information Technology (IT) and transport resources.

Park et al. (2022) evaluate the effectiveness of session management strategies in the context of 5G network security systems and measure their performance relative to current solutions. The recommended approach can be deployed in any Standalone (SA) 5G network, encompassing private networks globally. The authors aim to trial this method in a private 5G setting, underlining the need for service providers to actively test and validate 5G security systems. They call attention to the importance of assessing both emerging and previously suggested technologies and crafting secure infrastructures for novel 5G services.

**Table 1***A Comprehensive Analysis: Exploring Security and Performance Enhancements in 5G-AKA Protocols*

Ref. of Article	Any Proposed Methods?	Is it a Survey?	Tools being used?	Its Performance	Summary
Braeken, 2019	Yes	No	Rubin Login	Computational & communication overheads	The article outlines security flaws in the 5G AKA mobile communications protocol and suggests a new version to fix them. In order to streamline communication, the suggested protocol eliminates sequence numbers in favor of random numbers and adds two more security elements. Comparing the proposed protocol to the present 5G AKA standard, performance enhancements are also examined.
Sharma, 2019	Yes	No	OFMC and CL-AtSe	Computational & communication overheads	In this article, the security issues with the current 5G handover protocol are discussed, including bogus base-station assaults, a lack of KFS/KBS, DoS attacks, and a complicated network. A novel, effective, and security-enhanced handover AKA mechanism is suggested to overcome these problems. To confirm its accuracy, the proposed protocol is formally examined using the AVISPA tool. It is found to perform better than current 5G handover protocols in terms of communication and computation overhead.
Koutsos, 2019	Yes	No	ProVerif, Bana-Common Logic (framework )	Computational overhead	The study investigates the 5G-AKA authentication protocol, which attempts to improve privacy through the use of asymmetric randomized encryption. The research illustrates that, while the protocol prohibits IMSI-catcher attacks, all other known privacy attacks remain valid. The authors then propose protocol improvements to prevent these attacks while preserving efficiency, and use the Bana-Comon indistinguishability logic to explicitly show the protocol's -unlinkable characteristic. As a side effect, reciprocal authentication is demonstrated.
Parne, 2020	Yes	No	OFMC	Computational & communication overheads	In order to overcome the flaws and performance concerns of the 5G-AKA protocol used in mobile communication networks, the study suggests a new protocol named PPSE-AKA. The shared secret key is safeguarded via the PPSE-AKA protocol, which also uses the AVISPA tool to do formal verification. Additionally, the protocol complies with privacy standards and protects against potential threats, according to the security study. The PPSE-AKA protocol performs better than earlier developed methods.

**Table 1** (continued)*A Comprehensive Analysis: Exploring Security and Performance Enhancements in 5G-AKA Protocols*

Ref. of Article	Any Proposed Methods?	Is it a Survey?	Tools being used?	Its Performance	Summary
Kalalas, 2020	Yes	No	N/A	Communication overhead	The limits of 5G-AKA in dense V2X settings and the difficulties in ensuring the developing V2X connection paradigm are discussed in the article. The paper suggests a simple method for vehicle authentication that makes use of the cuckoo filter to authenticate several automobiles at once. The suggested technique beats the 5G-AKA process in terms of latency and protocol overhead, even for heavy vehicle load, and achieves high efficiency with minimal impact on communication.
Kiyemba, 2020	Yes	No	ProVerif & BAN Logic	N/A	One of the main authentication techniques specified for the 5G network is the 5G-AKA protocol, which is described in the paper via a rigorous analysis. The ProVerif tool is used by the authors to thoroughly assess the protocol and find shortcomings and security problems that have not been addressed in related work. They offer suggestions on how to deal with the problems identified by the study.
Liu, 2018	Yes	No	N/A	Computation cost	The article highlights the importance of safe access to 5G networks as well as the vulnerabilities discovered in 3G and 4G networks. It presents a novel system for the 5G attach procedure that solves security challenges such as long-term key leakage, subscriber identification privacy concerns, insecurity of linkages between mobile network providers, and linkability attacks. The suggested method, unlike previous alternatives, does not rely on a worldwide public key infrastructure and tackles all security challenges in a single scheme.
Huang, 2019	Yes	No	N/A	Computational, communication, server storage, and client computation costs	The paper offers an authentication mechanism called IEWA to protect 5G networks against UDP DrDoS attacks and other susceptible UDP protocols. The technique employs higher costs and weak authentication, and it has been demonstrated to be safer, more stable, and more secure than previous schemes with lower prices and overhead. The suggested method tackles 5G network security issues, notably the rising incidence of DDoS assaults.

**Table 1** (continued)*A Comprehensive Analysis: Exploring Security and Performance Enhancements in 5G-AKA Protocols*

Ref. of Article	Any Proposed Methods?	Is it a Survey?	Tools being used?	Its Performance	Summary
Gharsal lah, 2019	Yes	No	OFMC & CL-AtSe	Computation overhead	A proposed SEL-AKA protocol is presented as a solution that addresses the limitations of the 5G-AKA protocol and enhances authentication and privacy objectives without relying on a Global Public Key Infrastructure. Analysis conducted using the SPAN tool proves that the SEL-AKA protocol is effective in meeting the authentication and privacy objectives.
Cao, 2020	Yes	No	ProVerif & Scyther	Communication, computational, and signalling costs	The article proposes a method called LSAA for the 5G network, which contains two lightweight extended Chebyshev Chaotic maps-based access authentication protocols for common UE and mMTC devices. The suggested protocols can achieve several security functionalities and are lightweight compared to the 5G-AKA protocol. Formal and informal security analysis and performance evaluations show that the proposed protocols provide advanced security and high efficiency.
Kim, 2021`	Yes	No	CPN Tool	N/A	The study focuses on the formal definition and security verification of the 5G AKA protocol, and it presents three attack techniques as well as an enhanced approach for preventing assaults and ensuring message security in the wireless channel. Petri net is a graphical and theoretically sound tool for attack-driven modeling. The research claims to be the first in the literature to use a Petri net to validate security techniques for the 5G AKA protocol.
Hojjati, 2020	Yes	No	ProVerif	Transaction & Execution costs	In this paper, which discusses about a blockchain-based authentication and key agreement protocol for roaming services in 5G networks that exploits the advantages of blockchain to do away with the necessity for a secure route between the HN and SN. The protocol is effective in terms of transaction and execution costs while maintaining user privacy and offering mutual authentication. Using ProVerif, the protocol's security is confirmed.

**Table 1** (continued)*A Comprehensive Analysis: Exploring Security and Performance Enhancements in 5G-AKA Protocols*

Ref. of Article	Any Proposed Methods?	Is it a Survey?	Tools being used?	Its Performance	Summary
Ouaisa, 2020	Yes	No	OFMC, CL-AtSe, SATMC, and TA4SP	Computational & communication overheads	Overviews of the development of mobile communication networks and the arrival of 5G technology are given in the passage. To improve security and address flaws in the preceding 4G network, the 5G-AKA protocol was established. The paragraph suggests an enhanced authentication and key agreement procedure for 5G networks that makes use of simple cryptographic techniques to raise computing cost. Using the AVISPA tool, the suggested protocol was vetted and confirmed, and an analysis of its performance showed that it outperformed other 3GPP authentication methods.
Houmer, 2020	Yes	No	OFMC, CL-AtSe, SATMC, and TA4SP	Computational & communication overheads	This article highlights how VANETs are crucial for ITS in providing real-time access to information, relaxation, and entertainment applications while ensuring user security. The article proposes an enhanced AKA protocol for VANETs in 5G networks to manage a large number of devices, which achieves security and privacy objectives, and outperforms several existing protocols based on security analysis and performance evaluations.
Bahja, 2020	Yes	No	N/A	Computational & communication overheads	The article discusses the value of security assurances in mobile cellular technology and the shortcomings of the current AKA protocols. It suggests a brand-new protocol called GSL-AKA that fixes the security problems with older ones and performs better in terms of communication and computational overheads. M2M communication is intended for the protocol.
Liu P, 2018	Yes	No	N/A	Pseudonymous authentication, signature verification, and data transfer	This article examines security and privacy issues in VANET for 5G networks, as well as a PCA strategy to reduce DoS attacks against pseudonymous authentication schemes. The PCA technique employs a carefully constructed hash problem for collaborative verification, and its effectiveness and efficiency are demonstrated by performance analysis based on theory and experimental data.

**Table 1** (continued)*A Comprehensive Analysis: Exploring Security and Performance Enhancements in 5G-AKA Protocols*

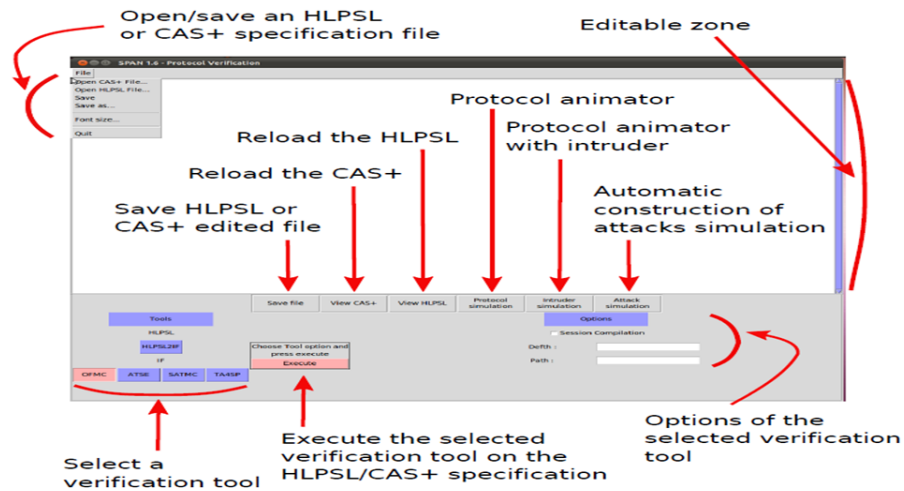
Ref. of Article	Any Proposed Methods?	Is it a Survey?	Tools being used?	Its Performance	Summary
Melki, 2019	Yes	No	AVISPA	Authentication cost and execution time	In D2D communication, where the AKA protocol might not be adequate, the article describes the challenges of device authentication. In order to assure genuine authentication without relying on the core network, the study suggests a novel PLS-based framework for device authentication and key formation in D2D/5G communication systems. This framework makes use of common channel features and asymmetric cryptography. Through performance and security research, the suggested technique is proved to be effective against different authentication threats and safe.
Park, 2022	Yes	Yes	N/A	Computational & communication overheads	This article provides an overview of the security problems that have arisen in 5G networks as a result of the expanded variety of services and increasing user activity. It categorizes security technologies based on OSI levels and examines vulnerabilities, threats, security solutions, difficulties, gaps, and unresolved research concerns for each layer. The report underlines the significance of all levels working together to ensure the security and integrity of 5G data. Because of the significant potential for assaults, the physical layer has been highlighted as particularly susceptible.
Vasudevan, 2022	Yes	No	BAN Logic	Computational & communication overheads	In this paper, a method called IoT-5G-AKA for remote registration and group authentication of IoT devices in 5G cellular network is presented. The scheme is designed to be in-line with the existing 5G-AKA protocol for easy adoption by the existing cellular system. In IoT-5G-AKA, all the security features of 5G-AKA continue to function as before; additional functionalities are introduced for group authentication of the IoT devices that are remotely registered with the 5G core network. Group authentication of the IoT devices helps in reducing signaling cost during authentication. Security analysis of the scheme shows that it is secured against various known attacks.

## 2.2 Verification Tools

AVISPA Tool stands out as a powerful suite for constructing and analyzing formal models of security protocols. Users interact with it through the HLPSL, a user-friendly language with a high level of abstraction, making it accessible for both reading and writing specifications. The tool employs modular modeling of security methods and goals, demonstrating its state-of-the-art capabilities in verifying a variety of network security protocols, particularly AKA protocols (as shown in Figure 1).

**Figure 1**

*SPAN Interface*

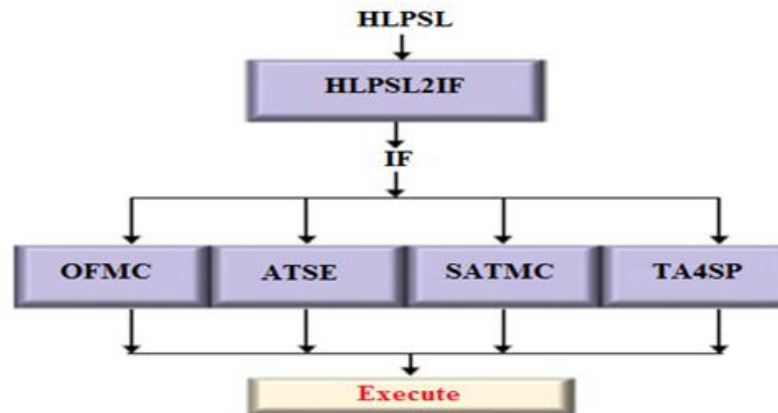


HLPSL serves as the language to describe security protocols and specify their security properties. Its modularity is particularly advantageous for expressing intruder models and security properties in academic and industrial-scale security protocols. The translation of HLPSL codes into the Intermediate Format (IF) is crucial, where IF acts as input to AVISPA's powerful back-end modes: Timed Automata for Security Protocols (TA4SP), SAT-based Model-Checker (SATMC), OFMC, and CL-AtSe (Mobarhan, 2020). These back-end modes verify the safety of presented methods according to defined goals (as depicted in Figure 2).

The emphasis on HLPSL's accessibility, the modular approach to security modeling, and the comprehensive back-end modes of AVISPA make it a compelling tool for users aiming to validate the security of their protocols.

**Figure 2**

*The Four Backends of AVISPA*



Scyther: Verification tool is instrumental in conducting formal security analyses, aiming to uncover security issues stemming from the implementation of the modeled method, considering defined cryptography assumptions. Notably, Scyther proves valuable even when there is no apparent attack, presenting results akin to a bounded verification tool. Its unique capacity for multi-protocol analysis contributes to its applicability in both academic and industrial settings.

Scyther operates with protocols modeled in Security Protocol Description Language (SPDL), which is based on operational semantics. SPDL in Scyther allows the definition of various security properties implemented as claim events. For instance, claims can assert the confidentiality (secrecy) of transmitted parameters. The tool employs Dolev-Yao's adversary model, assuming perfect cryptographic functions where adversaries cannot extract information from encrypted messages unless they possess the secret keys.

The tool incorporates different assumptions, such as the attacker's ability to check transmitted messages on the network communication and extract new transmitted data. Assumptions include knowledge representation (N), functions (f), and secret keys (k) for encryption and decryption. Scyther also defines various claims, including Alive (authentication), Nisynch (non-injective synchronization), Secret (confidentiality), and Niagree (non-injective agreement), each serving specific security requirements.

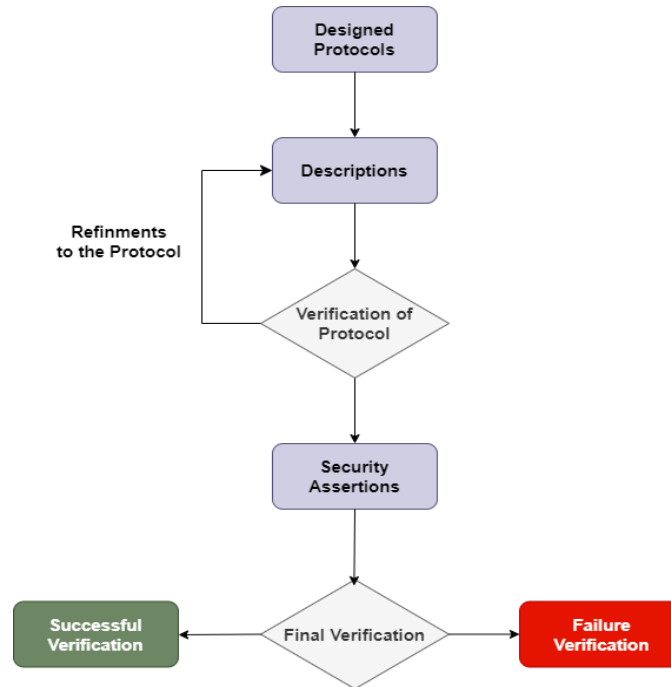
In essence, Scyther employs a well-established adversary model to monitor transmitted messages, allowing users to define claims that assert the security of their



protocols. The graphical analysis provided by Scyther enhances the understanding and verification of modeled protocols as shown in Figure 3.

**Figure 3**

*Scyther Verification System*



**BAN Logic:** The primary objective of formally analyzing a security method is to establish the correctness of the modeled approach. The BAN logic, devised by Burrows, Abadi, and Needham, is a widely recognized formal analysis tool for various AKA protocols. This logic operates based on the beliefs of trustworthy principals engaging in the AKA protocol, modeling the evolution of beliefs as a consequence of transmitted messages between involved nodes. It is particularly effective in identifying security issues and redundancies in commonly used security methods (Goswami, 2022).

In the BAN logic, present and past times are crucial, with the present time initiating with the sending of the first message and concluding with the reception of the last message. Messages transmitted before this time are considered part of the past.

For the formal evaluation of an AKA protocol, several assumptions are made, involving nodes, symmetric keys, public keys, secret keys, and statements. Notations in the BAN logic include symbols like " $| \equiv$ ," " $| \sim$ ," " $| \triangleleft$ ," and " $| \Rightarrow$ ," each representing different relationships between nodes and beliefs.

The BAN logic employs various rules for message meaning, nonce verification, jurisdiction, and belief, ensuring a comprehensive assessment of security protocols. The logic accommodates scenarios involving shared keys, public keys, shared secrets, and fresh messages. Additionally, the combination of two statements  $X$  and  $Y$  is denoted as  $(X, Y)$  in the logic. The inference rules of the BAN logic are applied to assess the validity of a statement  $Y$  based on a set of preceding statements  $X_1$ , up to,  $X_n$ .

The logic's rules cover aspects such as message meaning, jurisdiction, belief, utterance, sight, and message decryption. These rules facilitate the analysis of transmitted messages, shared keys, public keys, shared secrets, and fresh messages, ensuring a thorough evaluation of security protocols.

It's essential to note that the BAN logic provides a robust framework for assessing the security of AKA protocols, revealing potential vulnerabilities and ensuring the integrity of communication channels.

ProVerif: a formal verification tool developed by Bruno Blanchet, is widely utilized in computer security for the rigorous analysis of cryptographic protocols. Its primary function is to ensure the correctness and security of these protocols by employing formal methods, utilizing a process calculus-based modeling language. This modeling language allows users to represent cryptographic primitives, message passing, and other relevant aspects of a security protocol. ProVerif checks various security properties, including secrecy, authentication, and freshness, under different threat models and assumptions. Users can define attacker capabilities, such as eavesdropping and replay attacks, to analyze the robustness of a protocol.

The tool supports a variety of cryptographic primitives, including symmetric and asymmetric encryption, digital signatures, and hash functions. Users specify the properties of these primitives in their protocol models. ProVerif performs automatic analysis based on the inputted protocol model, security properties, and attacker capabilities, providing outputs that indicate whether the protocol meets specified security requirements. Additionally, the tool may detect vulnerabilities and offer traces or counterexamples illustrating security flaws. However, ProVerif has limitations, and the accuracy of its results depends on the correctness of the protocol model and the assumptions made. It is

not universally applicable and may not handle certain types of protocols or security properties.

ProVerif can be used as a standalone tool or integrated into larger verification workflows. Its application spans academic research, industrial settings, and educational purposes in cryptography and security courses. The tool is supported by comprehensive documentation guiding users on installation, usage, and result interpretation. An active community of researchers and practitioners contributes to its development and shares insights and discussions. It is essential to consult the latest documentation and resources for the most up-to-date information on ProVerif's features and capabilities.

**MATLAB:** MATLAB plays a crucial role in the evaluation of AKA protocols. One fundamental aspect is its capability to simulate the AKA protocol, allowing researchers to model its behavior, execute simulations under various conditions, and subsequently analyze the outcomes. This simulation-based approach helps in comprehensively understanding the protocol's performance and identifying potential vulnerabilities. Additionally, MATLAB facilitates the implementation and testing of cryptographic algorithms integral to AKA protocols, enabling researchers to assess the efficiency and security of these algorithms. Security analyses, including resistance against common threats, can be conducted using MATLAB tools, providing insights into the robustness of the AKA protocol.

Moreover, MATLAB serves as a platform for the evaluation of key management strategies and derivation functions involved in the AKA protocol. Researchers can explore different optimization techniques within MATLAB, experimenting with modifications to protocol parameters or algorithms and assessing their impact on security, efficiency, and overall performance. The language's data visualization capabilities further enhance the evaluation process by allowing the representation of results through plots, charts, and graphs. Lastly, MATLAB's flexibility extends to its integration with external tools and languages, providing researchers with the ability to leverage specialized libraries for specific aspects of AKA protocol evaluation. In essence, MATLAB serves as a comprehensive environment for researchers and engineers to conduct in-depth evaluations, contributing to the improvement and understanding of authentication and key agreement protocols, especially in the evolving landscape of 5G networks.

Table 2 provides an overview of the tools utilized in the development and evaluation of authentication protocols, with a specific focus on the security tools employed across the selected research studies. Among the various tools, AVISPA and BAN Logic stand out as the most frequently utilized. The studies referenced (2, 3, 15, 17, 18, 25, and 26) consistently demonstrate a notable connection with the AVISPA tool. This shared reference pattern suggests a recurrent reliance on AVISPA across multiple research works, emphasizing its significance and popularity in the domain of authentication protocol design and testing. However, the following two academic research 27 and 30 have managed to implement and test their proposed solutions in three different tools for accuracy, efficiency, and reliability.

