An Improved Privacy Authentication Protocol for 5G Mobile Networks

Mariya Ouaissa, Mariyam Ouaissa
Laboratory of Mathematics and Computer Science, ENSAM
Moulay Ismail University
Meknes, Morooco
mariya.ouaissa@edu.umi.ac.ma, mariyam.ouaissa@edu.umi.ac.ma

***Abstract*—Mobile communication networks have always undergone continuous and rapid evolution since their launch as telephone networks only. From one generation to the next, services have multiplied and diversified to include data first, then video and many other services as they go along. This progress was followed by an exponential growth in the number of users and mobile devices, and consequently, in the volume of data traffic. Fifth Generation (5G) is a new generation of mobile telephony standards. This wireless telecommunications technology promises to revolutionize the way the world communicates by supporting a set of requirements such as quality of service, performance for the integration of new services and network security. The 3rd Generation Partnership Project (3GPP) proposed an Authentication and Key Agreement (AKA) protocol named 5G-AKA for the 5G network in order to improve the security requirements and surmount the vulnerabilities existing in EPS-AKA protocol of Fourth Generation (4G) network. In this work, we propose an improved and efficient authentication and key agreement protocol for 5G mobile network, that overcome the weakness discover in the existing 5G-AKA and using of lightweight cryptographic methods in order to increase the computational cost in different entities. For the validation and verification of our proposed, we use Automated Validation of Internet Security Protocols and Applications (AVISPA) tool to demonstrate that the objectives of authentication and security are checked. In addition, the performance evaluation in terms of different metrics illustrates that our solution outperforms several 3GPP authentication protocols.**

Keywords—5G, 5G-AKA, 3GPP, Authentication, Privacy.

I. INTRODUCTION

In recent years, we have witnessed an exponential development of new applications and technologies in the fields of health, media, industry, transport, energy, etc. This evolution goes hand in hand with the appearance of new services linked to a proliferation of connected objects [1]. The world is becoming more and more digital where everything is connected. The objects will be connected to each other, on the internet and with billions of people. This increase requires a lot of progress on mobile telecommunications systems, although the current Fourth Generation (4G) network based on the Long Term Evolution (LTE) standard [2] has brought many solutions such as the increase in speed and bandwidth compared to older generations of mobile networks. Using IP technology, 4G enables comfortable internet browsing with smartphones, tablets or laptops. However in this network, the frequency spectrum of which is fairly overloaded, will no longer be able to meet the various requirements due to the development of connected objects with their different categories of uses.

Faced with these problems, a new revolution is announced with a new standard for mobile telecommunications systems, called Fifth Generation (5G). This standard opens perspectives to meet current needs, but also those of the future, when we will have several hundred billion connected objects and autonomous cars. Faced with all these requirements, the future generation of mobile telecommunications systems will have to combine several technologies in order to have a mobile network that can meet expectations [3]. The 5G network is, of course, vulnerable to attack. Time and time again, offenders have been able to access communications while connecting the device to the network to intercept conversations or steal data.

In order to support security, the device and the network must be able to authenticate each other at the time of connection. At the same time, user data, identity and location must be kept confidential. For this, a communication protocol called Authentication and Key Agreement (AKA) [4] has been implemented since the introduction of the Third Generation (3G) standard which works by negotiating and establishing keys to encrypt communications between a telephone and the cellular network. The AKA version designed for the 5G protocol, also known as 5G-AKA standardized by The 3rd Generation Partnership Project (3GPP), had however been specially designed to thwart International Mobile Subscriber Identity (IMSI) collectors, with a reinforced authentication negotiation system.

The protection of data transmitted at very high speed by 5G is improved compared to 3G and 4G. The conception of 5G-AKA protocol is an improved secure version of EPS-AKA protocol standardized in 4G network, but there are some weaknesses in this new authentication protocol that will be affected the privacy of users and data security in 5G network. Therefore, it is necessary to enhance the 5G-AKA protocol in order to establish a strong authentication procedure [5].

In this paper, we propose an enhanced version of authentication and key agreement protocol for 5G system that surmount the limitations existing in 5G-AKA standard. The objective of our proposed is to guarantee the privacy preservation of subscriber identity of mobile, avoid IMSI catchers, and exchange the secret key K between network equipment and also using a set of lightweight cryptographic methods in order to increase the computational cost in different entities.