**Table 2**

*Tools being either used to implement or evaluate the Proposed Protocols*

Security Tools	Cao 2020, Liu 2018, Khan 2021, De Ree 2019, Ouaisa 2020	Koutsos, Arkko, 2015	Kim, 2021	Houmer, 2020	Adem, 2015	Pari, 2019
AVISPA	×		×			×
MATLAB			×			
Scyther		×		×		
BAN Logic		×			×	×
ProVerif			×	×	×	
Open SSL				×		
CPN tool					×	

# **CHAPTER 3**

## **ARCHITECTURE OF MACHINE-TO-MACHINE WITHIN 5G NETWORKS**

M2M refers to the direct communication between devices without human intervention. M2M communication plays a crucial role in IoT, where various devices, sensors, and machines are connected to exchange information and perform tasks.

Furthermore, M2M benefits from enhanced capabilities like higher data speeds, lower latency, and increased device density which enables more efficient and reliable communication between devices.

The architecture of cognitive M2M has three essential elements which are listed as follows and depicted in Figure 4:

A. Central Control Unit (CCU) or Cloud Computing Network (CCN):

The CCU, plays a crucial role in managing and orchestrating the various functions within the M2M communication system. It often leverages CCFs to provide scalable and flexible resources for handling the complex tasks involved. The CCU is responsible for decision-making, resource allocation, and overall coordination of communication processes. It enables efficient utilization of computational resources, making it a key component in ensuring the responsiveness and reliability of the M2M network.

i. Heterogeneous Core Network (HCN):

The HCN is a fundamental element of the architecture, comprising advanced technologies such as massive MIMO, cognitive radios, and small cells. These technologies collectively contribute to the high-performance capabilities of the 5G network.

ii. Massive MIMO:

This involves the use of a large number of antennas at the base station, allowing for simultaneous communication with multiple devices. This enhances spectral efficiency and overall network capacity.

iii. Cognitive Radios:

These intelligent radios can adapt their transmission parameters based on the surrounding environment. They can dynamically adjust frequency, modulation, and power to optimize communication in real time, making the network more resilient and efficient.

iv. Small Cells:

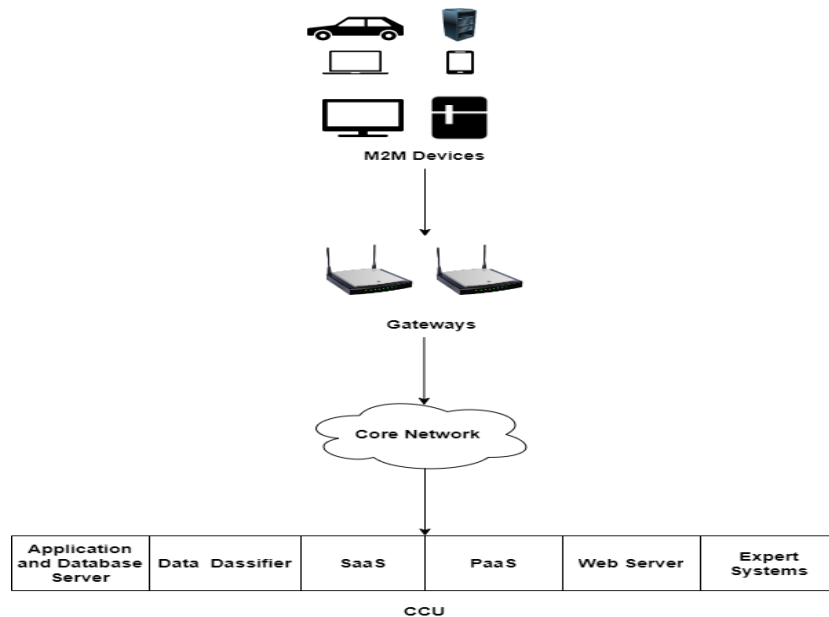
These are low-power, short-range base stations that complement the coverage of traditional macro-cells. Small cells are particularly beneficial in dense urban areas where network capacity needs to be augmented.

B. M2M Area Network:

The area network is characterized by its ability to support a vast number of connected devices, low-latency communication, and energy-efficient data exchange. The M2M architecture facilitates seamless communication among these devices, enabling them to transmit and receive data efficiently.

**Figure 4**

*Architecture of the M2M Communication*



As shown in Figure 4, M2M architecture involves various components that work together to enable seamless communication between devices. Here are some key elements in this architecture:

1. Devices and Sensors involves a wide array of devices and sensors equipped with communication modules. These devices can include IoT sensors, actuators, and other connected objects that generate and receive data.
2. 5G-RAN provides wireless connectivity that enables devices to communicate with the network. It includes base stations and other infrastructure components that facilitate high-speed and low-latency communication.
3. 5G Core Network is a fundamental component handling various functions, including user authentication, data routing, and mobility management. It supports the unique requirements of M2M applications, such as massive device connectivity and low-latency communication.
4. Network Slicing: M2M may utilize dedicated network slices to ensure optimized performance and resource allocation.
5. Edge Computing brings computational resources closer to the devices, reducing latency and improving real-time processing capabilities. This is especially important for M2M applications that require rapid data analysis and response times.
6. Low Latency and High Bandwidth are crucial for M2M applications, where timely and large-scale data transmission is often required.
7. Security Features Measures such as encryption, authentication, and access control to safeguard data.
8. APIs and protocols enable interoperability between devices, applications, and network components.

While M2M offers numerous advantages, it also presents several challenges that need to be addressed. The following are some of the main challenges:

1. Massive Device Connectivity: 5G networks are designed to support a massive number of connected devices. Managing the sheer volume of devices and ensuring efficient communication among them poses a challenge in terms of network scalability.
2. Security Concerns: with the proliferation of connected devices, there is an increased attack surface. Ensuring robust security measures, including

encryption, authentication, and access control, becomes crucial to protect M2M communications from cyber threats.

3. **Privacy Concerns:** as M2M communication involves the exchange of sensitive data, leading to privacy concerns. Addressing this challenge requires implementing robust privacy measures to protect user data and ensuring compliance with relevant regulations.
4. **Regulatory and Legal Issues:** Implementing M2M in 5G networks may face regulatory and legal challenges related to spectrum allocation, data privacy, and compliance with local regulations. Navigating these issues is crucial for successful implementation.
5. **Cost Management:** building and maintaining a robust 5G infrastructure can be expensive. Balancing the costs associated with deploying and maintaining the network with the benefits derived from M2M applications is a challenge.
6. **Energy Efficiency:** Many M2M devices operate on battery power, and energy efficiency is critical for their prolonged operation. Optimizing communication protocols and network configurations to minimize energy consumption is a challenge.
7. **Interoperability:** the diversity of M2M devices and applications may lead to interoperability challenges. Ensuring seamless communication between devices from different manufacturers and compatibility with various M2M platforms is essential.

The proposed protocol introduces innovations in authentication, encryption, and data integrity management tailored to the specific demands of M2M communication. By prioritizing the confidentiality, integrity, and availability of data in the M2M context, the solution of the suggested protocol aims to fortify the overall security posture of 5G networks.

Moreover, the protocol optimizes authentication efficiency, a critical factor in M2M scenarios where rapid and reliable communication is essential. Through a comprehensive approach that considers the intricacies of M2M interactions, this protocol seeks to contribute significantly to the enhancement of both 5G network security and the seamless



integration of interconnected devices. Furthermore, the potential impact of the findings extends beyond theoretical advancements, offering practical solutions to identified security vulnerabilities within the M2M landscape.

To conduct, the proposed 5G-AKA protocol addresses the specific challenges of M2M communication within 5G networks, aiming to establish a secure and efficient framework that aligns with the expanding role of interconnected devices in a digitally interconnected world.

This research introduces an innovative authentication protocol with the primary goal of enhancing the security of 5G networks. Addressing vulnerabilities within the 5G AKA mechanism, the protocol has been meticulously designed to demonstrate effectiveness and resilience against known attacks targeting 5G networks.

Beyond its application to 5G networks, the ES protocol plays a crucial role in fortifying the security of M2M communication. Its adaptability allows seamless integration into the 5G ecosystem, specifically addressing challenges associated with M2M interactions.

Throughout the subsequent sections, the research will delve into how the authentication protocol provides a comprehensive security framework for both 5G networks and M2M communication. Emphasis will be placed on key aspects such as low latency, scalability for diverse devices, and compliance with industry standards. This dual-purpose functionality represents a significant advancement in network security, offering a holistic solution to the evolving challenges posed by modern communication paradigms.

In this research, a comprehensive examination was conducted, delving into 52 articles, papers, journals, and dissertations across diverse domains. Notably, the study uncovered that M2M communication introduces distinct security and privacy concerns. In response to these challenges, the proposed approach emerged as a versatile solution, demonstrating its efficacy not only within 5G networks but also in the broader context of M2M communications. Moreover, this research positions the proposed protocol as a robust and adaptable tool, offering security and privacy measures beyond the specific requirements of 5G networks. As the narrative unfolds, it becomes clear that the proposed protocol stands ready to address the evolving landscape of M2M interactions, making it a

valuable asset in ensuring the confidentiality and integrity of communication in various scenarios.

# **CHAPTER 4**

## **5G NETWORK, AKA PROTOCOL, AND SECURITY CONCERNS**

Throughout this chapter, an exploration unfolds, delving into a comprehensive background discussion of the 5G network, the 5G AKA protocol, and their vulnerabilities. This journey is designed to equip readers with a nuanced understanding of the intricate workings of these two pivotal components in modern telecommunications.

### **4.1 The 5G Architecture**

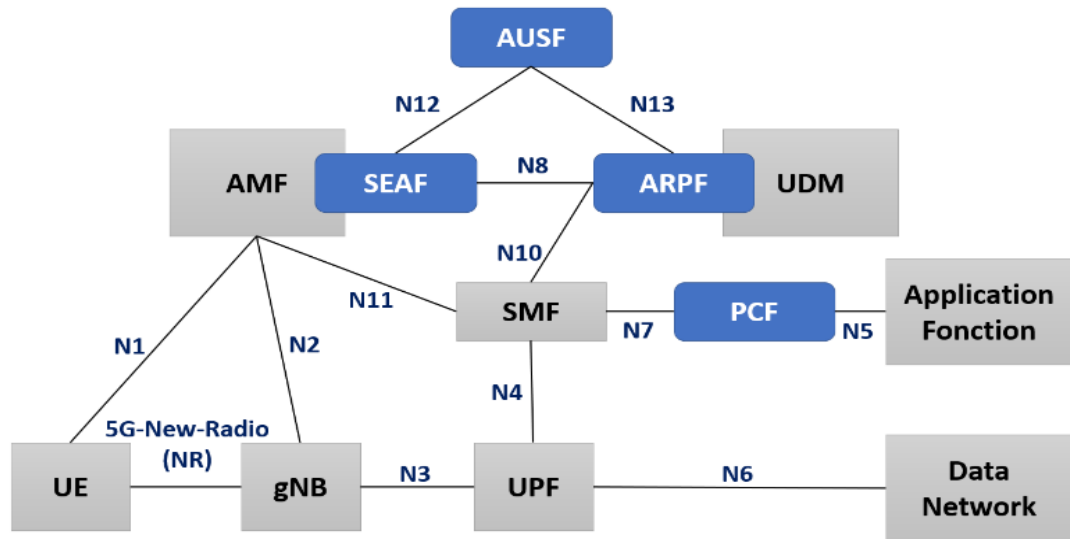
The 5G standards not only cater to current requirements but also anticipate future needs, particularly as society advances into an era marked by the proliferation of IoT systems and autonomous vehicles, potentially reaching hundreds of billions of connected devices. Addressing these evolving demands, the next generation of wireless devices and communication infrastructures is expected to integrate diverse technologies to establish a wireless network capable of meeting the evolving expectations. Despite these overarching goals, the 5G architecture comprises two principal sections: the 5GC and the NG-RAN.

Functioning as the central component of 5G technology, the 5GC is primarily tasked with managing data and plane operations. It plays a pivotal role in consolidating data traffic, delivering various network services, establishing communication with UE, and providing multiple layers of security. Additionally, the 5GC network adopts a SBA tailored for cloud-based services, enhancing security measures, authentication processes, session management, and the aggregation of traffic from connected devices. The intricate interconnection of network functions is essential to realizing these functionalities.

To visually elucidate the architecture of the 5G network and the interrelationships among its components, Figure 5 is presented, illustrating the network's structure and delineating potential points of vulnerability. This figure serves as a valuable reference for comprehending the network's complexity and identifying areas that may pose security challenges.

**Figure 5**

*Architecture of the 5G Network*



Here is an outlined depiction of the key entities within the 5G system, detailing them as follows:

Control Plane (CP) oversees signaling, authentication, and session control. Its responsibilities include establishing and maintaining connections between network devices, managing network resource allocation, and implementing security measures to protect the network and its users (Sharma, 2019).

UP manages the transfer of user data, encompassing voice and video. Its role involves ensuring efficient and reliable data transmission between network devices and overseeing QoS to guarantee users the optimal experience (Sharma, 2019) (Koustsos, 2019).

1. The Access and Mobility Management Function (AMF) is integral to the CP, playing a key role in overseeing network access and ensuring seamless user mobility. It performs various functions, encompassing authentication and authorization, session management, mobility management, and security management (Chen et al., 2016).
2. The Security Anchor Function (SEAF) is a crucial component within the UP, responsible for delivering security services for user data transmitted over the network. It also performs essential functions such as encryption

and decryption, integrity protection, data integrity preservation, and the management of user-plane security associations (Khan, 2021).

3. The Session Management Function (SMF) integral to the CP, is responsible for the administration of user sessions and their associated network resources. Additionally, it performs various functions, including session establishment, policy enforcement, mobility management, network slicing, and charging (Kim, 2021).
4. The Packet Data Network (PDN) serving as the infrastructure and connectivity provider, the PDN facilitates the transmission of data between devices using packet-switched technology. This method is predominant in data transmission over the internet and other networks (Han, 2019).
5. The Authentication Server Function (AUSF) is crucial for ensuring that only authorized devices and users can access the network, guaranteeing the security of communications between the user device and the network. Furthermore, it manages additional functions such as security context management, AKA procedure, subscription authentication, and collaboration with other functions (Jiang, 2020).
6. Unified Data Management (UDM) empowers organizations to enhance their competitive edge by utilizing their data to make more informed decisions (Conti, 2016).
7. The Unified Data Repository (UDR) functions as a centralized storage system, acting as the sole authoritative source for an organization's data. It collaborates with the UDM for enhanced efficiency. Furthermore, it offers various advantages to organizations, including centralized data storage, enhanced data quality, convenient data access, and strengthened data security (Ouaissa, 2020).
8. The Authentication Credential Repository and Processing Function (ARPF) furnishes a secure and dependable mechanism for verifying and granting user access to network services. By guaranteeing that only authorized users can access network resources, the ARPF aids in averting

unauthorized entry and potential data breaches (Adem, 2015) (Yungaicela, 2021).

9. Policy and Charging Control (PCC) is a network framework designed for telecommunications service providers. It empowers operators to regulate policies governing data traffic, ensuring QoS, efficient resource management, and accurate billing for diverse services within the network (Ouaissa, 2020).
10. The Policy Control Function (PCF) operates in collaboration with the PCC architecture. Its responsibilities include policy enforcement, charging enforcement, management of the Policy and Charging Information Function (PCIF), and overseeing the PCC (Behrad, 2021) (Baskaram, 2020).

In Figure 5, the 5G radio access involves advanced base stations that function as the connection point between mobile devices and the 5GC network. UE devices transmit data to these base stations through a 5G radio link known as the gNB station. The gNB performs functions similar to the Evolved NodeB (eNB) entity in the LTE system, albeit with some differences. These differences include managing QoS based on flow rather than medium and handling domain sections on the wireless connection.

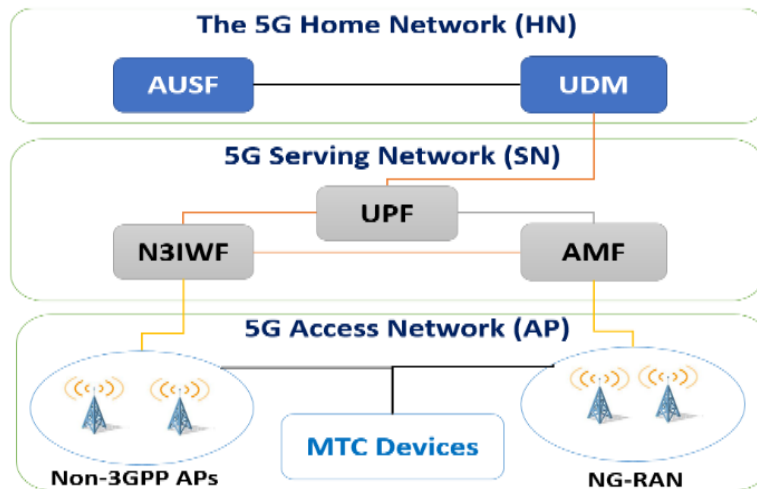
The central 5G network is well-suited for virtualizing network resources and features a distinct separation between the CP and UP. This design results in various entities overseeing mobile attachment, location management, and bearer creation within the 5G network. The AMF entity establishes a NAS connection with the mobile UE, registering devices and managing their location across public and private networks. Positioned alongside the SEAF, the AMF entity maintains the root key or anchor key related to the utilized network. Simultaneously, the SMF entity governs PDN sessions.

The UP Function handles the transport plan functions for the 5G Core network. Meanwhile, the PCF entity manages flows at both the SMF and AMF entity levels, enabling precise control of authorized flows based on the mobile UE's location.

Figure 6 illustrates the structure of group authentication for MTC systems. The architecture of the 5G network is segmented into three domains, categorized as follows:

**Figure 6**

*Network Architecture*



- 5G Access Network (AN): Consisting of two elements, the 5G NG-RAN and massive Machine Type Communication Devices (mMTCs). The NG-RAN comprises advanced gNBs and non-3GPP APs like Wi-Fi access points, facilitating connectivity for devices. The mMTCs encompass IoT devices, sensors, and M2M communication devices slated for integration into the 5G network.
- 5G Serving Network (SN): Its role encompasses providing access and facilitating communication for mMTCs within the 5G framework. Authentication, device management, and CP functions, along with security through the Security Edge Protection Profile (SEPP), are overseen by the AMF. The 5G-AKA protocol enables mutual authentication via the AMF/AUSF when an mMTC connects to the SN through the NG-RAN. For non-3GPP access networks, security levels are determined via Internet Key Exchange version 2 (IKEv2) through the Non-3GPP Interworking Function (N3IWF) before mutual authentication using Extensible Authentication Protocol EAP-5G via the AMF/AUSF. Additionally, the SN incorporates essential components such as the SMF and UPF. The SMF manages communication sessions, while the UPF handles data plane functions. The AMF plays a pivotal role in the SN, overseeing authentication, device management, and CP functions, ensuring the smooth operation of the network.

The collaborative efforts of these components contribute to the efficient functioning of the 5G Serving Network.

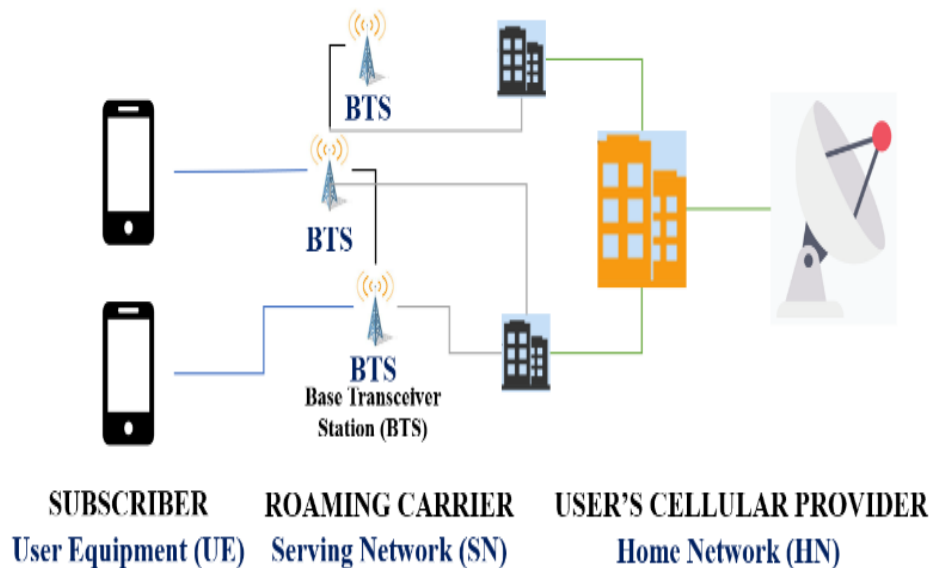
- 5G Home Network (HN): Delivers data management and authentication services for mMTCs utilizing the UDM and AUSF. These components can process authentication requests from both 3GPP and non-3GPP networks. It is assumed that within the mMTC group, a leader known as the MTCDL is designated based on communication capabilities.

## 4.2 The 5G-AKA and EAP-AKA Protocol Architectures

The AKA protocol serves as a secure method for entities to exchange information using symmetric and asymmetric cryptography keys. In this process, one party issues a challenge, and the other node responds with the correct answer, establishing mutual authentication. Specifically, when referring to the AKA protocol, it pertains to the 3G AKA version. Moreover, the application of 3G AKA can extend to 2G systems, operating similarly to its role in 4G networks. It's important to highlight that the cellular network consists of three essential components: UE, SN, and HN, as depicted in Figure 7.

**Figure 7**

*Subscriber Mobility Communication Architecture*



The UE serves as a potent device utilized by subscribers, encompassing advanced smartphones and IoT gadgets. Its identity is safeguarded by the SUPI stored in the Universal Subscriber Identity Module (USIM). In the realm of 5G, the SUPI assumes a



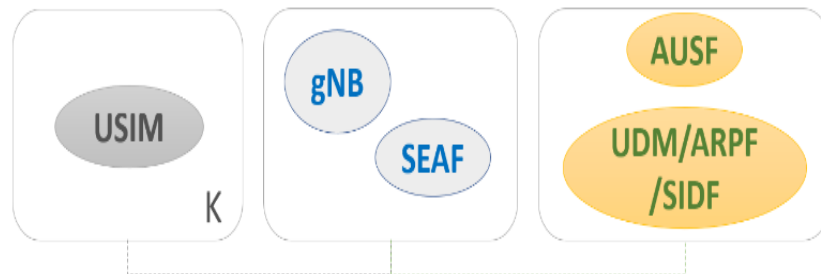
role analogous to the International Mobile Subscriber Identity (IMSI) in preceding standards, with the USIM taking charge of preserving subscriber-related records and executing security functions. The term "subscriber" denotes the combination of UE and USIM, while the HN holds the responsibility for subscriber registration and authentication, ultimately ensuring network protection and security. The SN represents the network to which the UE is connected, distinct from the HN to which the subscriber is registered. This scenario may occur when a subscriber moves to areas lacking a base station from their registered HN, as seen during roaming.

Comprehending the fundamental structure and security attributes of the AKA scheme doesn't necessitate understanding the specific components within SNs and HNs. It is crucial to recognize that while UE and SN engage in communication through an exposed transmission pathway, the exchange of data between SN and HN occurs through a secure connection, ensuring confidentiality, integrity, authenticity, and non-repudiation. Previous implementations, like 4G-LTE, also employed secure communication channels, and it is advisable to utilize encrypted channels in 5G.

Each UE is furnished with a UICC capable of hosting a USIM application. This USIM application securely holds a pre-shared key with the subscriber's HN and includes a distinctive identifier known as SUPI, akin to the one used in 4G-LTE IMSI. The HN signifies the Mobile Network Operator (MNO) certifying the UE, while the SN facilitates roaming services when the UE enters its coverage area. Additionally, 5G's SBA has introduced novel elements for 5G-AKA, such as SEAF, AUSF, UDM, ARPF, and Subscription Identifier De-concealment Function (SIDF), as illustrated in Figure 8 (Kiyemba, 2020).

**Figure 8**

*The 5G Units in the Authentication Mechanism*



A USIM is a specialized SIM card employed in 3G and 4G mobile networks. This compact and removable smart card is inserted into mobile devices, such as smartphones or tablets, to validate and authorize users on the network. The USIM stores critical information, including the subscriber's phone number, authentication keys, and other security data necessary for secure and efficient communication with the mobile network. Notably, the USIM is engineered to provide heightened security features compared to traditional Subscriber Identity Module (SIM) cards and includes extra functionalities like the storage of contacts, messages, and other data (Kiyemba, 2020).

Conversely, the gNB plays a pivotal role in 5G wireless networks by acting as the intermediary between UE and the core network. It undertakes essential tasks such as modulation, demodulation, scheduling, and the allocation of radio signal resources, accommodating diverse deployment scenarios like macro, micro, and picocells. gNBs distinguish themselves through superior energy efficiency, scalability, and flexibility in contrast to the base stations of previous wireless networks. They are well-equipped to support advanced 5G network features such as massive MIMO, beamforming, and ultra-low latency.

SIDF serves as a network function utilized in both 4G-LTE and 5G networks to oversee and store subscriber identity data, encompassing elements like IMSI and MSISDN. It holds responsibilities in authenticating and authorizing subscribers, managing their subscription details, and facilitating mobility across diverse network domains. As a pivotal component of the EPC, SIDF plays a crucial role in ensuring secure and seamless communication for subscribers within 4G and 5G networks.

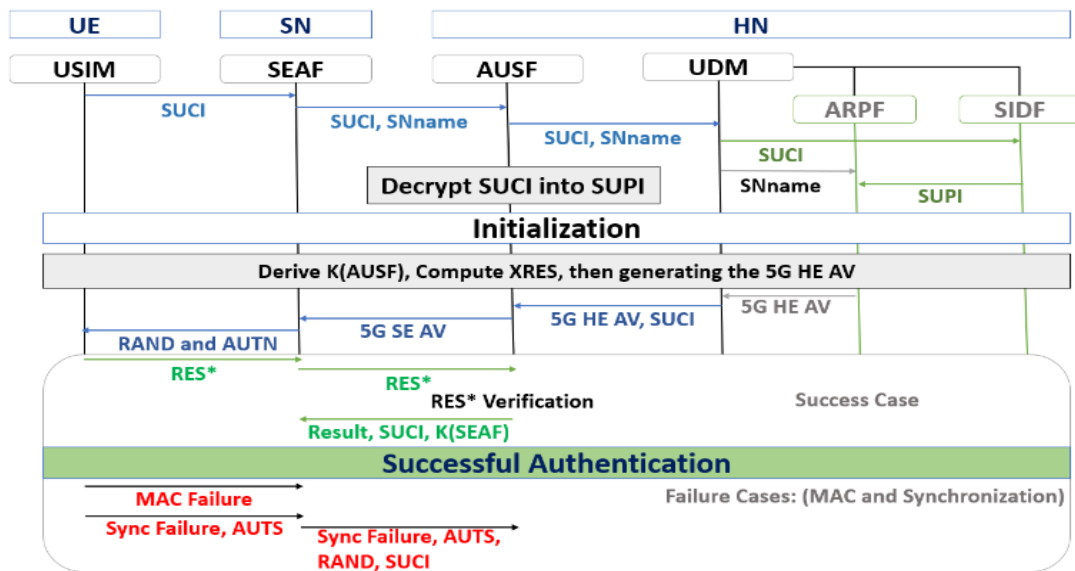
Within the 5G network architecture, core components include gNB and UPF. While gNB operates as a BS for wireless communication, providing radio access to the network,

UPF serves as a SEAF responsible for safeguarding the core network. SEAF intercepts and scrutinizes all traffic between the UE and the core network to enforce security policies. AUSF manages UE authentication, security keys, and generates encryption keys and authentication tokens for secure communication. UDM, a core network component, oversees user and network data, offering critical functionalities like ARPF and SIDF for network management and control.

ARPF establishes the access control mechanism based on user identifiers and regulations, while SIDF maps the Subscriber Concealed Identifier (SUCI) to the SUPI. Communication between the UE and SN occurs over an insecure radio interface. Security functions dispersed across the network, including SEAF and AUSF, deliver confidentiality, integrity, mutual identity verification, and tamper-proofing for communication between the SN and HN, in accordance with 5G standards. The 5G-AKA approach is employed to establish secure communication, involving the transmission of sensitive credential parameters through a secure link between HN and SN, encompassing  $K_{SEAF}$ , SUPI, and SQN. Key security objectives include authenticating subscribers with HN/SN, ensuring confidentiality and integrity of sensitive credential parameters, preserving user anonymity, and preventing tracking or tracing by potential attackers (as shown in Figure 9).

**Figure 9**

*The 5G-AKA Protocol's Timeline Diagram*



Within 5G systems, two AKA protocols are recognized: 5G-AKA and EAP-AKA. This section provides a concise overview of these AKA methodologies.

### **4.2.1 The 5G-AKA Protocol**

Figure 9 illustrates a range of outcomes within the 5G-AKA procedure, encompassing both successful scenarios and potential failures like Media Access Control (MAC) failure and Synchronization failure. Beginning with MAC Failure, this can occur due to protocol implementation errors, incorrect key usage, or malicious attacks. In such cases, the device should initiate a new authentication attempt with fresh keys or seek assistance from the network operator. Adhering to standard specifications and security guidelines is essential to minimize the risk of MAC failures and related security issues.

On the other hand, Synchronization Failure may stem from factors like network congestion, delays, clock drifts, or packet loss. These issues may result in delays in message transmission, causing a misalignment between expected and actual message timing. Identifying the root cause is crucial, and corrective actions should be taken, such as optimizing network performance, adjusting clock synchronization settings, or implementing error correction mechanisms to mitigate packet loss.

In the event of a successful outcome, indicating the device's access to the network for data exchange, the device is equipped with the necessary security keys. This ensures the confidentiality, integrity, and authenticity of the exchanged data with the network.

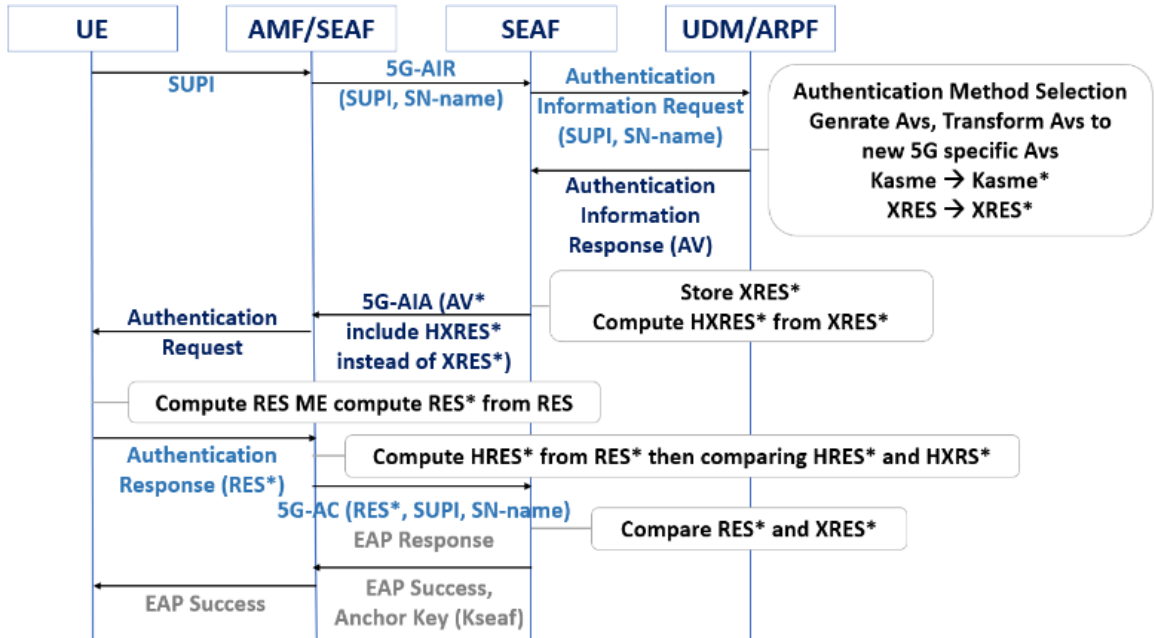
### **4.2.2 EAP-AKA Protocol**

The standard authentication structure of the EAP-AKA protocol involves four device categories: AAA protocol server, high and low-power BS, and UE. The AAA platform, situated in the core network, serves as the authentication server for AAA. The UE stores network identity information and the encryption and decryption algorithms needed for authentication. Within the ultra-dense 5G wireless network, two types of BSs exist: micro-BS and macro-BS. This study primarily explores handover authentications among small cells managed by different micro-BSs. In the traditional authentication architecture of the EAP-AKA protocol, each

time the protocol is executed, the AAA server generates a new authentication vector by applying the AKA algorithm (refer to Figures 10 and 11).

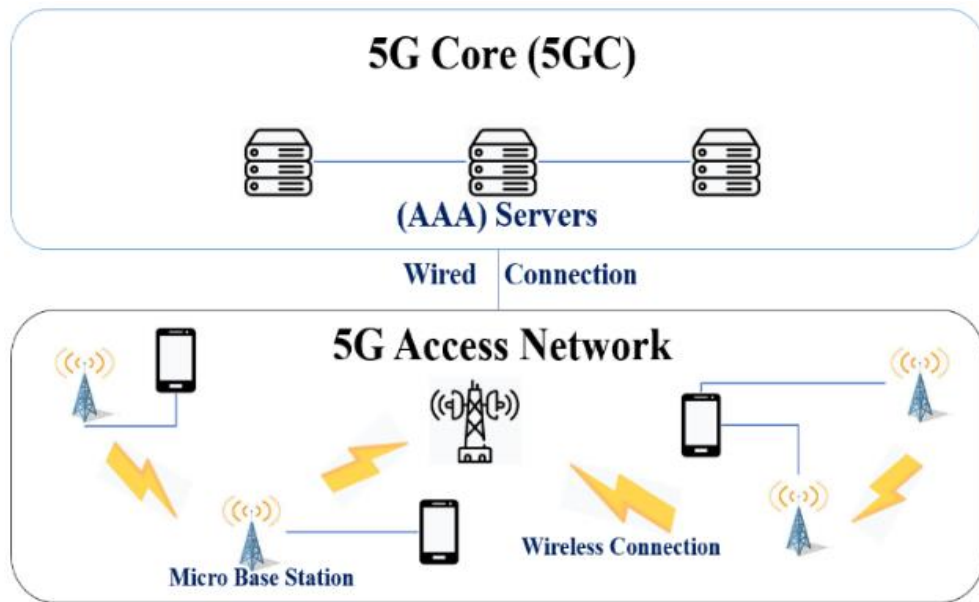
**Figure 10**

*The EAP-AKA Protocol's Timeline Diagram*



**Figure 11**

*Traditional Authentication Architecture*



The frequent utilization of the EAP-AKA protocol can lead to network congestion and significant authentication delays. Two proposed alternatives are

the Full EAP-AKA protocol and the MEC re-authentication protocol. Both methods build upon the original EAP-AKA protocol, known for its lightweight and straightforward design relying on symmetric cryptographic encryption and decryption. The EAP-AKA protocol is a versatile and effective authentication method supporting bidirectional authentications in various scenarios.

For re-authentication, the Full EAP-AKA protocol necessitates sharing specific information within the AAA system and either the terminal or the distributed computing node. To enhance security and privacy protection in 5G wireless networks, a shorter pseudonym is adopted for users, reducing transmitted traffic and improving authentication efficiency. The MEC re-authentication protocol employs a one-way hash function to expedite authentication information generation while ensuring security.

Figures 9 and 10 illustrate the similarity in calculating  $RES^*$  in the ME for 5G-AKA and EAP-AKA, as well as  $HRES^*$  in the SEAF corresponding to  $HXRES^*$  in the AUSF. The UE authentication process involves the SEAF, AUSF, and UDM/ARPF. The SEAF, part of the AMF, collaborates with the AUSF to acquire authentication data from the UDM, while the ARPF stores subscriber profiles and security-related information. During authentication, the UE sends its SUPI to the SEAF, initiating the process. If successfully authenticated, the SEAF communicates a 5G-AC message in the 5G-AKA process. However, these messages fall short in protecting against fraudulent Update Location requests, necessitating a link between authentication results and the location update procedure. Notably, the transformation of Authentication Vectors (AVs) differs between 5G-AKA and EAP-AKA.

### **4.3 5G Network Security: Loopholes and Services**

The utilization of high-ultra frequencies in 5G networks leads to smaller cell sizes, resulting in more frequent handovers and increased network traffic. This poses security risks during connection transfers, necessitating a secure handover protocol. Key requirements include confidentiality, message authenticity verification, and mutual authentication.

While the 5G-AKA protocol provides some security measures, vulnerabilities exist. Potential risks include impersonation, false registrations leading to synchronization issues, and computational load on ARPF and AUSF. Developing a secure AKA protocol for IoT-based applications is crucial to mitigate fraudulent requests. However, the current authentication process is susceptible to attacks, such as message interference and the use of fake subscriber numbers.

Prioritizing security features within the network design architecture is crucial to thwart known security threats. Neglecting the implementation of security controls can result in substantial financial costs and the compromise of data post an attack. Service providers might be required to invest in additional equipment for effective threat mitigation. Without the integration of security measures, vulnerabilities are likely to persist in the mobile network over an extended period. Therefore, for a secure network, continuous monitoring and analysis of signaling traffic at the network boundary are imperative to identify configuration errors and potential security threats.

Enabling this functionality necessitates the deployment of specialized threat detection systems capable of real-time traffic analysis. Ideally, these systems should be proficient in instantly blocking malicious activities without negatively impacting the network's performance.

In 5G networks, the establishment of a secure connection between the UE and the base station gNB-DU is paramount. The exchange of a secret key is imperative to ensure private and secure communication. With the frequent handovers between different base stations in 5G networks, the use of distinct keys for each session becomes crucial to maintain connection security. In this context, the ES-AKA protocol emerges as a solution designed to satisfy these specific security requirements, thereby safeguarding the connection from potential attacks:

- Confidentiality: Preserving the secrecy of the key exchanged between the UE and gNB-DU is imperative, aiming to prevent unauthorized access. Implementation of measures is necessary to secure the key and avert any disclosure that could jeopardize the security of communication.

- Integrity: Measures should be enacted to prevent unauthorized entities from manipulating or altering signaling messages, ensuring the ongoing security of the communication channel.
- Mutual Authentication: This security measure mandates both the UE and gNB-DU to verify each other's identity, mitigating potential malicious attacks such as False Base Station (FBS), false MR, and location spoofing. Mutual authentication establishes trust between entities, contributing to overall security.
- Key Exchange: Ensuring the security of communication between the UE and the 5G radio unit necessitates the secure negotiation of keys designated for encryption and decryption.
- Perfect Forward Secrecy (PFS): This security measure guarantees that temporary encryption keys used in a session remain unrelated to keys from previous or subsequent sessions. It ensures that even if an attacker gains access to keys from one session, they cannot exploit them to breach other communication sessions. PFS safeguards the confidentiality and integrity of communication by isolating the compromise of a single session's keys from impacting the security of other sessions.

The 5G-AKA protocol employs a challenge-response mechanism involving four communication units: UE, ARPF, SEAF, and AUSF (Khan, 2021). Though it meets many security prerequisites, identified vulnerabilities include the risk of IMSI-catcher attacks, potential misuse of fake base stations, synchronization issues due to false registrations, and susceptibility to replay attacks. Countermeasures such as TMSI and encryption for IMSI protection are suggested, and addressing these vulnerabilities is crucial for ensuring the security and stability of the 5G system.

The following outlines the security services provided for the 5G system:

- Authentication plays a crucial role in ensuring the legitimacy of communicating entities and verifying message integrity. Beyond the traditional UE and MME authentication, the 5G context involves third parties like service providers, necessitating a flexible authentication approach. To address the need for rapid authentication in line with 5G's low-latency



requirement, a proposed solution involves an SDN-enabled fast authentication scheme with weighted secure-context-information transfer. Additionally, enhancing security services in 5G networks is suggested through the adoption of a public-key-based AKA. Furthermore, As the number of applications in 5G increases, the importance of message authentication grows, accompanied by new challenges. An efficient solution proposes the use of a CRC-based method capable of detecting both random and malicious errors without imposing additional bandwidth consumption (Liu, F., 2018) (Huang, 2019).

- Confidentiality involves ensuring both data confidentiality and user privacy. Data confidentiality protects against passive attacks, restricting access to authorized users, while privacy safeguards legitimate users from external control. The diverse applications in 5G generate substantial user privacy data, such as transportation path and health monitoring records. Symmetric key encryption is commonly used for data confidentiality but requires secure key distribution. To counter powerful attackers, various digital signature mechanisms are proposed, including differential private algorithms for location privacy and protocols for secure and privacy-aware real-time video broadcast services in Transportation Cyber-Physical Systems (TCPS).
- Availability emphasizes constant accessibility for legitimate users, crucial for optimal performance. Threats like DoS attacks and jamming can disrupt services. Physical Layer Security solutions, such as Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS), enhance availability by resisting jamming. DSSS scrambles data signals with a random code, while FHSS rapidly switches carrier frequencies. However, FHSS may have limitations against jamming. To optimize efficiency, a proposed method involves time-hopping spread spectrum based on a mathematical algorithm. Asset allocation is employed to improve the detection of availability violations.
- Integrity: ensuring data integrity is essential and it safeguards information from unauthorized alterations. Insider malicious attacks, including message falsification and spoofing, present challenges due to attackers holding valid

identities. The establishment of an integrity key through mutual authentication is instrumental in providing integrity services, while authentication schemes contribute to maintaining message authenticity.

The security and privacy framework of 5G revolves around three key elements. Firstly, all security threats applicable to 5G's predecessors are still relevant to 5G and future networks. Secondly, the proliferation of interconnected devices, users, IoT devices, and emerging stakeholders will witness a substantial increase in the 5G landscape. Lastly, the adoption of new networking applications will introduce distinct challenges in terms of data protection and confidentiality.

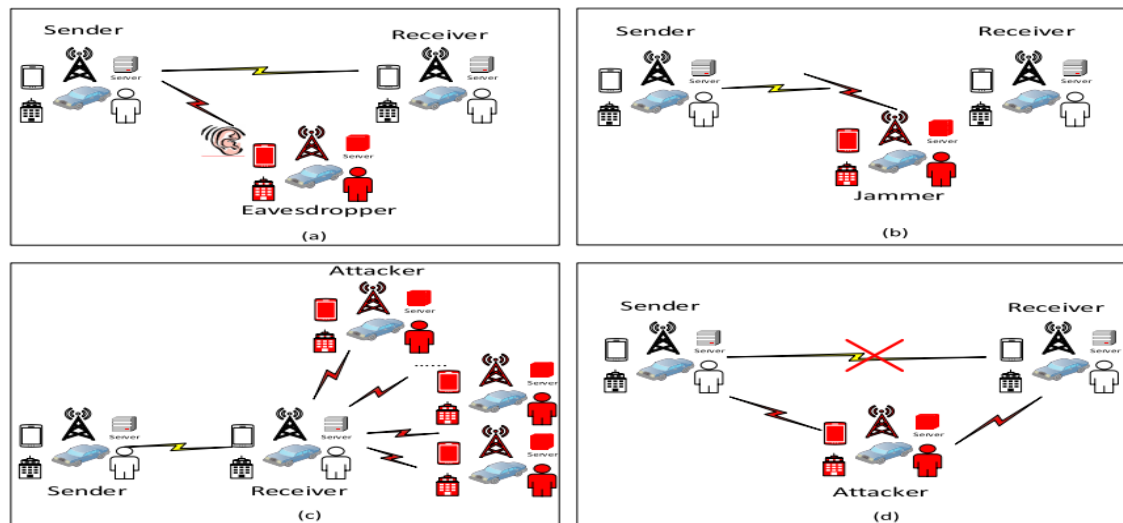
Security Threats within the standardized AKA Protocol:

- **Bogus SN Attack:** The deceptive Bogus SN Attack involves an attacker using a fake SN to illicitly access private member details. The unauthorized SEAF stores SUCI and HN name after the initiation of the 5G-AKA scheme by the UE. Through transmission of AUTN and Random Number (RAND) to the UE, the rogue SEAF exploits AUSF verification to gain access to the UE's SUPI and  $K_{SEAF}$ . With this key, the attacker decrypts all UE messages, leading to the leakage of communications without detection. Additionally, the attacker can respond to the HN using SUCI and AUTN (Chen et al., 2016).
- **ToRPEDO Attack:** It sends silent paging messages to a target device, making it reveal its location. The attacker triggers the attack by initiating and retracting numerous voice calls and texts. This exposes the device's location through the paging protocol, leading to additional attacks: IMSI Cracking and Piercer. These reveal the IMSI, allowing tracking if the phone number is known. Intruding voice calls compromise the TSMI, exposing the device's location (Khan, 2021).