The remainder of this paper is organized as follows: the next section presents the background includes system architecture, description of existing protocol 5G-AKA and their weakness. In section 3, we propose our improved secure

978-1-7281-9785-2/20/$31.00 ©2020 IEEE

protocol for 5G network. Section 4 analyzes the security of our proposed using a formal verification and evaluates the performances of the existing protocols as well as our proposition. Finally, we draw our conclusion in Section 5.

II. Background

In this section, we describe the system architecture of 5G communication and we present the existing protocol 5G-AKA and their weakness

A. System Architecture

The 5G network consists of a New Generation Radio Access Network (NG-RAN) and a 5G Core (5GC) network. Fig.1 shows the 5G architecture and the interfaces between each entity [6].

5G radio access consists of new generation base stations which form the connection node for mobiles with 5GC network. User Equipment (UE) mobiles communicate with base stations by a 5G radio link called Generation Node Base (gNB) station. The functions of the gNB base station are quite similar with the Evolved NB (eNB) entity. However, the differences concern the management of the quality of service by flow and not by medium and the management of network slices on the radio interface.

The 5G core network is suitable for network virtualization and is based on the division of the control plane and the user plane. Thus, the entities that manage both the attachment of mobiles, the location and the creation of bearers in 5G are, the Access and Mobility Management Function (AMF) entity establishes a NAS connection with the UE mobile and has the role of registering the UE mobiles and managing the location of the mobiles on the 3GPP and non-3GPP networks. AMF is collocated with the SEcurity Anchor Function (SEAF) that holds the root key known as anchor key for the visited network, the Session Management Function (SMF) entity is used to control Packet Data Network (PDN) sessions.

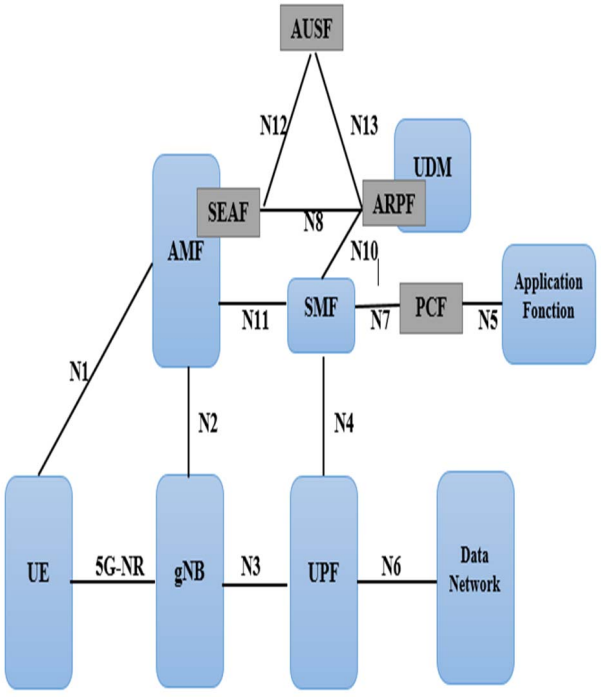

Fig. 1. System Architecture

For the 5G core network, the transport plan functions are the responsibility of the User Plane Function (UPF). The Policy Charging Function (PCF) entity makes it possible to control flows both at the level of the SMF entity but also at the level of the AMF entity to be able to provide better granularity on the authorized flows taking into account the location of the mobile UE. The registration of the mobile requires double authentication performed at the level of the AMF entity and of the mobile UE using authentication vectors provided by the AUthentication Server Function (AUSF).

The user profile is saved in an Unified Data Repository (UDR) database accessible via the Unified Data Management (UDM) entity. The UDM entity keeps the profiles of data sessions and of the AMF entity to which the UE mobile is attached. The Authentication Credential Repository and Processing Function (ARPF) is collocated with the UDM and stores the long-term security credentials like the key K.

B. Existing 5G-AKA Protocol

Thanks to the progress of the different generations of mobile networks, the architecture has been and is always evolving and new mechanisms and protocols are still proposed to improve network security and especially the radio access part by focusing on the authentication service. For this, the protocol AKA proposed by 3GPP has been implemented since the introduction of the 3G standard and has been evolved until the appearance of the new version of 5G mobile standard.