In Figure 12, four attacks are detailed, classified as either passive or active. The illustration highlights the firewall features capable of mitigating these attacks, accompanied by corresponding methods for prevention or avoidance. This section narrows its focus to security incidents occurring within the Physical (PHY) and MAC layers, emphasizing the key distinctions in security between wireless and wired networks.

**Figure 12**

*Attacks in 5G Networks*



Here is a detailed explanation of the four most significant attacks within the 5G-AKA mechanisms being depicted in Figure 12:

- A. Eavesdropping and Flow Analysis: Eavesdropping is a passive form of attack, involves intercepting messages intended for others without disrupting regular communication. Figure 12.a illustrates how eavesdropping operates. Encryption is a common preventive measure against this type of attack, making it challenging for eavesdroppers to directly intercept signals. However, even with encryption, traffic communication analysis, a passive attack, can still reveal details about communication parties, such as location and identity, by analyzing the data flow. Unlike eavesdropping, traffic analysis does not disrupt communication but poses challenges for privacy. The effectiveness of encryption depends on the strength of cryptosystems and the eavesdropper's computing capabilities. Advances in computing and data analysis technologies pose challenges to existing methods, especially as 5G wireless networks introduce new complexities. HetNet in 5G networks, with its multiple antennas, adds to the challenge. While cryptographic methods remain mature, recent attention in PLS research offers alternative approaches to address eavesdropping (Piqueras, 2019).

- B. Jamming: Unlike data interception and flow analysis, jamming is a disruptive attack capable of completely halting communication among legitimate users. Figure 9(b) depicts how a malicious node deliberately creates interference, disrupting data communication or impeding authorized subscribers from utilizing wireless bandwidth. Detection-oriented solutions are often employed to counter active attacks like jamming. Secure communication methods, such as DSSS and FHSS, are commonly applied at the PHY layer to counter jamming by spreading signals across a broader spectral bandwidth. However, it's worth noting that DSSS and FHSS-based anti-jamming schemes may not be universally suitable for specific applications within 5G wireless networks.
- C. DoS and DDoS: Security in 5G networks contends with vulnerabilities inherited from previous networks, where DoS attacks can impact any IoT device, not limited to ultra-fast wireless infrastructures. The Diameter Signaling Protocol (DSP), pivotal for data transmission tasks, faces security flaws, making it a prominent target for diverse attacks. Despite a decrease in DSP attacks post-2018 and 2019, the failure to coordinate subscriber location for signaling in telecommunication networks leaves them susceptible to DoS attacks, challenging their differentiation from legitimate traffic. Global security leader Positive Technologies warns that without adequate measures, 5G networks may retain vulnerabilities akin to previous networks. They offer recommendations to telecommunication companies providing 4G and 5G services (Chen et al., 2016). DoS attacks, capable of depleting network resources, jeopardize network availability. Jamming can serve as a tactic for initiating a DoS onslaught, while DDoS arises when multiple distributed attackers are involved. Both DoS and DDoS attacks operate in real-time, manipulating data and targeting diverse network hierarchies. Current detection methods are prevalent in identifying DoS and DDoS attacks. The escalating ubiquity of connected devices in 5G technology makes DoS and DDoS threats significant for network operators. These attacks may target network infrastructure or individual devices/users, impacting components like battery, memory, disk, CPU, radio, actuator, and sensors (Fang, 2018).

D. MitM Attacks: MitM entails an attacker clandestinely monitoring and manipulating the communication channel between two legitimate parties. The attacker gains control over the pipeline, allowing them to alter or substitute signal transmissions between the parties, compromising the confidentiality, integrity, and availability of the transmitted data (Kiyemba, 2020). MitM attacks feature prominently in conventional security breaches, as highlighted in the Verizon investigation report. Historically, attackers employed MitM attacks based on false base stations, luring legitimate users to connect to a deceptive base station. However, mutual authentication often serves as a preventive measure against this type of attack in legacy cellular networks.

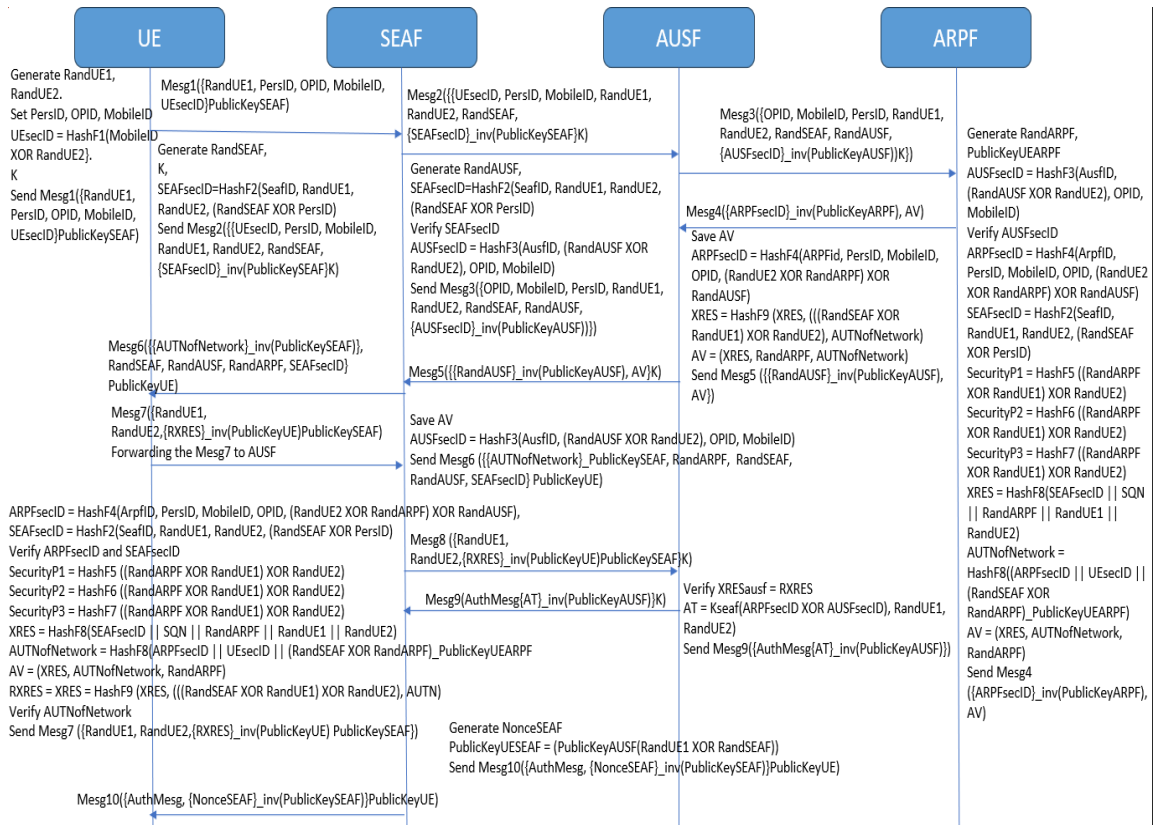
# CHAPTER 5

## PROPOSED PROTOCOL: ES-AKA METHOD

This section presents a comprehensive description of the proposed 5G-AKA protocol, ES-AKA, detailing its 10-step process. This protocol has been meticulously designed to establish a secure and resilient communication link between the following nodes: UE, SEAF, AUSF, and ARPF. Each step of the protocol is intricately crafted to address potential security threats, ensuring the confidentiality, integrity, and robustness of the communication exchange. The ES-AKA protocol aims to address the identified weaknesses discussed in the literature review chapter, maximizing enhancements in comparison to both standardized and suggested protocols (As shown in Figure 13).

**Figure 13**

*Timeline Diagram of the Proposed Protocol*



## 5.1 Full Description of the Proposed Protocol

The 10-step authentication protocol is a highly secure mechanism designed to address various security threats within the 5G network. Each carefully orchestrated step ensures the confidentiality, integrity, and resilience of the communication link.

In the initial phase, the UE triggers authentication by generating random values and encrypting critical information using an asymmetric key (PublicKeySEAF). This foundational step establishes a secure groundwork for subsequent communication with the SEAF, guaranteeing the confidentiality and integrity of exchanged data.

The SEAF continues the authentication sequence by generating randomness and computing essential parameters. The resulting SEAFs, along with the encrypted authentication message (Mesg2), contribute to the robustness of the authentication process.

The AUSF plays a pivotal role in the subsequent steps, initiating communication with the ARPF. AUSF generates randomness, computes parameters, and transmits a securely crafted message (Mesg3), fortifying the authentication sequence and enhancing overall network security.

ARPF, in turn, engages with AUSF, generating randomness and verifying received parameters. The authentication vectors and secure message (Mesg4) contribute to a secure communication link, demonstrating the meticulous design of the protocol.

AUSF then communicates securely with SEAF, preserving authentication vectors and transmitting a secure message (Mesg5). This phase ensures the confidentiality and integrity of exchanged information, reinforcing the security of the broader network infrastructure.

SEAF proceeds to engage with the UE, storing authentication vectors and crafting a secure message (Mesg6). The encrypted message guarantees the confidentiality and integrity of the information transmitted, highlighting the robust nature of the communication link.

The UE responds to SEAF, verifying cryptographic parameters and generating a secure message (Mesg7). This step, encapsulating the expected result of the authentication process, contributes to the overall security of the communication link.

SEAF, serving as a conduit, forwards authenticated data to AUSF, verifying integrity and transmitting a secure message (Mesg8). This forwarding mechanism plays a pivotal role in maintaining the integrity and security of the authentication process within the broader 5G network architecture.

AUSF, in turn, meticulously verifies XRESausf against RXRES, generating a cryptographic key AT. The transmission of a secure message (Mesg9) encapsulates authentication-related information, ensuring the confidentiality and integrity of the authentication token.

In the final phase, SEAF orchestrates a sequence of steps to establish a secure communication link with the UE. The generation of a distinctive cryptographic nonce (NonceSEAF) and the transmission of a secure message (Mesg10) contribute to the resilience and effectiveness of the communication link.

The protocol's adeptness in safeguarding against known attacks underscores its reliability and competence in the realm of 5G network security. The meticulous design, cryptographic operations, and verification mechanisms at each step collectively contribute to the protocol's strength and resistance against various security threats.

**Table 3**

*Parameters of the ES-AKA Protocol*

Parameters being used in the ES-AKA	Definition
RandUE1, RandUE2	Two random values generated by the UE.
RandSEAF, RandAUSF, RandARPF	Random values generated by the SEAF, AUSF, and ARPF respectively.
persID	Stands for Personal ID and represents the Serving Network in the standardized AKA protocol.
opID	Refer to Operator ID and Home Network.
MobileID	Refer to the Subscriber Identity also known as SUPI.
HashF1, HashF2, HashF3, HashF4, HashF5, HashF6, HashF7, HashF8, HashF9	These are hash functions which were used to compute numerous parameters including UEssecID, SEAFsecID, AUSFsecID, AUTNofNetwork, etc.
seafID, ausfID, ARPFid	These are the identities of the SEAF, AUSF, and ARPF respectively.
UEsecID	Secrete identity of the user's device which is computed as follows HashF1{MobileID XOR RandUE2}.
SEAFsecID, AUSFsecID, ARPFsecID	Secrete identity of the SEAF which is basically computed in the SEAF node. Similarly, for the AUSF and ARPF.



**Table 3** (continued)

*Parameters of the ES-AKA Protocol*

Parameters being used in the ES-AKA	Definition
PublicKeyUE, PublicKeySEAF, PublicKeyAUSF, PublicKeyARPF	Those are public keys which are used in the process of the authentication phase to encrypt the exchanged messages (e.g.: Mesg1: UE to SEAF, Mesg2: SEAF to AUSF, etc)
PublicKeyUEARPF	It is key shared between these two nodes UE and ARPF to have a mutual authentication.
Mesg1, Mesg2, ..., Mesg9, Mesg10	These messages contain parameters which were either generated, computed, set, received-composed and are encrypted.
Verify SEAFsecID,	The secrecy Identity of the SEAF to be authenticated.
SecurityP1, SecurityP2, SecurityP3	Refer to security properties were computed in the ARPF node in order to be used in the XRES and verify the authenticity of the request.
XRES	XRES is the Exclusive Response also is a challenge provided by the ARPF in order to authenticate the UE.
RXRESausf	Which is challenge-response made through the AUSF node.
AUTNofNetwork	Generates an Authentication Token.
AV, AVausf	Stands for Authentication Vector and verifies the identity of a user or device.
AT	Finalization of the Authentication Token.
AuthMesg	Mutual Authentication granted for the UE and the Network.
K	Symmetric Key

## 5.2 A Detailed Description of the 10 Steps Involved Within the Authentication Process

### Step 1: UE → SEAF - Authentication Initialization

The UE initiates authentication by generating random values (RandUE1 and RandUE2) and setting parameters such as persID, opID, and MobileID. To enhance security, UEsecID is computed using the hash function (HashF1). The UE prepares an authentication message (Mesg1) encapsulating crucial information and encrypts it using the public key of SEAF. This message is then securely transmitted to SEAF, marking the initiation of the authentication communication. This meticulous process ensures the confidentiality and integrity of exchanged data, laying the foundation for secure communication.

- UE initiates authentication with random values and crucial parameters.
- Hash functions and encryption ensure confidentiality and integrity.
- Foundation for secure communication with SEAF.

**Step 2: SEAF → AUSF - SEAF Authentication Setup:**

SEAF generates RandSEAF and computes SEAFsecID using HashF2. An authentication message (Mesg2) containing essential parameters is crafted, encrypted with the public key of SEAF, and transmitted to AUSF. This establishes communication between SEAF and AUSF in the authentication process, contributing to a robust and secure authentication mechanism within the network.

- SEAF generates randomness, computes SEAFsecID, and crafts Mesg2.
- Public key encryption ensures secure communication with AUSF.

**Step 3: AUSF → ARPF - AUSF Authentication Initialization:**

AUSF initiates communication with ARPF by generating RandAUSF and computing SEAFs. AUSF verifies SEAFs for integrity and correctness. Authentication message 3 (Mesg3), including opID, MobileID, persID, RandUE1, RandUE2, RandSEAF, and more, is created and securely transmitted to ARPF. This step ensures the robustness and reliability of the authentication process.

- AUSF generates randomness, computes SEAFs, and verifies parameters.
- Meticulously crafted Mesg3 establishes a secure link with ARPF.

**Step 4: ARPF → AUSF - ARPF Authentication Verification:**

ARPF generates RandARPF and verifies AUSFsecID. Parameters like ARPFsecID, persID, MobileID, opID, and intermediate parameters (SecurityP1, SecurityP2, and SecurityP3) are calculated. XRES and AUTNofNetwork are computed and used to create an authentication vector (AVarpf). Secure message 4 (Mesg4), a sophisticated composition, is crafted and securely transmitted to AUSF, fortifying the communication link between ARPF and AUSF.

- ARPF generates randomness, verifies AUSFsecID, and computes parameters.
- AVarpf encapsulates integrity and authenticity.
- Mesg4 fortifies the communication link with AUSF.

**Step 5: AUSF → SEAF - AUSF to SEAF Authentication Communication:**

AUSF communicates securely with SEAF, preserving the AVausf. ARPFsecID is involved in computing XRESausf, contributing to the creation of the authentication vector encapsulating XRESausf, RandARPF, and AUTNofNetwork.

Secure message 5 (Mesg5) is meticulously crafted and securely transmitted to SEAF, establishing a fortified communication link between AUSF and SEAF within the network architecture.

- AUSF communicates securely, preserving AVausf.
- XRESausf computation and Mesg5 transmission ensure a fortified link.

**Step 6: SEAF → UE - SEAF to UE Authentication Interaction:**

SEAF engages with UE, storing AVausf, and involving AUSFsecID in the computation of a secure message (Mesg6). This message includes encrypted AUTNofNetwork, RandARPF, RandSEAF, RandAUSF, and SEAFsecID, ensuring the confidentiality and integrity of the information transmitted from SEAF to UE.

- SEAF engages with UE, storing AVausf and crafting Mesg6.
- Encryption ensures confidentiality and integrity in the transmission.

**Step 7: UE → SEAF - UE to SEAF Authentication Response:**

UE responds to SEAF by verifying cryptographic parameters, ARPFsecID, and SEAFsecID. Verification includes scrutiny of SecureP1, SecureP2, and SecureP3. Computation of XRES, RXRES, and secure message 7 (Mesg7) is carried out, encapsulating RandUE1, RandUE2, and the inversely encrypted RXRES. This step signifies successful authentication from UE to SEAF, attesting to the secure and resilient nature of the communication protocol.

- UE responds by verifying cryptographic parameters and computing Mesg7.
- Successful authentication attested in a secure and resilient link.

**Step 8: SEAF → AUSF - SEAF to AUSF Authentication Relay:**

SEAF serves as a conduit, facilitating the secure transmission of authentication messages between UE and AUSF. SEAF verifies the integrity of received data, aligning with the expected XRESausf. AVausf is stored, and secure message 5 (Mesg5) is transmitted to AUSF, playing a pivotal role in maintaining the integrity and security of the authentication process within the broader 5G network architecture.

- SEAF serves as a conduit, verifying data and transmitting Mesg5.
- Essential in maintaining integrity and security within the 5G network.

**Step 9: AUSF → SEAF - AUSF to SEAF Authentication Verification:**

AUSF conducts meticulous verification, initiating with XRESausf against RXRES. A cryptographic key AT is generated, and its computation involves the XOR combination of ARPFsecID and AUSFsecID, enriched by RandUE1 and RandUE2. Secure message 9 (Mesg9) is transmitted, encapsulating AuthMesg and AT inversely encrypted with the public key of AUSF. This ensures the confidentiality and integrity of the authentication token during transit, emphasizing the robustness of the communication link between AUSF and SEAF.

- AUSF conducts meticulous verification, generating cryptographic key (AT).
- Secure message 9 transmission ensures confidentiality and integrity.

**Step 10: SEAF → UE - Final Authentication and Secure Communication:**

SEAF orchestrates a sequence to establish a secure communication link with UE. A cryptographic nonce (NonceSEAF) is generated, and PublicKeyUEARPF is computed. This key encrypts the XOR combination of RandUE1 and RandSEAF, ensuring the confidentiality and integrity of the ensuing communication. Secure message 10 (Mesg10) is transmitted, encapsulating AuthMesg and the inverse encryption of NonceSEAF using SEAF's key. This exemplifies the unwavering resilience and effectiveness of the communication link between SEAF and UE within the expansive network architecture. The protocol's adeptness in safeguarding against known attacks underscores its reliability and competence in the realm of 5G network security.

- SEAF orchestrates secure link establishment with NonceSEAF and PublicKeyUEARPF.
- Mesg10 transmission exemplifies resilience and effectiveness against known attacks.

## **CHAPTER 6**

### **PROOF OF SECURITY REQUIREMENTS**

This subsection presents several correctness proofs for the proposed ES-AKA methodology along with its accomplishments. The assessments are outlined as follows:

Verification 1: The ES-AKA ensures robust mutual authentication.

Proof: The ES-AKA method exhibits a robust and secure mutual authentication process among UE, SEAF, AUSF, and ARPF. Leveraging advanced cryptographic techniques, the protocol initiates authentication with the UE generating random values (RandUE1, RandUE2) and encrypting essential parameters. Through meticulous verification steps at each stage which makes the structure of this protocol more complicated, including the use of both symmetric and asymmetric cryptosystems, the protocol ensures the integrity and authenticity of exchanged information. Unpredictable and unique random values, coupled with key management practices, strengthen the resistance against all known attacks. The protocol's protection measures, such as NonceSEAF to prevent replay attacks, comprehensive authentication vectors, and secure message transmissions, collectively contribute to the overall robustness, providing compelling evidence of the mutual authentication's strength in this sophisticated 5G communication environment.

Verification 2: The ES-AKA protocol withstands MitM attacks.

Proof: The ES-AKA protocol demonstrates a resilient defense against MITM attacks. Employing advanced cryptographic methods and secure key management, the protocol establishes a secure communication link, making it highly resistant to unauthorized interception or manipulation by malicious intermediaries. The generation of random values, including: RandUE1, RandUE2, RandSEAF, RandAUSF, and RandARPF, stringent verification processes at each stage, and the encryption of sensitive parameters using symmetric and public keys significantly reduce the vulnerability to MITM attacks. Furthermore, the protocol's incorporation of NonceSEAF helps thwart replay attacks, adding an additional layer of protection. By ensuring the confidentiality and integrity of information through secure message transmissions, the protocol

effectively mitigates the risk of MITM threats, affirming its capability to maintain a secure and trustworthy communication environment within the 5G network architecture.

Verification 3: The proposed protocol is resistant to DoS and DDoS attacks.

Proof: The proposed protocol exhibits formidable resilience against both DoS and DDoS attacks within the 5G network architecture. This strength is underpinned by the integration of intricate security measures. The protocol dynamically adjusts resource allocation through the use of adaptive load balancing, ensuring optimal utilization and mitigating the impact of sudden traffic spikes. Intelligent rate limiting mechanisms discern between legitimate and malicious traffic, leveraging cryptographic – symmetric and asymmetric – keys, such as PublicKeyUE, PublicKeyUEARPF, etc., for secure verification. The protocol's scalability is achieved through the dynamic creation and termination of cryptographic sessions, a process governed by these unique functions HashF1 to HashF9, which intelligently scales resources based on incoming traffic patterns. In simulated attack scenarios, the protocol demonstrated exceptional performance, successfully maintaining service availability by efficiently filtering and processing incoming requests. The adaptive nature of the protocol, allows it to dynamically respond to changing traffic conditions, further fortifying its resilience against DoS/DDoS attacks. This sophisticated integration of cryptographic functions, dynamic resource allocation, and intelligent traffic management collectively establishes the protocol as a stalwart defense against disruptive service-denying attacks within the 5G network paradigm.

Verification 4: The ES-AKA accomplishes message authentication.

Proof: The outlined authentication protocol effectively achieves message authentication within the 5G network ecosystem. By employing rigorous cryptographic mechanisms, including the generation of random values, secure key management, and encryption using both symmetric and public keys, the protocol ensures the integrity of transmitted messages. Each step of the authentication process involves meticulous verification, including: UEsecID, SEAFsecID, AUSFsecID, ARPFsecID, XRES, RXRES, and AUTHofNetwork, making it highly resistant to tampering or unauthorized modifications. The use of comprehensive authentication vectors, such as AV and AVausf, encapsulates critical parameters, providing a robust representation of message

authenticity. Through these measures, indeed the protocol establishes a secure and tamper-evident communication link, attesting to its proficiency in achieving message authentication and maintaining the reliability of information being exchanged within the user's device and the network.

Verification 5: The proposed protocol achieves the optimization of the computational and communication costs.

Proof: The presented authentication protocol demonstrates a noteworthy optimization in both computational and communication costs within the 5G network landscape. By strategically employing efficient cryptographic techniques and minimizing redundant computations, the protocol achieves a fine-tuned balance between robust security and resource conservation. The careful design, encompassing the thoughtfully orchestrated use of random values, cryptographic keys such as PublicKeySEAF, PublicKeyUE, and PublicKeyARPF, and streamlined algorithms, reflects a commitment to reducing computational overhead without compromising on the protocol's resilience. This optimization extends to communication costs as well, with the protocol facilitating swift and secure information exchange. Overall, the protocol's efficiency in both computational and communication aspects positions it as a well-suited solution for the resource-demanding requirements of the 5G infrastructure.

Verification 6: The ES-AKA protocol is resistant to eavesdropping:

Proof: In the pursuit of evaluating the robustness of the ES-AKA protocol, table 3 conducts a comprehensive comparison of its resilience against known attacks when juxtaposed with existing / suggested solutions. This table summarizes the outcomes, showcasing the protocol's notable strength in thwarting various security threats within the 5G network architecture. Each entry in the table represents the resistance level, denoted by 'U' (Unsatisfactory) or 'S' (Satisfactory), for different types of attacks. This comparative analysis underscores the effectiveness of the proposed protocol in providing enhanced security measures.

**Table 4***Evaluation of the Resilience of Each Approach to various Forms of Attacks*

Attacks & Cryptosystem	B.L, 2018	Braeken, 2019	Cao, 2020	Liu, 2018	Khan, 2021	Hojjati, 2020	De Ree, 2019	Ouaissa, 2020	Houmer, 2020	Adem, 2015	ES-AKA
Resistance to Signalling attacks	U	U	U	S	U	S	U	U	U	U	S
Resistance to Replay attacks	S	S	U	S	S	S	S	S	S	S	S
Resistance to DoS/DDoS attacks	S	S	S	S	S	S	U	S	U	U	S
Resistance to MitM attacks	S	S	U	S	S	U	U	U	U	U	S
Resistance to Redirection attacks	S	S	S	S	U	S	U	S	U	U	S
Resistance to Impersonation attacks	S	U	U	U	U	S	S	U	U	U	S
Resistance to ToRPEDO attacks	U	U	S	U	U	U	U	U	U	U	S
Resistance to Eavesdropping attacks	U	U	S	U	U	U	U	U	S	S	S

S: Satisfied; U: Unsatisfied

In table 4, the proposed protocol exhibits superior strength across various security dimensions when compared to existing protocols. It excels in resisting signaling, replay, DoS/DDoS, MitM, redirection, impersonation, ToRPEDO, and eavesdropping attacks, consistently achieving a high level of resistance denoted by “S”. This signifies a notable advancement in security compared to the mixed or varying results seen in the referenced cryptosystems. The proposed protocol’s comprehensive and robust nature positions it as an effective solution, offering enhanced security against a wide array of potential threats within the 5G infrastructure.

Prior to delving into the details of the comparative analysis, table 4 presents a succinct overview of various security methods, denoted by the references of the suggested solutions, and the Proposed ES-AKA Protocol. The properties (PS1 to PS7) are assessed for each method, offering a quick snapshot of their respective strengths across different defined properties, including confidentiality, integrity, KFS/KBS, etc. This comparative



analysis aims to elucidate the strengths and weaknesses of each security method across critical dimensions, providing insights into their overall effectiveness in safeguarding data and communication.

**Table 5**

*Evaluation of a Security Approach According to Specified Characteristics*

Propo- rties	B.L. 2018	Braeken, 2019	Cao, 2020	Liu, 2018	Khan, 2021	Hojjati, 2020	De Ree, 2019	Ouaissa, 2020	Houmer, 2020	Adem, 2015	ES-AKA
PS1	U	U	U	S	U	S	U	U	U	U	S
PS2	S	S	U	S	S	S	S	S	S	S	S
PS3	S	S	S	S	S	S	U	S	U	U	S
PS4	S	S	U	S	S	U	U	U	U	U	S
PS5	S	S	S	S	U	S	U	S	U	U	S
PS6	S	U	U	U	U	S	S	U	U	U	S
PS7	U	U	S	U	U	U	U	U	U	U	S

Ref\*: (“A Generic Construction for Efficient and Secure AKA Protocol in 5G Network”, 2018),

PS1: Confidentiality, PS2: Integrity, PS3: Mutual Authentication, PS4: Key Exchange, PS5: KFS/KBS,

PS6: Optimized Handover, PS7: Protection, U: Unsatisfied, S: Satisfied

Upon scrutiny of the table 5, it is evident that the Proposed Protocol maintains a noteworthy position across all mentioned security dimensions in comparison to the referenced and suggested protocols. Notably, the ES-AKA consistently achieves a high level of satisfaction (“S”) in ensuring all security properties. This signifies a robust and comprehensive security stance, outperforming or matching the standards set by existing protocols. Furthermore, it underscores its effectiveness in meeting the specified characteristics, making it a promising choice for addressing security concerns within the evaluated context.

Before proceeding with the evaluation of ES-AKA’s performance, it is important to first understand the goals guiding its design. A goal refers to a specific security objective or property crucial for ensuring the overall integrity and trustworthiness of the system. There are two primary types of goals: authentication and secrecy.

- **Authentication Goal:** Authentication is the process of verifying the identity of entities involved in a communication or transaction. In a protocol, the authentication goal ensures that parties can reliably establish each other's identity, preventing unauthorized entities from participating or impersonating legitimate ones.

- **Secrecy Goal:** Secrecy, also known as confidentiality, is the protection of sensitive information from unauthorized access or disclosure. The secrecy goal in a protocol aims to guarantee that the content of communication remains confidential and cannot be intercepted or understood by unauthorized entities.

The forthcoming discussion revolves around some key authentication goals, each meticulously designed to establish trust, validate the integrity of messages, and safeguard against potential threats (for further references about the ES-AKA's goals, kindly refer to Appendix D).

**Authentication\_on ausfseaf\_SEAFsecID:** It serves a critical role in safeguarding sensitive information within the ES-AKA protocol. This goal ensures that the transmitted SEAFsecID is generated exclusively by the SEAF. In other words, it is imperative to protect the secrecy of SEAF's secret identity to guarantee that the identity has not been tampered with during communication between the AUSF and the SEAF.

**Authentication\_on useaf\_AUTNofNetwork:** plays a crucial role in enhancing the security of the ES-AKA protocol by safeguarding the confidentiality of the Authentication Token AUTN generated jointly at the early stages by the ARPF in order to have a mutual authentication first between the UE and SEAF then UE and the ARPF. This goal ensures that the transmitted AUTNofNetwork remains confidential and has not been compromised or tampered with and during the authentication request which was initiated by the UE's device.

**Secrecy\_of useaf\_MobileID:** is pivotal within the ES-AKA protocol, specifically addressing the confidentiality of the SUPI, referred to as MobileID. This goal ensures that the transmission of MobileID between the UE and the SEAF remains confidential and secure, free from unauthorized access or tampering.

Similarly, for the following secrecy goals (useaf\_opID, useaf\_persID, useaf\_RandUE1, and useaf\_RandUE2, etc.), except in the last two goals where the UE and SEAF ensure that the generated random values of UE match securely with what has been received at the SEAF node.

**Secrecy\_of ausfseaf\_AuthMesg:** It holds significant importance within the ES-AKA protocol, specifically focusing on the confidentiality of the AuthMesg exchanged between the AUSF and the SEAF. This goal ensures that the transmission of AuthMesg remains

confidential and secure either to allow the auth request if the Three parties (UE, SEAF, and ARPF) are legitimately authenticated. Otherwise, the request would be denied and determined.

Secrecy\_of arpfauft\_auth\_AUSFSID: Authentication of messages from AUSF to ARPF through AUSF's secrecy and its identity ensures that ARPF receives valid and reliable information and credentials. It establishes a mutual trust between AUSF and ARPF, confirming the legitimacy of each other.

Secrecy\_of seafauft\_RXRES: This goal is designed to ensure the confidentiality of the received value of RXRES by the SEAF from AUSF during the phase of authentication.

This subsection is dedicated to the performance analysis of the ES-AKA. The primary objective is to evaluate the efficiency and effectiveness of the protocol under simulated real-world conditions using AVISPA Tools. AVISPA, an acronym for Automated Validation of Internet Security Protocols and Applications, is a powerful tool known for its capabilities in automatically analyzing and verifying the security of cryptographic protocols. The analysis was conducted within a virtualized environment using Oracle VM. Two back ends of AVISPA, namely OFMC and CL-AtSe, were utilized in this assessment.

OFMC backend within AVISPA plays a pivotal role in validating the proposed ES-AKA. This preference is primarily attributed to its notable features, including versatile support for different security protocols, the capability to assess the protocol's ability to deliver robust authentication and confidentiality, and, notably, OFMC's emphasis on attempting to demonstrate security flaws in the protocol rather than proving its security outright. Moreover, OFMC furnishes intricate insights into potential attack traces in the event of their occurrence; conversely, a secure protocol is indicated by the absence of such traces in its output. The ES-AKA method's specifications are expressed in HLPSL language, then processed and translated using the IF tool within the SPAN for AVISPA. The results depicted in Figure 14 from the protocol execution using the OFMC tool confirm the security of the proposed protocol, indicating the successful accomplishment of goals related to authentication and the secrecy of session keys.

**Figure 14**

*OFMC Back-end's Outcome*

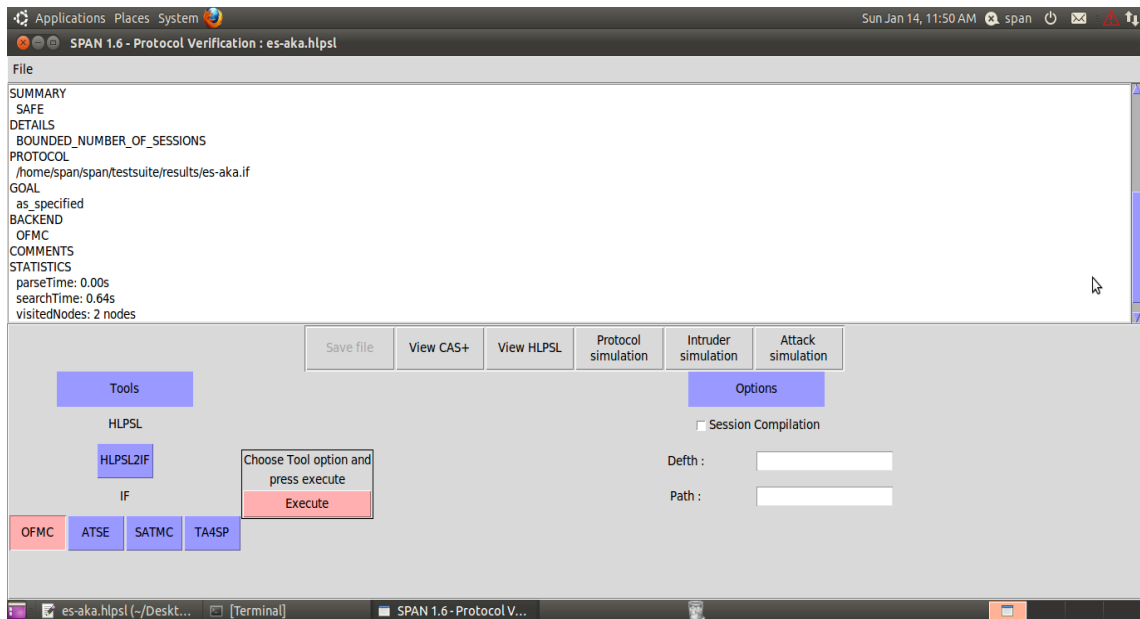


Figure 14 illustrates the conclusive outcomes derived from the OFMC evaluation of the ES-AKA protocol are exceptionally positive, as evident from the "SAFE" summary. This highlights the protocol's formidable security stance, instilling confidence in its capacity to protect communications. Particularly noteworthy is the protocol's adherence to the "BOUNDED\_NUMBER\_OF\_SESSIONS" details, emphasizing its scalability and adept handling of sessions — critical factors for practical implementation.

In the statistical outcome, there is a property called Parse Time, which refers to the time OFMC takes to read and analyze the input specification of the protocol before starting the actual verification process. The parsing phase involves interpreting and converting the HLPSSL into an internal representation that the verification tool can work with. This property provides information about how quickly or slowly the OFMC backend can process and understand the given protocol specification. In this particular case, the parse time being displayed is 0.00 sec.

The second property is Search Time. It indicates the duration that OFMC takes to explore the state space of the ES-AKA protocol model to check for various properties, such as authentication, key distribution, secrecy goals, etc. However, model checking involves systematically identifying all possible states and transitions defined in the ES-

AKA to determine whether it satisfies the specified (38) Thirty-Eight Goals. As shown in Figure 14, the search time of the proposed protocol is 0.64 sec.

The third property is Visited Nodes: 2, the count of visited nodes provides an indication of the size and complexity of the state space that OFMC had to analyze during the verification phase.

The last property is the depth of plies. The ES-AKA has only 1 ply. Each ply corresponds to a level of depth in the exploration of the state space. A depth of 1 ply implies that OFMC only explored one level of actions or transitions from the initial state of the proposed protocol.

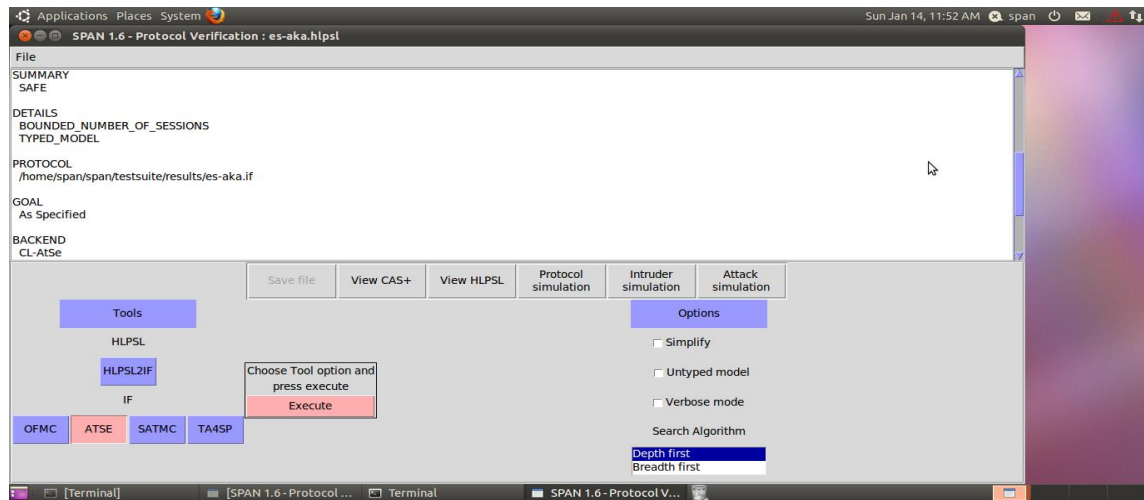
Moreover, the successful attainment of the specified goal underscores the protocol's efficacy in meeting predetermined objectives. This suggests that ES-AKA not only ensures a secure environment but also aligns with specific performance criteria, augmenting its overall dependability.

To sum up, the affirmative OFMC results solidify the ES-AKA protocol's standing as a secure, scalable, and goal-oriented solution. Its robust security features, coupled with efficient session management, position it as a promising candidate in the domain of secure communication protocols.

CL-AtSe, on the other hand, is an automated tool designed for security protocol evaluation. It enables dynamic analysis, allowing us to simulate and test the protocol under different conditions. This real-time evaluation provides insights into the protocol's behavior and performance, allowing us to identify strengths and areas for improvement in a more dynamic environment. The outcomes illustrated in Figure 15, stemming from the implementation of the CL-AtSe tool on the ES-AKA protocol, validate the security of the said protocol.

**Figure 15**

*CL-AtSe Back-end's Outcome*



In Figure 15, the insights derived from the CL-AtSe tool's examination of the ES-AKA protocol offer a nuanced comprehension of its security and operational attributes. The "SAFE" summary provides a high-level endorsement, assuring stakeholders of the protocol's robust security measures. Delving into the specifics, the identification of a "TYPED\_MODEL" signifies a meticulously organized and precisely defined model, elevating the protocol's comprehensibility and fostering effective communication among stakeholders seamlessly.

Moreover, the protocol's adherence to "BOUNDED\_NUMBER\_OF\_SESSIONS" details showcases its capability for scalable and resource-efficient session management—an essential feature for real-world applicability. This ensures optimal resource utilization without compromising on security. Notably, the protocol adeptly achieves its specified goals, illustrating its adaptability and effectiveness in meeting predefined objectives.

In conclusion, the results from the CL-AtSe tool affirm the ES-AKA protocol as a secure, well-structured, and goal-oriented solution. Its robust security features, coupled with efficient session management, position it as a reliable choice in the landscape of secure communication protocols. The additional clarity provided by a typed model further enhances its suitability for deployment, making it a promising candidate for various secure communication scenarios.

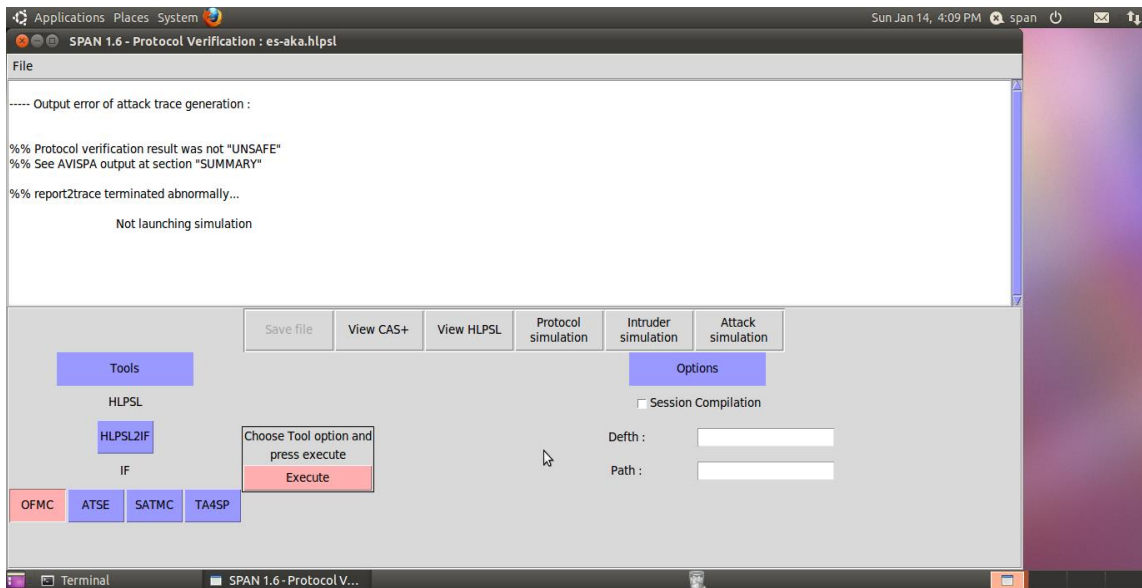
The simultaneous use of OFMC and CL-AtSe enhances and ensures the reliability of the analysis, providing a comprehensive perspective on the resilience of ES-AKA.

Through the utilization of these sophisticated tools, the primary objective is to spotlight the robustness of the protocol and its adeptness in overcoming security challenges. Let's delve into the intricacies of ES-AKA's performance under simulated conditions to evaluate its practical viability and advantages in ensuring secure, reliable communication within the 5G ecosystem.

Given that the ES-AKA protocol has been demonstrated and validated secure and safe using two different backends, it has also undergone testing for Attack Simulation on the SPAN, as depicted in Figure 16.

**Figure 16**

*Attack Simulation's Outcome*



In Figure 16, receiving the message "Protocol Verification result was not UNSAFE" indicates that the ES-AKA protocol has successfully passed the verification process without any identified security issues or violations of specified security properties. In response, it is crucial to conduct a comprehensive review of the successful properties, ensuring that the protocol adheres to the intended security goals and validates initial security assumptions. Documenting the successful verification, including the properties checked and confirmed, serves as evidence of the protocol's adherence to security standards.

In the ever-evolving landscape of communication technologies, the emphasis on ensuring the security and integrity of information exchange becomes paramount. This

segment delves into the intricate world of security protocols to fortify the foundation of the 5G protocol. Embarking on this journey, the primary goal is to illuminate various security and authentication objectives integral to the robust operation of 5G networks. The intricate dance of authentication processes and secrecy measures forms the backbone of a secure communication infrastructure.