The AKA version named Evolved Packet System (EPS-AKA) [7] used to realize mutual authentication between the subscriber and the network in 4G network knows several issues include transmission of the IMSI in clear, Man In The Middle (MITM) attack where the attacker obtains the IMSI then tries to register with the base station, Denial of Service (DoS) Attack that makes a service unavailable, to prevent legitimate users of a service from using it. EPS-AKA* [8] is an authentication protocol proposed for 5G, It makes a few modifications to EPS-AKA, but the main difficulty with both protocols was that UE never makes a cryptographically verifiable statement about its view on the identity SNid of the serving network.

Indeed, the 5G mobile communication standard is currently based on the 5G-AKA protocol, proposed by 3GPP in Technical Specification 33.501 [9]. The new protocol will significantly improve data protection compared to 3G and 4G technologies. In particular, thanks to him, a problem has been resolved concerning a flaw previously exploited by the IMSI interceptors. With these devices, the international mobile subscriber identity of a mobile phone card could be read to determine the location of a mobile device and track a user. To do this, the device only needed to listen to the transmissions between the mobile phone and the antenna of the mobile network. This is no longer possible with 5G-AKA.

Fig. 2 shows the process of the standard 5G-AKA protocol that contains four entities, it's about an equipment device UE, the function security in serving network SEAF and the security functions reside in home network AUSF and ARPF. The UE and ARPF share the secret symmetric key K.

C. Limitations of 5G-AKA Protocol

Although 5G security has been improved compared to previous generations, certain system limitations have been identified which are critical for security protocols and mechanisms, which make 5G systems susceptible to multiple

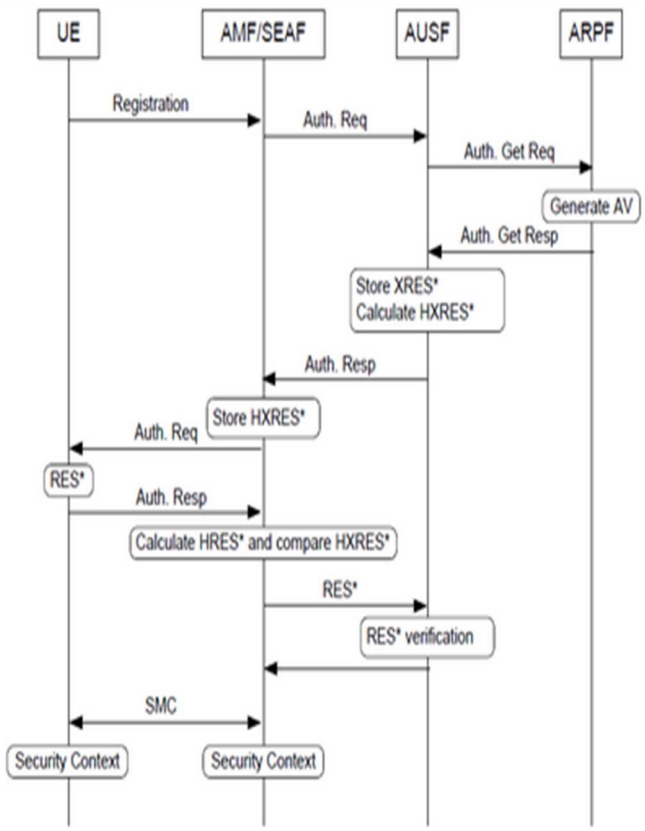

Fig. 2. 5G-AKA Authentication Procedure

attacks. Then we cite some of these limitations [10]:

- In order to protect and provide privacy preservation of the UE identity's Globally Unique Subscription Permanent Identifier (SUPI) in 5G-AKA protocol, 3GPP proposes to implement the Elliptic Curve Integrated Encryption Scheme (ECIES) [11] encryption that can causes a high computation overhead mainly in the intelligent objects that not able to support asymmetric encryption.
- In addition, the protocol suffers from the high communication and computation overheads in the core network causes by the number of authentication vectors calculating between the home network entities.
- In 5G-AKA, the verification of integrity is not available in ARPF entity and this later cannot be authenticated to the UE, in this case, any intruder can be authenticated in the network using the private identity of UE. Then, the protocol confronts several security attacks such as MITM, replay, and DoS attack.
- The synchronization problem is one of the most issues known in 5G authentication procedure when the sequence number is establish between UE and the ARPF.