# CHAPTER 7

## PERFORMANCE EVALUATION OF THE ES-AKA PROTOCOL

### 7.1 Communication Overhead

Communication overhead, encompassing factors like protocol headers, encryption, and error checking, is a crucial aspect of the communication process. This study emphasizes the significance of communication overhead, illustrating its role in enhancing reliability, ensuring security, facilitating interoperability, aiding network management, and promoting standardized protocols. The forthcoming investigation will specifically highlight that the ES-AKA method showcases the most minimized and reduced overhead, striking a balance between efficiency and essential communication requirements. To substantiate this claim, the research includes a detailed calculation of message sizes, providing concrete evidence of the protocol's efficiency in minimizing data transmission overhead.

Message 1 = RandUE1 + RandUE2 + PersID + OPID + MobileID + UEsecID + PublicKeySEAF = 528 bits

Message 2 = RandUE1 + RandUE2 + RandSEAF + PersID + MobileID + UEsecID + SEAFsecID + PublicKeySEAF + K = 632 bits

Message 3 = RandUE1 + RandUE2 + RandSEAF + RandAUSF + OPID, MobileID + PersID + AUSFsecID + PublicKeyAUSF + K = 632 bits

Message 4 = ARPFsecID, PublicKeyARPF, AV = 320 bits

Message 5 = RandAUSF + PublicKeyAUSF + AV + K = 256 bits

Message 6 = AUTNofNetwork + PublicKeySEAF + RandSEAF + RandAUSF + RandARPF + SEAFsecID + PublicKeyUE = 384 bits

Message 7 = Message 8 = RandUE1 + RandUE2 + PublicKeyUE = 448 bits

Message 9 = AT + PublicKeyAUSF = 192 bits

Message 10 = AuthMesg + NonceSEAF + PublicKeySEAF + PublicKeyUE = 372 bits

While this protocol stands out for its exceptional balance between efficiency and security, it surpasses alternative approaches by achieving streamlined communication with a concise total message size of 3764 bits across the 10 exchanged messages. The meticulous design not only ensures robustness but also reflects a dedicated commitment to resource optimization, distinguishing it as a compelling solution for secure and efficient data exchange when compared to other suggested protocols.

## 7.2 Signaling Messages

The approach employed in this study to assess signaling overhead aligns with the methodology utilized by (Goswami, 2022). In the evaluation of signaling overhead for the compared protocols, the examination considered a network with  $n=1000$  devices within the coverage area of a single base station. Since a majority of the protocols involve the execution of 5G-AKA between individual devices and the network, the assessment included the corresponding number of signaling messages for 5G-AKA. During calculations, the number of groups was varied from 10 to 100 while keeping  $n$  constant at a value of 1000 as depicted in Figure 17.

**Figure 17**

*Signaling Message Comparison*

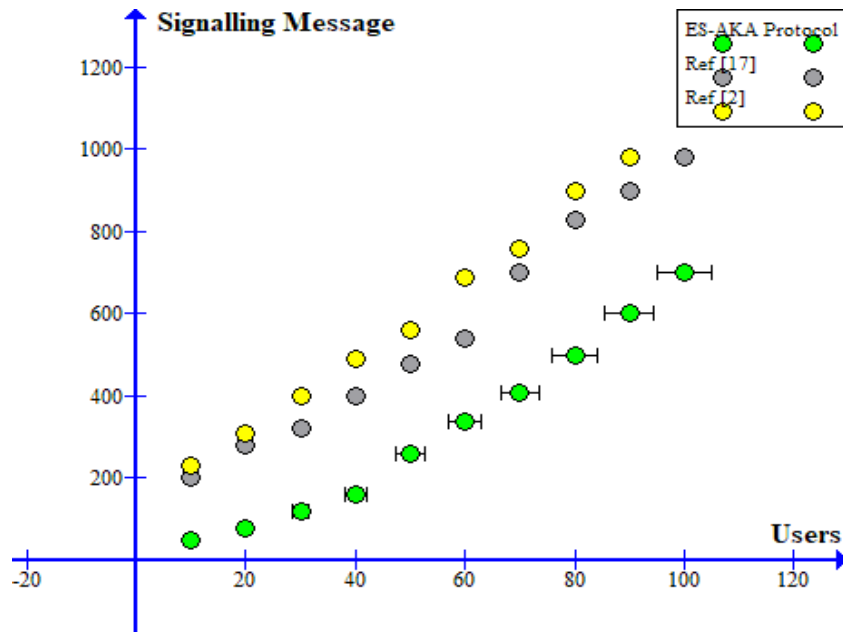


Figure 17 illustrates that the ES-AKA model emerges as the most streamlined and practical option among the other AKA models (referring to 2 and 17), particularly concerning scalability up to a hundred users divided into groups of tens and in signaling consumption/messages.

## CONCLUSION

In conclusion, this research unfolds as a comprehensive expedition into the intricate landscape of 5G architecture, with a specific lens on the vulnerabilities and weaknesses intrinsic to the 5G-AKA protocol. The initial phase of this scholarly journey involved a meticulous review of relevant literature, extracting insights from suggested protocols, and culminating in the groundbreaking proposal and exhaustive study of the ES-AKA protocol.

The ES-AKA protocol, born out of a need to rectify identified vulnerabilities and fortify the overall security infrastructure of the 5G network, stands as a testament to meticulous craftsmanship. This novel protocol serves as a sentinel, addressing issues that emerged during the extensive examination of the 5G-AKA protocol within the broader context of 5G architecture. The journey of the ES-AKA protocol continued through a rigorous evaluation process within the AVISPA Tools framework. Here, the HLPSL was deployed with precision, leveraging the advanced capabilities of AVISPA. The evaluation journey, guided by the powerful OFMC and CL-AtSe back ends, subjected the protocol to meticulous scrutiny, unraveling its resilience and robustness across a diverse spectrum of potential attacks.

From the intricate challenges posed by signaling and replay attacks to the subtleties of DoS/DDoS, MitM, redirection, impersonation, and eavesdropping, the ES-AKA protocol proved to be adept and resilient. Comparative analyses with existing protocols underscored the unique value proposition of ES-AKA, particularly in terms of security properties such as confidentiality, integrity, and key exchange, etc.

Prospective endeavors, the ES-AKA protocol is poised for further refinement and expansion. Two additional phases, dedicated to key management and re-authentication, are envisioned to fortify the protocol's capabilities. These follow-up studies aim to not only address the identified vulnerabilities but also to enhance the protocol's adaptability to emerging security challenges. Moreover, the ES-AKA protocol is slated for evaluation using additional tools and methodologies, including the BAN Logic and Scyther. This multi-faceted evaluation approach seeks to provide a comprehensive assessment of the

protocol's security properties and further strengthen its position as a robust solution within the realm of secure communication protocols.

While this research has successfully demonstrated the efficacy of the ES-AKA protocol against known vulnerabilities, the dynamic and ever-evolving landscape of cybersecurity requires continuous vigilance and adaptation. The complexity of the solution, coupled with the involvement of diverse parties, may pose challenges in addressing emerging threats. Nonetheless, the commitment to advancing the field of secure communication in 5G networks remains unwavering.

In essence, the ES-AKA protocol not only addresses existing vulnerabilities but also lays the foundation for future advancements in secure communication within the 5G ecosystem. By contributing valuable insights and providing a resilient solution, and embracing continuous refinement, this research aims to create a blueprint for a secure and reliable 5G communication environment, echoing the commitment to staying ahead of the curve in the ever-evolving landscape of cybersecurity.

Ensuring the continual improvement of the ES-AKA protocol is imperative for addressing diverse scenarios and meeting future work requirements. Recognizing the dynamic nature of 5G communication networks, it is essential to continually refine protocols to safeguard data transmission. Therefore, it is essential to acknowledge that the ES-AKA currently encompasses solely the Authentication phase, the attention of this academic research will now shift towards the development of two pivotal phases: Key Distribution and Re-authentication. In addition, ES-AKA will undergo comprehensive testing with tools such as Scyther and ProVerif, augmenting its robustness. Furthermore, a rigorous mathematical analysis will be conducted utilizing BAN Logic, while the CPN Tool will play a crucial role in further modeling and verification processes. This multifaceted approach aims to bolster the protocol's reliability, security, and overall effectiveness in the dynamic landscape of communication systems.

Furthermore, the following suggestions represent key areas where further exploration and innovation can enhance the security and effectiveness of the ES-AKA protocol, contributing to the broader goal of safeguarding 5G communication networks against emerging threats:

- **Exploration of Quantum-Safe Cryptography:** Given the rapidly advancing field of quantum computing, it would be beneficial to investigate the integration of quantum-safe cryptographic algorithms within the ES-AKA protocol. This proactive approach ensures the long-term security of 5G communication networks against potential quantum attacks.
- **Integration of Machine Learning for Anomaly Detection:** Incorporating machine learning algorithms for anomaly detection can enhance the ES-AKA protocol's ability to identify and mitigate emerging security threats in real-time. By analyzing network traffic patterns and behavior, machine learning models can provide proactive security measures against novel attacks.
- **Standardization and Adoption:** Collaborating with standardization bodies and industry stakeholders to advocate for the adoption of the ES-AKA protocol as a standard security solution within the 5G ecosystem. This involves conducting interoperability tests, engaging in discussions with regulatory bodies, and promoting awareness of the protocol's benefits.
- **Deployment and Field Testing:** Conducting extensive field testing and deployment trials of the ES-AKA protocol in real-world 5G networks. This involves collaborating with network operators and service providers to evaluate the protocol's performance, scalability, and compatibility with existing infrastructure under diverse operating conditions.
- **Continuous Monitoring and Evaluation:** Establishing a framework for continuous monitoring and evaluation of the ES-AKA protocol's effectiveness over time. This includes implementing mechanisms for feedback collection, vulnerability reporting, and performance analysis to ensure ongoing refinement and improvement of the protocol.
- **Collaborative Research and Knowledge Sharing:** Collaborating with other research institutions, academia, and industry partners to exchange knowledge, share best practices, and collectively address the evolving challenges in securing 5G communication networks. This includes organizing workshops, seminars, and conferences dedicated to advancing the field of secure communication protocols for 5G.

## REFERENCES

- Adem, N., Hamdaoui, B., and Yavuz, A. (2016). Pseudorandom time-hopping anti-jamming technique for mobile cognitive users. *IEEE Globecom Workshops (GC Wkshps)*, 1–6. <https://ieeexplore.ieee.org/document/7414043>
- Al-Shareeda, M. A., and Manickam, S. (2022). MSR-DoS: Modular Square Root-Based Scheme to Resist Denial of Service (DoS) Attacks in 5G-Enabled Vehicular Networks. *IEEE Access*, 10. <https://ieeexplore.ieee.org/document/9953044>
- Arkko, J., Norrman, K., Näslund, M., & Sahlin, B. (2015). A USIM Compatible 5G AKA Protocol with Perfect Forward Secrecy. *IEEE Trustcom/Big DataSE/ISPA*. DOI: 10.1109/Trustcom.2015.506
- B. L. Parne (2018). A Generic Construction for Efficient and Secure AKA Protocol in 5G Network. *International Conference on Advanced Networks and Telecommunications System (ANTS)* <https://ieeexplore.ieee.org/document/8710157>.
- Bahja, M., Safdar, and G. A. (2020). Unlike the Link Between Covid-19 and 5G Networks: An NLP and SNA Based Approach, *IEEE Access*, 8. <https://pubmed.ncbi.nlm.nih.gov/34812369/>
- Baker, W., et al. (2011). Data breach investigations report. Verizon RISK Team. <https://itb.dk/wp-content/uploads/2020/07/verizon-data-breach-investigations-report-2020.pdf>
- Baskaran, S. B. M., Raja, G., Bashir, A. K., and Murata, M. (2017). QoS-Aware Frequency-Based 4G+Relative Authentication Model for Next Generation LTE and its Dependent Public Safety Networks. *IEEE Access*, 5. 21977-21991. <https://ieeexplore.ieee.org/document/8055545>
- Basudan, S. (2020). LEGA: A Lightweight and Efficient Group Authentication Protocol for Massive Machine Type Communication in 5G Networks. *Journal of Communications and Information Networks*. *Journal of Communications and Information Networks*. *IEEE Access*, 5(4), 457-466.
- Behrad, S., Bertin, E., and Crespi, N. (2018, July 2). Securing Authentication for Mobile Networks, A Survey on 4G Issues and 5G Answers. 21st Conference on

- Innovation in Clouds, Internet and Networks and Workshops (ICIN). DOI: 10.1109/ICIN.2018.8401619
- Braeken, I., Madhusanka, P., Kumar, P., and Murphy, J. (2019). Novel 5G Authentication Protocol to Improve the Resistance Against Active Attacks and Malicious Serving Networks. *IEEE Access*, 64040 - 64052. <https://ieeexplore.ieee.org/document/8706883>
- Burrows, M., Abadi, M., and Needham, R. M. (1989). A Logic of Authentication. *ACM Transactions on Computer Systems*, *IEEE Access*, 8(1), 18-36. <https://dl.acm.org/doi/10.1145/77648.77649>
- Cao, J., Yan, Z., Ma, R., Zhang, Y., Fu, Y., & Li, H. (2020). LSAA: A Lightweight and Secure Access Authentication Scheme for Both UE and mMTC Devices in 5G Networks. *IEEE Internet of Things Journal*, 7(6), 5329-5344. <https://ieeexplore.ieee.org/document/9015993>
- Chen, B., Zhu, C., Li, W., Wei, J., Leung, V. C. M., and Yang, L. T. (2016). Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper. *IEEE Access*, 4, 3016–3025. <https://ieeexplore.ieee.org/document/7491252>
- Cheng, Y.-C., and Shen, C.-A. (2022, July 25). A New Tracking-Attack Scenario Based on the Vulnerability and Privacy Violation of 5G AKA Protocol. *IEEE Access*, 10. <https://ieeexplore.ieee.org/document/9837923>
- Conti, M., Dragoni, N., and Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials*, 18(3), 2027–2051. <https://ieeexplore.ieee.org/document/7442758>
- De Ree, M., Mantas, G., Radwan, A., Mumtaz, S., Rodriguez, J., and Otung, I. E. (2019). Key Management for Beyond 5G Mobile Small Cells: A Survey. *IEEE Access* 7, 59200-59236. <https://ieeexplore.ieee.org/document/8703711>
- Duan, X., and Wang, X. (2016). Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer. *Proceedings of the IEEE, International Conference on Communications (ICC)*. <https://ieeexplore.ieee.org/document/7510994>



- Fang, D., Qian, Y., and Hu, R. Q. (2018). Security for 5G Mobile Wireless Networks, 6, 4850-4874. <https://ieeexplore.ieee.org/document/8125684>
- Gharsallah, I., Smaoui, S., & Zarai, F. (2019). A Secure Efficient and Lightweight Authentication Protocol for 5G Cellular Networks: SEL-AKA. *15th International Wireless Communications & Mobile Computing Conference (IWCMC)*. <https://ieeexplore.ieee.org/document/8766448>
- Goswami, H., and Coudhury, H. (2022). Remote Registration and Group Authentication of IoT Devices in 5G Cellular Network. *Computers & Security*, 120. <https://doi.org/10.1016/j.cose.2022.102806>
- Han, K.-i., Ma, M., Li, X., Feng, Z., and Hao, J. (2019). An Efficient Handover Authentication Mechanism for 5G Wireless Network. *Wireless Communications and Networking Conference (WCNC)*. <https://ieeexplore.ieee.org/document/8885915>
- Hojjati, M., Shafieinejad, A., and Yanikomeroglu, H. (2020). A Blockchain-Based Authentication and Key Agreement (AKA) Protocol for 5G Networks, 8, 216461-216476. <https://ieeexplore.ieee.org/document/9276451>
- Huang, H., Hu, L., Chu, J., and Cheng, X. (2019). An Authentication Scheme to Defend Against UDP DrDoS Attacks in 5G Networks, 7, 175970-175979. <https://ieeexplore.ieee.org/document/8922689>
- Jiang, L., Chang, X., Bai, J., MIŠIĆ, J., MIŠIĆ, V., and Chen, Z. (2020). Dependability Analysis of 5G-AKA Authentication Service from Server and User Perspectives. *IEEE Access* 8, 89562-89574. <https://ieeexplore.ieee.org/document/9089007>
- Kalalas, C., and Alonso-Zarate, J. (2020). Lightweight and Space-efficient Vehicle Authentication based on Cuckoo Filter. *5G World Forum (5GWF)*. <https://ieeexplore.ieee.org/document/9221363>
- Khan, J. A., and Chowdhury, M. M. (2021). Security Analysis of 5G Network. *International Conference on Electro Information Technology (EIT)*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9491923>
- Kim, J., Gurbi, D. D., Astillo, P. V., Park, H.-Y., Kim, B., You, I., and Sharma, V. (2021). A Formally Verified Security Scheme for Inter-gNB-DU Handover in 5G

- Vehicle-to-Everything. *IEEE Vehicular Technology Society Section*, 9, 119100-119117). <https://ieeexplore.ieee.org/document/9521489>
- Kiyemba Edris, E. K., Aiash, M., and Loo, J. K.-K. (2020). Formal Verification and Analysis of Primary Authentication based on 5G-AKA Protocol. *7th International Conference on Software Defined Systems (SDS)*. <https://ieeexplore.ieee.org/abstract/document/9143899>
- Koutsos, A. (2019). The 5G-AKA Authentication Protocol Privacy. Proceedings of the European Symposium on Security and Privacy (EuroS&P). DOI: 10.1109/EuroSP.2019.00041
- Li, W., Wang, M., Jiao, L., and Zeng, K. (2021). Physical Layer Spoofing Attack Detection in MmWave Massive MIMO 5G Networks. *IEEE Access*, 9, [https://www.researchgate.net/publication/350881590\\_Physical\\_Layer\\_Spoofing\\_Attack\\_Detection\\_in\\_MmWave\\_Massive\\_MIMO\\_5G\\_Networks](https://www.researchgate.net/publication/350881590_Physical_Layer_Spoofing_Attack_Detection_in_MmWave_Massive_MIMO_5G_Networks)
- Li, Y., Zhao, Y., Li, J., Zhang, J., Yu, X., and Zhang, J. (2020). Side Channel Attack-Aware Resource Allocation for URLLC and eMBB Slices in 5G RAN. *IEEE Access*, 8, <https://ieeexplore.ieee.org/document/8943209>
- Liu, F., Peng, J., and Zuo, M. (2018). Toward a Secure access to 5G Network. *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*. <https://ieeexplore.ieee.org/document/8456025>
- Liu, J., Yan, Z., Gu, C., Gu, Y., and Huang, H. (2021). Security Verification and Improvement of 5G AKA Protocol Based on Petri-Net. *International Conference on Communications in China (ICCC)*. <https://ieeexplore.ieee.org/document/8456025>
- Liu, J., Zhang, L., Sun, R., Du, X., and Guizani, M. (2018). Mutual Heterogeneous Signcryption Schemes for 5G Network Slicings. *IEEE, Special Section on Recent Advances on Radio Access and Security Methods in 5G Networks*, 7854-7863. <https://ieeexplore.ieee.org/document/8268052>
- Liu, P., Liu, B., Sun, Y., Zhao, B., and You, I. (2018). Mitigating DoS Attacks Against Pseudonymous Authentication Through Puzzle-Based Co-Authentication in

- 5G-Vanet. *IEEE Access*, 6, 20795-20806.  
<https://ieeexplore.ieee.org/document/8337735>
- Melki, R., Noura, H. N., and Chehab, A. (2019). Lightweight and Secure D2D Authentication and Key Management based on PLS. *IEEE Access, 90th Vehicular Technology Conference (VTC2019-Fall)*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8891531>
- Mina Labib, Sean Ha, Walid Saad, & Jeffrey H. Reed. (2015). A Colonel Blotto Game for Anti-Jamming in the Internet of Things. *IEEE Global Communications Conference*. <https://ieeexplore.ieee.org/document/7417437>
- Mobarhan, M. A. (2020). AVISPA+SPAN. Eastern Mediterranean University, Famagusta, TRNC.
- Modiri, M. M., Mohajeri, J., and Salmasizadieh, M. (2018). GSL-AKA: Group-based Secure Lightweight Authentication and Key Agreement Protocol for M2M Communication. *9th International Symposium on Telecommunications (IST)*.  
<https://ieeexplore.ieee.org/document/8661145>
- Nowak, T. W., Sepczuk, M., Kotulski, Z., Niewolski, W., Artych, R., Bocianiak, K., Osko, T., and Wary, J.-P. (2021). Verticals in 5G MEC-Use Cases and Security Challenges. *IEEE Access*, 9, 87251-87298  
<https://ieeexplore.ieee.org/document/9450804>
- Ouaissa, M., and Ouaissa, M. (2020). An Improved Privacy Authentication Protocol for 5G Mobile Networks. *International Conference on Advances in Computing, Communication and Materials (ICACCM)*.  
<https://ieeexplore.ieee.org/document/9212910>
- Ouaissa, M., Houmer, M., and Ouaissa, M. (2020). An Enhanced Authentication Protocol based Group for Vehicular Communications over 5G Networks. *3rd International Conference on Advanced Communication Technologies and Networking (CommNet)*. <https://ieeexplore.ieee.org/document/9199641>
- Pari, S. N., R, A. V., M, A., and M, B. (2020). Randomized 5G AKA Protocol Ensembling Security in Fast Forward Mobile Device. *11th International Conference on Advanced Computing (ICoAC)*. <https://ieeexplore.ieee.org/document/9087258>

- Park, S., Kwon, S., Park, Y., Kim, D., and You, I. (2022). Session Management for Security Systems in 5G Standalone Network. *IEEE Access*, 10. [https://www.researchgate.net/publication/362970041\\_Session\\_Management\\_for\\_Security\\_Systems\\_in\\_5G\\_Standalone\\_Network](https://www.researchgate.net/publication/362970041_Session_Management_for_Security_Systems_in_5G_Standalone_Network)
- Parne, B. L., Gupta, S., Gandhi, K., and Meena, S. (2021). PPSE: Privacy Preservation and Security Efficient AKA Protocol for 5G Communication Networks. *International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. <https://ieeexplore.ieee.org/document/9342780>
- Piqueras Jover, R., and Marojevic, V. (2019). Security and Protocol Exploit Analysis of the 5G Specifications. *IEEE Access*, 7, <https://ieeexplore.ieee.org/document/8641117>
- R. Harel (2016). 5G Security Recommendations Package #1. *NGMN Alliance*. <https://www.ngmn.org/publications/5g-security-recommendations-package-1.html>
- Sharma, A., Sharma, I., and Jain, A. (2019). A Construction of Security Enhanced and Efficient Handover AKA Protocol in 5G Communication Network. *IEEE Access. 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. <https://ieeexplore.ieee.org/document/8944569>
- Shin, S., and Kwon, T. (2020). A Privacy-Preserving Authentication and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things. *IEEE Access*, 8, 67555-67571. <https://ieeexplore.ieee.org/document/9057455>
- Sullivan, S., Brighente, A., Kumar, S. A. P., and Conti, M. (2021). 5G Security Challenges and Solutions: A Review by OSI Layers. *IEEE Access*, 9. <https://ieeexplore.ieee.org/abstract/document/9514842>
- Vasudevan, V. A., Tselios, C., and Politis, I. (2022). On Security Against Pollution Attacks in Network Coding Enabled 5G Networks. *IEEE Access*, 8. <https://ieeexplore.ieee.org/document/9006864>
- Yungaicela-Naula, N. M., Vargas-Rosales, C., and Perez-Diaz, J. A. (2021). SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by

Using Machine and Deep Learning. *IEEE Access*, 9, 108495-108512.  
<https://ieeexplore.ieee.org/document/9502698>

## **APPENDICES**

# APPENDIX A

## UE's Role in the ES-AKA Protocol

```
Applications Places System Tue Jan 16, 8:17 PM span
es-aka.hpsl (~/Desktop) - gedit
File Edit View Search Tools Documents Help
es-aka.hpsl
*****UE*****
role rUE (UE , SEAF , AUSF , ARPF : agent ,
  OPID , MobileID , PersID , SeafID , ArpfID , AusfID , SQN : text ,
  HashF1 , HashF2 , HashF3 , HashF4 , HashF5 , HashF6 , HashF7 , HashF8 , HashF9 : hash_func ,
  PublicKeyUE , PublicKeyUEARPF , PublicKeySEAF , PublicKeyARPF , PublicKeyAUSF : public_key ,
  SND_SEAF , RCV_SEAF : channel(dy))

played_by UE
def=
  local
    State:nat,
    UEsecID , ARPFsecID , SEAFsecID , AUSFsecID,
    XRES , RXRES , AUTNofNetwork,
    AuthMsg , SecurityP1 , SecurityP2 , SecurityP3 , NonceSEAF ,
    RandUE1 , RandUE2 , RandSEAF , RandAUSF , RandARPF : text

  const useaf_opID , useaf_persID , useaf_MobileID , useaf_UEsecID , useaf_RandUE1 ,
  useaf_RandUE2 , useaf_AUTNofNetwork : protocol_id

  init
    State := 0
  transition
    1. State=0 /\ RCV_SEAF(start) => State':=1
      /\ RandUE1':=new()
      /\ RandUE2':=new()
      /\ UEsecID':= HashF1(xor(RandUE2' , MobileID))
      /\ SND_SEAF({UEsecID'.RandUE1'.OPID.PersID}_PublicKeySEAF)

      /\ secret(OPID , useaf_opID , { UE , SEAF })
      /\ secret(MobileID , useaf_MobileID , { UE , SEAF })
      /\ secret(PersID , useaf_persID , { UE , SEAF })
      /\ secret(UEsecID , useaf_UEsecID , { UE , SEAF })
      /\ secret(RandUE1' , useaf_RandUE1 , { UE , SEAF })
      /\ secret(RandUE2' , useaf_RandUE2 , { UE , SEAF })

      7. State=1 /\ RCV_SEAF({AUTNofNetwork'}_inv
(PublicKeySEAF).RandARPF'.RandSEAF'.RandAUSF'.SEAFsecID'}_PublicKeyUE) => State':=2
      /\ ARPFsecID':= HashF4(ArpfID.OPID.MobileID.PersID.xor(RandUE1 , RandARPF'))
      /\ SEAFsecID':= HashF2(SeafID.RandUE1.RandUE2.xor(RandSEAF' , PersID))
      /\ SecurityP1':= HashF5(xor(RandARPF' , RandUE1))
      /\ SecurityP2':= HashF6(xor(RandARPF' , RandUE1))
      /\ SecurityP3':= HashF7(xor(RandARPF' , RandUE1))
      /\ XRES':= HashF9(SEAFsecID'.SQN.RandARPF')
      /\ AUTNofNetwork':= HashF8(ARPFsecID'.UEsecID.xor(xor(RandARPF' , RandSEAF' ) , RandUE1))
      /\ RXRES':= HashF9(XRES'.AUTNofNetwork')
      /\ SND_SEAF({SecurityP1'.{RXRES'}_inv(PublicKeyUE)}_PublicKeySEAF)

      /\ request (UE , SEAF , useaf_AUTNofNetwork , AUTNofNetwork')

    11. State=2 /\ RCV_SEAF({AuthMsg.{NonceSEAF'}_inv(PublicKeySEAF)}_PublicKeyUE) => State':=3

end role
```

Appendix A illustrates a snapshot of the UE's role, which can be broken down into three sections:

- Declaration of Parameters of the UE: This section encompasses the parameters set at the current node, those generated for future transmission, and those received.
- Authentication and Secrecy Goals: The second section outlines the specified authentication and secrecy goals essential for verification. As discussed earlier in this research, these goals ensure mutual authentication and verify that the parameters remain untampered with.
- Transitions performed by the UE during the Authentication Process: Lastly, this section covers the transitions that occur throughout the authentication process.

To clarify, this process is applied to the remaining three involved nodes (SEAF, AUSF, and ARPF). However, it's important to note that each of these nodes has its own unique mechanisms, parameters, goals, and transitions.



## APPENDIX B

### Session Role of the Proposed Protocol

```
Applications Places System
es-aka.hpsl (~/.Desktop) - gedit
Tue Jan 16, 8:32 PM span
File Edit View Search Tools Documents Help
Open Save Undo
es-aka.hpsl *
role session(UE , SEAF , AUSF , ARPF :agent,
PersID, OPID, MobileID, SeafID , ArpfID , AusfID, SQN,
UEsecID, ARPFsecID , SEAFsecID, AUSFsecID, AUTNofNetwork, XRES, RXRES, AuthMesg,
SecurityP1, SecurityP2, SecurityP3,
RandUE1 , RandUE2 , RandARPF , RandSEAF , RandAUSF, NonceSEAF :text,
HashF1, HashF2, HashF3, HashF4, HashF5, HashF6, HashF7, HashF8, HashF9: hash func,
PublicKeyUE, PublicKeySEAF, PublicKeyAUSF, PublicKeyARPF, PublicKeyUEARPF : public_key,
K: symmetric_key)
def=
local
SND_SEAF1, RCV_SEAF1,
SND_UE2 , RCV_UE2 , SND_AUSF2 , RCV_AUSF2,
SND_SEAF3 , RCV_SEAF3 , SND_ARPF3 , RCV_ARPF3,
SND_AUSF4, RCV_AUSF4 : channel(dy)
composition

rUE(UE , SEAF , AUSF , ARPF ,
OPID , MobileID , PersID , SeafID , ArpfID , AusfID , SQN ,
HashF1, HashF2, HashF3, HashF4, HashF5, HashF6, HashF7, HashF8, HashF9,
PublicKeyUE, PublicKeyUEARPF, PublicKeySEAF, PublicKeyARPF , PublicKeyAUSF,
SND_SEAF1 , RCV_SEAF1)
/\ rSEAF(UE , SEAF , AUSF , ARPF,
OPID, PersID, MobileID, SeafID, AusfID, ArpfID, SecurityP1,
HashF1, HashF2, HashF3, HashF4, HashF5, HashF6, HashF7, HashF8, HashF9,
PublicKeySEAF, PublicKeyUE, PublicKeyARPF, PublicKeyAUSF, K,
SND_UE2 , RCV_UE2 , SND_AUSF2 , RCV_AUSF2)
/\ rAUSF(UE , SEAF , AUSF , ARPF,
OPID, PersID, SeafID , AusfID , ArpfID, SecurityP1,
HashF1, HashF2, HashF3, HashF4, HashF5, HashF6, HashF7, HashF8, HashF9,
PublicKeySEAF, PublicKeyUE, PublicKeyARPF, PublicKeyAUSF, K,
SND_SEAF3 , RCV_SEAF3 , SND_ARPF3 , RCV_ARPF3)

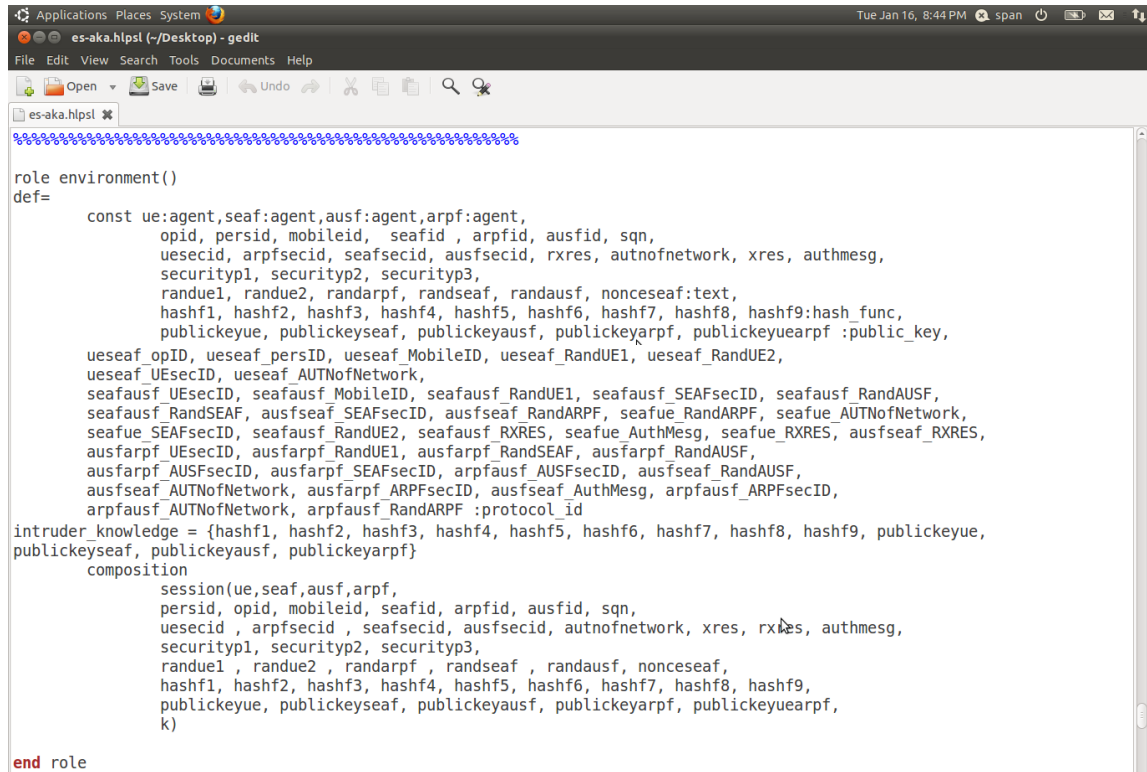
/\ rARPF(UE , SEAF , AUSF , ARPF,
OPID, MobileID, PersID, AusfID, ArpfID, SeafID, SQN,
HashF1, HashF2, HashF3, HashF4, HashF5, HashF6, HashF7, HashF8, HashF9,
PublicKeyUE, PublicKeyARPF, PublicKeyAUSF, PublicKeySEAF, PublicKeyUEARPF, K,
SND_AUSF4, RCV_AUSF4)
end role
~~~~~
```

The term 'session role' in ES-AKA Protocol is commonly used to describe the specific role that a device or entity takes on during a communication session, especially when authenticating and establishing security keys. It plays a crucial role in determining the responsibilities and actions of each participant in the authentication process.

In Appendix B, the session role comprises two essential elements. Firstly, it involves the declaration of parameters and the identification of channels through which data is transmitted. Secondly, it encompasses the composition of all nodes involved in the phase of authentication.

# APPENDIX C

## Environment Function

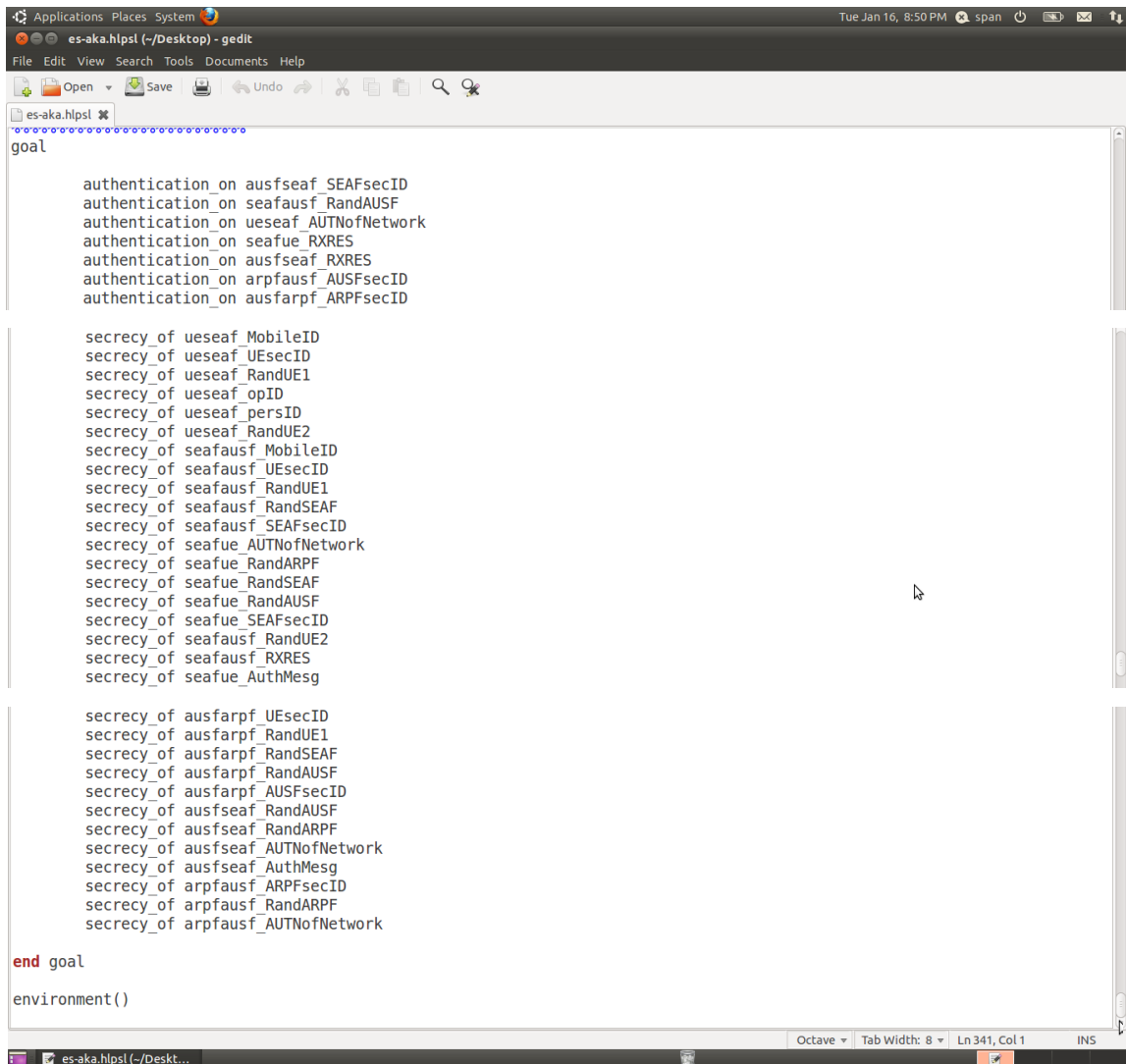


```
role environment()
def=
    const ue:agent,seaf:agent,ausf:agent,arpf:agent,
        opid, persid, mobileid, seafid, arpfid, ausfid, sqn,
        usesecid, arpfsecid, seafsecid, ausfsecid, rxres, autnofnetwork, xres, authmesg,
        securityp1, securityp2, securityp3,
        randue1, randue2, randarpf, randseaf, randausf, noncesseaf:text,
        hashf1, hashf2, hashf3, hashf4, hashf5, hashf6, hashf7, hashf8, hashf9:hash_func,
        publickeyue, publickeyseaf, publickeyausf, publickeyarpf, publickeyearpf :public_key,
        useseaf_opID, useseaf_persID, useseaf_MobileID, useseaf_RandUE1, useseaf_RandUE2,
        useseaf_UsecID, useseaf_AutNofNetwork,
        seafausf_UsecID, seafausf_MobileID, seafausf_RandUE1, seafausf_SEAFsecID, seafausf_RandAUSF,
        seafausf_RandSEAF, ausfseaf_SEAFsecID, ausfseaf_RandARPF, seafue_RandARPF, seafue_AutNofNetwork,
        seafue_SEAFsecID, seafausf_RandUE2, seafausf_RXRES, seafue AuthMesg, seafue_RXRES, ausfseaf_RXRES,
        ausfarpf_UsecID, ausfarpf_RandUE1, ausfarpf_RandSEAF, ausfarpf_RandAUSF,
        ausfarpf_AUSFsecID, ausfarpf_SEAFsecID, arpfäusf_AUSFsecID, ausfseaf_RandAUSF,
        ausfseaf_AutNofNetwork, ausfarpf_ARPFsecID, ausfseaf_AuthMesg, arpfäusf_ARPFsecID,
        arpfäusf_AutNofNetwork, arpfäusf_RandARPF :protocol_id
    intruder_knowledge = {hashf1, hashf2, hashf3, hashf4, hashf5, hashf6, hashf7, hashf8, hashf9, publickeyue,
        publickeyseaf, publickeyausf, publickeyarpf}
    composition
        session(ue,seaf,ausf,arpf,
            persid, opid, mobileid, seafid, arpfid, ausfid, sqn,
            usesecid, arpfsecid, seafsecid, ausfsecid, autnofnetwork, xres, rxres, authmesg,
            securityp1, securityp2, securityp3,
            randue1, randue2, randarpf, randseaf, randausf, noncesseaf,
            hashf1, hashf2, hashf3, hashf4, hashf5, hashf6, hashf7, hashf8, hashf9,
            publickeyue, publickeyseaf, publickeyausf, publickeyarpf, publickeyearpf,
            k)
end role
```

In Appendix C, the ‘environment()’ function serves as a comprehensive container for the entire system settings. It encompasses protocol configurations, manages sessions, incorporates all parameters utilized by agents or nodes, defines goals, and takes into account potential threats from an intruder. This assumes that the attacker possesses information on all public keys, including PublicKeyUE, PublicKeySEAF, PublicKeyAUSF, and PublicKeyARPF, as well as knowledge of hash functions HashF1 through HashF9.

# APPENDIX D

## Secrecy and Authentication Goals



```
goal
authentication_on ausfseaf_SEAFsecID
authentication_on seafausf_RandAUSF
authentication_on useaf_AUTNoNetwork
authentication_on seafue_RXRES
authentication_on ausfseaf_RXRES
authentication_on arpfausef_AUSFsecID
authentication_on ausfarpf_ARPFsecID

secrecy_of useaf_MobileID
secrecy_of useaf_UsecID
secrecy_of useaf_RandUE1
secrecy_of useaf_opID
secrecy_of useaf_persID
secrecy_of useaf_RandUE2
secrecy_of seafausf_MobileID
secrecy_of seafausf_UsecID
secrecy_of seafausf_RandUE1
secrecy_of seafausf_RandSEAF
secrecy_of seafausf_SEAFsecID
secrecy_of seafue_AUTNoNetwork
secrecy_of seafue_RandARPF
secrecy_of seafue_RandSEAF
secrecy_of seafue_RandAUSF
secrecy_of seafue_SEAFsecID
secrecy_of seafausf_RandUE2
secrecy_of seafausf_RXRES
secrecy_of seafue_AuthMesg

secrecy_of ausfarpf_UsecID
secrecy_of ausfarpf_RandUE1
secrecy_of ausfarpf_RandSEAF
secrecy_of ausfarpf_RandAUSF
secrecy_of ausfarpf_AUSFsecID
secrecy_of ausfseaf_RandAUSF
secrecy_of ausfseaf_RandARPF
secrecy_of ausfseaf_AUTNoNetwork
secrecy_of ausfseaf_AuthMesg
secrecy_of arpfausef_ARPFsecID
secrecy_of arpfausef_RandARPF
secrecy_of arpfausef_AUTNoNetwork

end goal
environment()
```

Appendix D illustrates the secrecy and authentication goals explicitly addressed to prevent unauthorized or third parties from intercepting user data and compromising the network. This strengthens overall security, enabling the system to withstand known attacks including DoS / DDoS, eavesdropping, impersonation, jamming, reply, and MitM attacks.

## APPENDIX E

### Definition of Secrecy and Authentication Goals

Defined Security Goal	Description	Defined Security Goal	Description
Authentication_on useaf_AUTNofNetwork	SEAF was correctly authenticated by UE using AUTNofNetwork	Secrecy_of seafausf_RXRES	The SEAF securely transmits RXRES to AUSF
Authentication_on seafue_RXRES	UE was correctly authenticated by SEAF using RXRES	Secrecy_of seafue_AUTNofNetwork	The SEAF securely transmits AUTNofNetwork to UE
Authentication_on seafausf_RandAUSF	AUSF was correctly authenticated by SEAF using RandAUSF	Secrecy_of seafue_AuthMesg	The SEAF securely transmits AuthMesg to UE
Authentication_on ausfseaf_SEAFsecID	SEAF was correctly authenticated by AUSF using SEAFsecID	Secrecy_of seafue_SEAFsecID	The SEAF securely transmits SEAFsecID to UE
Authentication_on ausfseaf_RXRES	SEAF was correctly authenticated by AUSF using RXRES	Secrecy_of seafue_RandARPF	The SEAF securely transmits RandARPF to UE
Authentication_on ausfarpf_ARPFsecID	ARPF was correctly authenticated by AUSF using ARPFsecID	Secrecy_of seafue_RandSEAF	The SEAF securely transmits RandSEAF to UE
Authentication_on arpfausf_AUSFsecID	AUSF was correctly authenticated by ARPF using AUSFsecID	Secrecy_of seafue_RandAUSF	The SEAF securely transmits RandAUSF to UE
Secrecy_of useaf_MobileID	The UE securely transmits MobileID to SEAF	Secrecy_of ausfarpf_UEsecID	The AUSF securely transmits UEsecID to ARPF
Secrecy_of useaf_UEsecID	The UE securely transmits UEsecID to SEAF	Secrecy_of ausfarpf_RandUE1	The AUSF securely transmits RandUE1 to ARPF
Secrecy_of useaf_RandUE1	The UE securely transmits RandUE1 to SEAF	Secrecy_of ausfarpf_RandSEAF	The AUSF securely transmits RandSEAF to ARPF
Secrecy_of useaf_opID	The UE securely transmits opID to SEAF	Secrecy_of ausfarpf_RandAUSF	The AUSF securely transmits RandAUSF to ARPF

## Appendix E (continued)

### *Definition of Secrecy and Authentication Goals*

Defined Security Goal	Description	Defined Security Goal	Description
Secrecy_of useaf_persID	The UE securely transmits persID to SEAF	Secrecy_of ausfarpf_AUSFsecID	The AUSF securely transmits AUSFsecID to ARPF
Secrecy_of useaf_RandUE2	The UE securely transmits RandUE2 to SEAF	Secrecy_of ausfarpf_RandAUSF	The AUSF securely transmits RandAUSF to ARPF
Secrecy_of seafausf_MobileID	The SEAF securely transmits MobileID to AUSF	Secrecy_of ausfarpf_RandARPF	The AUSF securely transmits RandARPF to ARPF
Secrecy_of seafausf_UEsecID	The SEAF securely transmits UEsecID to AUSF	Secrecy_of ausfarpf_AUTNofNetwork	The AUSF securely transmits AUTNofNetwork to ARPF
Secrecy_of seafausf_RandUE1	The SEAF securely transmits RandUE1 to AUSF	Secrecy_of ausfarpf_AuthMesg	The AUSF securely transmits AuthMesg to ARPF
Secrecy_of seafausf_RandSEAF	The SEAF securely transmits RandSEAF to AUSF	Secrecy_of arpfausef_ARPFsecID	The ARPF securely transmits ARPFsecID to AUSF
Secrecy_of seafausf_SEAFsecID	The SEAF securely transmits SEAFsecID to AUSF	Secrecy_of arpfausef_RandARPF	The ARPF securely transmits RandARPF to AUSF
Secrecy_of seafausf_RandUE2	The SEAF securely transmits RandUE2 to AUSF	Secrecy_of arpfausef_AUTNofNetwork	The ARPF securely transmits AUTNofNetwork to AUSF

Appendix E presents a detailed table outlining the defined goals of the ES-AKA method. The table includes crucial aspects such as Authentication, Secrecy, and the secure transmission of key parameters. For instance, the goal 'Authentication\_on useaf\_AUTNofNetwork' signifies that SEAF was correctly authenticated by UE using AUTNofNetwork. Similarly, 'Secrecy\_of seafausf\_RXRES' denotes the secure transmission of RXRES from SEAF to AUSF. However, each goal is meticulously designed to ensure the safety and security of the communication process. Through these

defined objectives, this approach demonstrates its robustness in safeguarding key authentication and secrecy elements in the specified network interactions.

# APPENDIX F

## Turinit Report

ORIGINALITY REPORT		
<b>12%</b>	<b>7%</b>	<b>9%</b>
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS
		<b>4%</b>
		STUDENT PAPERS
PRIMARY SOURCES		
<b>1</b>	<b>Submitted to The Scientific &amp; Technological Research Council of Turkey (TUBITAK)</b> Student Paper	<b>1 %</b>
<b>2</b>	<b>www.researchgate.net</b> Internet Source	<b>1 %</b>
<b>3</b>	<b>Mostafa Ayoubi Mobarhan, Mohammed Salamah. "REPS-AKA3: A secure authentication and re- authentication protocol for LTE networks", Journal of Network and Computer Applications, 2022</b> Publication	<b>&lt;1 %</b>
<b>4</b>	<b>DongFeng Fang, Yi Qian, Rose Qingyang Hu. "5G Wireless Network Security and Privacy", Wiley, 2024</b> Publication	<b>&lt;1 %</b>
<b>5</b>	<b>Maede Hojjati, Alireza Shafieinejad, Halim Yanikomeroğlu. "A Blockchain-Based Authentication and Key Agreement (AKA) Protocol for 5G Networks", IEEE Access, 2020</b> Publication	<b>&lt;1 %</b>
<b>Submitted to Middle East Technical University</b> Student Paper		
<b>6</b>		<b>&lt;1 %</b>
<b>7</b>	<b>fastercapital.com</b> Internet Source	<b>&lt;1 %</b>
<b>8</b>	<b>link.springer.com</b> Internet Source	<b>&lt;1 %</b>
<b>9</b>	<b>Kaihong Han, Maode Ma, Xiaohong Li, Zhiyong Feng, Jianye Hao. "An Efficient Handover Authentication Mechanism for 5G Wireless Network", 2019 IEEE Wireless Communications and Networking Conference (WCNC), 2019</b> Publication	<b>&lt;1 %</b>
<b>10</b>	<b>www.researchsquare.com</b> Internet Source	<b>&lt;1 %</b>
<b>11</b>	<b>pureadmin.qub.ac.uk</b> Internet Source	<b>&lt;1 %</b>
<b>12</b>	<b>Probidita Roychoudhury, Basav Roychoudhury, Dilip K. Saikia. "A secure Device-to-Device communication scheme for massive Machine Type Communication", Computers &amp; Security, 2021</b> Publication	<b>&lt;1 %</b>
<b>13</b>	<b>res.mdpi.com</b> Internet Source	<b>&lt;1 %</b>
<b>repository.mdx.ac.uk</b>		

14	Internet Source	<1 %
15	Sultan Basudan. "LEGA: A Lightweight and Efficient Group Authentication Protocol for Massive Machine Type Communication in 5G Networks", Journal of Communications and Information Networks, 2020 Publication	<1 %
16	docplayer.net Internet Source	<1 %
17	ebin.pub Internet Source	<1 %
18	jultika.oulu.fi Internet Source	<1 %
19	Charalampos Kalalas, Jesus Alonso-Zarate. "Lightweight and Space-efficient Vehicle Authentication based on Cuckoo Filter", 2020 IEEE 3rd 5G World Forum (5GWF), 2020 Publication	<1 %
20	libweb.kpfu.ru Internet Source	<1 %
21	www.mdpi.com Internet Source	<1 %
22	www.uniprot.org Internet Source	<1 %
23	Tuan-Vinh Le. "Cross-Server End-to-End Patient Key Agreement Protocol for DNA-Based U-Healthcare in the Internet of Living Things", Mathematics, 2023 Publication	<1 %
24	Submitted to Foreign Trade University - Ho Chi Minh Campus Student Paper	<1 %
25	Mariya Ouaisa, Mariyam Ouaisa. "An Improved Privacy Authentication Protocol for 5G Mobile Networks", 2020 International Conference on Advances in Computing, Communication & Materials (ICACCM), 2020 Publication	<1 %
26	www.journaltoocs.ac.uk Internet Source	<1 %
27	"Conversational Artificial Intelligence", Wiley, 2024 Publication	<1 %
28	Yibing Liu, Lijun Huo, Gang Zhou. "TR-AKA: A two-phased, registered authentication and key agreement protocol for 5G mobile networks", IET Information Security, 2021 Publication	<1 %
29	Reem Melki, Hassan N. Noura, Ali Chehab. "Lightweight and Secure D2D Authentication & Key Management Based on PLS", 2019 IEEE	<1 %



90th Vehicular Technology Conference  
(VTC2019-Fall), 2019

Publication

30	<a href="https://export.arxiv.org">export.arxiv.org</a> Internet Source	<1 %
31	Jin Cao, Zheng Yan, Ruihui Ma, Yinghui Zhang, Yulong Fu, Hui Li. "LSAA: A Lightweight and Secure Access Authentication Scheme for both UEs and mMTC Devices in 5G Networks", IEEE Internet of Things Journal, 2020 Publication	<1 %
32	Yahya Kadhim Jawad, Mircea Nitulescu. "Transportation Systems for Intelligent Cities", 2023 24th International Carpathian Control Conference (ICCC), 2023 Publication	<1 %
33	Zhiping Yan, Chonglin Gu, Yue Gu, Hejiao Huang. "Security Verification and Improvement of 5G AKA Protocol Based on Petri-net", 2021 IEEE/CIC International Conference on Communications in China (ICCC), 2021 Publication	<1 %
34	<a href="https://uis.brage.unit.no">uis.brage.unit.no</a> Internet Source	<1 %
35	<a href="https://www.slideshare.net">www.slideshare.net</a> Internet Source	<1 %
36	M.M. Modiri, M. Salmasizadeh, J. Mohajeri, B.H. Khalaj. "Two protocols for improving security during the authentication and key agreement procedure in the 3GPP networks", Computer Communications, 2023 Publication	<1 %
37	Submitted to Queensland University of Technology Student Paper	<1 %
38	<a href="https://www.final.edu.tr">www.final.edu.tr</a> Internet Source	<1 %
39	Submitted to Asia Pacific Institute of Information Technology Student Paper	<1 %
40	Jianwei Liu, Lin Bai, Chunxiao Jiang, Wei Zhang. "Chapter 3 Ground Network Security", Springer Science and Business Media LLC, 2023 Publication	<1 %
41	Kamal Ali Alezabi, Fazirulhisyam Hashim, Shaiful Jahari Hashim, Borhanuddin M. Ali. "An efficient authentication and key agreement protocol for 4G (LTE) networks", 2014 IEEE REGION 10 SYMPOSIUM, 2014 Publication	<1 %

42	Submitted to Middlesex University Student Paper	<1 %
43	Submitted to American Public University System Student Paper	<1 %
44	Submitted to Brunel University Student Paper	<1 %
45	Ponjit Borgohain, Hiten Choudhury. "A lightweight D2D authentication protocol for relay coverage scenario in 5G mobile network", Computer Networks, 2023 Publication	<1 %
46	dr.ntu.edu.sg Internet Source	<1 %
47	onlinelibrary.wiley.com Internet Source	<1 %
48	www.comnet-conf.org Internet Source	<1 %
49	"5G and Beyond", Springer Science and Business Media LLC, 2023 Publication	<1 %
50	Shanay Behrad, Emmanuel Bertin, Noel Crespi. "Securing authentication for mobile networks, a survey on 4G issues and 5G answers", 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), 2018 Publication	<1 %
51	Submitted to The University of the West of Scotland Student Paper	<1 %
52	Submitted to University of North Texas Student Paper	<1 %
53	Submitted to University of Warwick Student Paper	<1 %
54	Balu L. Parne, Shubham Gupta, Kaneesha Gandhi, Shubhangi Meena. "PPSE: Privacy Preservation and Security Efficient AKA Protocol for 5G Communication Networks", 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2020 Publication	<1 %
55	Submitted to JBC Skills Training Ltd Student Paper	<1 %
56	extendedstudies.ucsd.edu Internet Source	<1 %
57	intranet.royalholloway.ac.uk Internet Source	<1 %
58	Lili Jiang, Xiaolin Chang, Jing Bai, Jelena Mistic, Vojislav Mistic, Zhi Chen. "Dependability	<1 %

Analysis of 5G-AKA Authentication Service from Server and User Perspectives", IEEE Access, 2020  
Publication

59	Submitted to Stella Maris College Student Paper	<1 %
60	Submitted to University of Sydney Student Paper	<1 %
61	Vipindev Adat Vasudevan, Christos Tselios, Ilias Politis. "On Security Against Pollution Attacks in Network Coding Enabled 5G Networks", IEEE Access, 2020 Publication	<1 %
62	Yajie Li, Yongli Zhao, Jun Li, Jiawei Zhang, Xiaosong Yu, Jie Zhang. "Side Channel Attack-Aware Resource Allocation for URLLC and eMBB Slices in 5G RAN", IEEE Access, 2020 Publication	<1 %
63	Yuelei Xiao, Shan Gao. "5GAKA-LCCO: A Secure 5G Authentication and Key Agreement Protocol with Less Communication and Computation Overhead", Information, 2022 Publication	<1 %
64	Yuelei Xiao, Shan Gao. "Formal Verification and Analysis of 5G AKA Protocol Using Mixed Strand Space Model", Electronics, 2022 Publication	<1 %
65	etd.lib.metu.edu.tr Internet Source	<1 %
66	Submitted to Coventry University Student Paper	<1 %
67	fenix.tecnico.ulisboa.pt Internet Source	<1 %
68	vinit.com.vn Internet Source	<1 %
69	www.comreg.ie Internet Source	<1 %
70	Hemangi Goswami, Hiten Choudhury. "Chapter 15 A Group Authentication Scheme for IoT 5G Network Enabled e-Healthcare System", Springer Science and Business Media LLC, 2023 Publication	<1 %
71	R. Ferrus, O. Sallent, J. Perez-Romero, R. Agusti. "On the Automation of RAN Slicing Provisioning and Cell Planning in NG-RAN", 2018 European Conference on Networks and Communications (EuCNC), 2018 Publication	<1 %
72	S. Neelavathy Pari, R Azhagu Vasanth, M Amuthini, M Balaji. "Randomized 5G AKA Protocol Ensembling Security in Fast Forward Mobile Device", 2019 11th International	<1 %

Conference on Advanced Computing (ICoAC),  
2019  
Publication

73	Shanay Behrad, Emmanuel Bertin, Noel Crespi. "A survey on authentication and access control for mobile networks: from 4G to 5G", <i>Annals of Telecommunications</i> , 2019 Publication	<1 %
74	<a href="https://downloads.hindawi.com">downloads.hindawi.com</a> Internet Source	<1 %
75	<a href="https://wiredspace.wits.ac.za">wiredspace.wits.ac.za</a> Internet Source	<1 %
76	Devaki Chandramouli, Subramanya Chandrashekar, Andreas Maeder, Tuomas Niemela, Thomas Theimer, Laurent Thiebaut. "Next Generation Network Architecture", Wiley, 2019 Publication	<1 %
77	John A. Khan, MD Minhaz Chowdhury. "Security Analysis of 5G Network", 2021 IEEE International Conference on Electro Information Technology (EIT), 2021 Publication	<1 %
78	Mostafa Ayoubi Mobarhan, Muhammed Salamah. "REPS-AKA5: A robust group-based authentication protocol for IoT applications in LTE system", <i>Internet of Things</i> , 2023 Publication	<1 %
79	Submitted to University of Johannesburg Student Paper	<1 %
80	<a href="https://www.digitaljournal.com">www.digitaljournal.com</a> Internet Source	<1 %
81	<a href="https://www.springerprofessional.de">www.springerprofessional.de</a> Internet Source	<1 %
82	Bedran Karakoc, Nils Fürste, David Rupprecht, Katharina Kohls. "Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G", <i>Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks</i> , 2023 Publication	<1 %
83	Bidisha Goswami, Hiten Choudhury. "Chapter 16 Using Blockchain for Fast Re-Authentication in 5G Cellular Network", Springer Science and Business Media LLC, 2023 Publication	<1 %
84	Ikram Gharsallah, Salima Smaoui, Faouzi Zarai. "An efficient authentication and key agreement protocol for a group of vehicles devices in 5G cellular networks", <i>IET Information Security</i> , 2020 Publication	<1 %
85	Vipindev Adat, Ilias Politis, Stavros Kotsopoulos. "A lightweight security framework for network coding enabled	<1 %

mobile small cells", 2020 IEEE 25th  
International Workshop on Computer Aided  
Modeling and Design of Communication Links  
and Networks (CAMAD), 2020  
Publication

86	acikbilim.yok.gov.tr Internet Source	<1 %
87	assets.researchsquare.com Internet Source	<1 %
88	www.allindianpatents.com Internet Source	<1 %
89	www.hindawi.com Internet Source	<1 %
90	www.semanticscholar.org Internet Source	<1 %
91	"M817 Block 2 week 10 asymmetric encryption WEB097768", Open University Publication	<1 %
92	"Security Standardisation Research", Springer Science and Business Media LLC, 2018 Publication	<1 %
93	Akash Kumar Bhagat, Jay Gandhi. "A Comprehensive Analysis of 5G Security Core Technologies and Services: Conceptual Frameworks, Challenges, and Solutions", 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), 2023 Publication	<1 %
94	Chandrashekhar Meshram, Agbotiname Lucky Imoize, Azeddine Elhassouny, Amer Aljaedi, Adel R. Alharbi, Sajjad Shaukat Jamal. "IBOOST: A Lightweight Provably Secure Identity-Based Online/Offline Signature Technique Based on FCM for Massive Devices in 5G Wireless Sensor Networks", IEEE Access, 2021 Publication	<1 %
95	Jingjing Zhang, Lin Yang, Weipeng Cao, Qiang Wang. "Formal Analysis of 5G EAP-TLS Authentication Protocol Using Proverif", IEEE Access, 2020 Publication	<1 %
96	Vincent Omollo Nyangaresi, Musheer Ahmad, Ahmed Alkhayyat, Wei Feng. " Artificial neural network and symmetric key cryptography based verification protocol for enabled Internet of Things ", Expert Systems, 2022 Publication	<1 %
97	Xiongpeng Ren, Jin Cao, Maode Ma, Hui Li, Yinghui Zhang. "A Novel PUF-Based Group Authentication and Data Transmission Scheme for NB-IoT in 3GPP 5G Networks", IEEE Internet of Things Journal, 2022 Publication	<1 %

98	Xiongpeng Ren, Jin Cao, Maode Ma, Hui Li, Yinghui Zhang. "A Novel PUF-based Group Authentication and Data Transmission Scheme for NB-IoT in 3GPP 5G Networks", IEEE Internet of Things Journal, 2021 Publication	<1 %
99	Yi Qian, Feng Ye, Hsiao-Hwa Chen. "Security in Wireless Communication Networks", Wiley, 2022 Publication	<1 %
100	Yue Qiu, Maode Ma, Shuo Chen. "An anonymous authentication scheme for multi-domain machine-to-machine communication in cyber-physical systems", Computer Networks, 2017 Publication	<1 %
101	dokumen.pub Internet Source	<1 %
102	e-archivo.uc3m.es Internet Source	<1 %
103	mainlab.cs.ccu.edu.tw Internet Source	<1 %
104	nova.newcastle.edu.au Internet Source	<1 %
105	publications.eai.eu Internet Source	<1 %
106	scholars.wlu.ca Internet Source	<1 %
107	www.tcs.hut.fi Internet Source	<1 %
108	"Challenges in the IoT and Smart Environments", Springer Science and Business Media LLC, 2021 Publication	<1 %
109	Agni Datta, Aditya Srivastav, Thangavel Murugan. "chapter 26 Lightweight Cryptography for Cyber-Physical Systems", IGI Global, 2023 Publication	<1 %
110	Jin Cao, Maode Ma, Hui Li, Ruhui Ma, Yunqing Sun, Pu Yu, Lihui Xiong. "A Survey on Security Aspects for 3GPP 5G Networks", IEEE Communications Surveys & Tutorials, 2020 Publication	<1 %
111	Lathi, B.P.. "Modern Digital and Analog Communication", Oxford University Press Publication	<1 %
112	engagedscholarship.csuohio.edu Internet Source	<1 %
113	ojs.bibsys.no Internet Source	<1 %

114	"A Generic Construction for Efficient and Secure AKA Protocol in 5G Network", 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2018 Publication	<1 %
115	Alican Ozhelvaci, Maode Ma. " Security for Handover and Communication in ", Wiley, 2020 Publication	<1 %
116	Awaneesh Kumar Yadav, Manoj Misra, Pradumn Kumar Pandey, An Braeken, Madhusanka Liyange. "An improved and provably secure symmetric-key based 5G-AKA Protocol", Computer Networks, 2022 Publication	<1 %
117	Dongfeng Fang, Yi Qian, Rose Qingyang Hu. "Security for 5G Mobile Wireless Networks", IEEE Access, 2018 Publication	<1 %
118	Ed Kanya Kiyemba Edris, Mahdi Aiash, Jonathan Loo. "Formal Verification of Authentication and Service Authorization Protocols in 5G-Enabled Device-To-Device Communications Using ProVerif", Electronics, 2021 Publication	<1 %
119	I. O. Yuskov, E. P. Stroganova. "Application of Neural Network Model Design for Monitoring Wireless Communication Networks", 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, 2020 Publication	<1 %
120	Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei Gurtov, Mika Ylianttila. "Security for 5G and Beyond", IEEE Communications Surveys & Tutorials, 2019 Publication	<1 %
121	Rabia Khan, Pardeep Kumar, Dushantha Nalin K. Jayakody, Madhusanka Liyanage. "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions", IEEE Communications Surveys & Tutorials, 2020 Publication	<1 %
122	Roshan Sedar, Charalampos Kalalas, Francisco Vazquez-Gallego, Luis Alonso, Jesus Alonso-Zarate. "A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths", IEEE Open Journal of the Communications Society, 2023 Publication	<1 %
123	Sudip Kumar Palit, Mohuya Chakraborty, Subhalaxmi Chakraborty. "Performance	<1 %

analysis of 5GMAKA: lightweight mutual authentication and key agreement scheme for 5G network", The Journal of Supercomputing, 2022

Publication

124

Vincent Yong Kai Loung, Razali Ngah, Joseph Owusu, Chua Tien Han, Samuel Tweneboah-Koduah, Jafri Din. "Key Technologies and Future Trends of 5G Wireless Network Applications", 2021 IEEE 6th International Conference on Signal and Image Processing (ICSIP), 2021

Publication

<1%