III. PROPOSED PROTOCOL

According to different limitations existing in 5G-AKA protocol and discussed in previous section, we propose an improved and efficient authentication and key agreement protocol that follows the network architecture of 5G cellular network and overcomes several attacks such as replay attack, redirection attack, man in the middle attack and DoS attack. The length of the parameters used in this procedure and the cryptographic functions are presented in Table 1.

TABLE I. THE DIFFERENT NOTATIONS USED IN THE PROTOCOL

Notation	Description
SUPI/SUCI	SUPI Subscription Permanent Identifier, Subscription Concealed Identifier, the concealed SUPI
MAC/XMAC	Message Authentication Code
$SEAF_{ID}$	Identity of SEAF
CK /IK	Cipher/Integrity key generated by x
K_{AUSF}/K_{SEAF} /K_{AMF}	Keys generated by ARPF, AUSF, SEAF
XRES*/HXRES*	Expected response value
RES*/HRES*	Authentication response value
AV	Authentication Vector
RAND	Random Number
f1 …… f6	Cryptographic functions Used to compute the authentication parameters

A. Initialization Phase

The process of authentication and key agreement in our proposed protocol achieves between the architecture entities, UE, AMF/SEAF, AUSF and UDM/ARPF.

Each mobile is identified by a permanent identity called SUPI that should be installed by the provider what allows the registration of the user in the core network 3GPP.

In order to provide privacy preservation of subscriber identity SUPI and avoids IMSI catchers, and to exchange the secret key K between UE and SEAF or UE and ARPF, we consider the key agreement protocol Elliptic Curve Diffie Hellman (ECDH) [12] that allows two parties, each having an elliptic curve and public/private key pair, to establish a shared secret over an insecure channel, and we use a symmetric encryption operation to encrypt the identity in order to obtain the identity Subscription Concealed Identifier (SUCI) that concealed the SUPI computed by the UE.

Also, we assume that the communication between the core network entities and security functions (AMF/AUSF/ARPF) are secure and maintaining long-term IPSec, (D)TLS, or DIAMETER sessions over the establishes channels, between the named parties.

In addition, our protocol permit the authentication of AUSF/SEAF in the ARPF when the UE is authenticated with success at ARPF.

B. Authentication Procedure

The Fig. 3 shows the authentication procedure of our proposed and the detailed explanation of each message is as follows:

M1: UE → AMF/SEAF: Attach Request

In order to start the process of authentication, the user equipment generates a random number $RAND_{UE}$ and sends its beside of SUCI identity to SEAF entity.

M2: AMF/SEAF → UE : Attach Request

After the reception of the fits message, the SEAF send the random number $RAND_{SEAF}$ and time stamp T1 to verify if the UE is under operation and to define the expiration time of the next response.

M3: UE → AMF/SEAF : Attach Request

The UE calculates its own authentication message MAC_{UE} and generates the random parameter $RAND'_{UE}$ and send them to the SEAF.

$$MAC_{UE}=f1_K\ (SUCI, RAND_{UE}) \quad (1)$$

$$RAND'_{UE} = f2_K(RAND_{UE}, RAND_{SEAF}) \quad (2)$$

M4: AMF/SEAF → AUSF/UDM/ARPF : Authentication Request

The SEAF verifies the random numbers and the SUCI if there are matches, and sends the parameters to ARPF through AUSF.

M5: UDM/ARPF → AUSF: Authentication Response

After receiving the authentication request message, the UDM/ARPF starts firstly by generating the secret key K and compares the received message authentication code MAC_{UE} with $XMAC_{UE}$. If these values are identical, the UE is authenticated. Then ARPF authenticates the SEAF after the verification of $SEAF_{ID}$. Moreover the ARPF generates its own random $RAND_{ARPF}$ and a random number RAND. Then, it computes MAC_{ARPF}, and computes successively, CK, IK, XRES*,$AUTH_{ARPF}$, K_{AUSF} and transfers AV_{ARPF} with SUPI to the AUSF.

$$MAC_{ARPF} = f1_K(RAND_{UE}, RAND) \quad (3)$$

$$CK = f3_K(RAND_{ARPF}) \quad (4)$$

$$IK = f4_K(RAND_{ARPF}) \quad (5)$$

$$XRES^*=f5_K(RAND'_{UE}, RAND_{ARPF}, RAND) \quad (6)$$

$$AUTN_{ARPF} = (RAND, MAC_{ARPF}, RAND_{ARPF}) \quad (7)$$

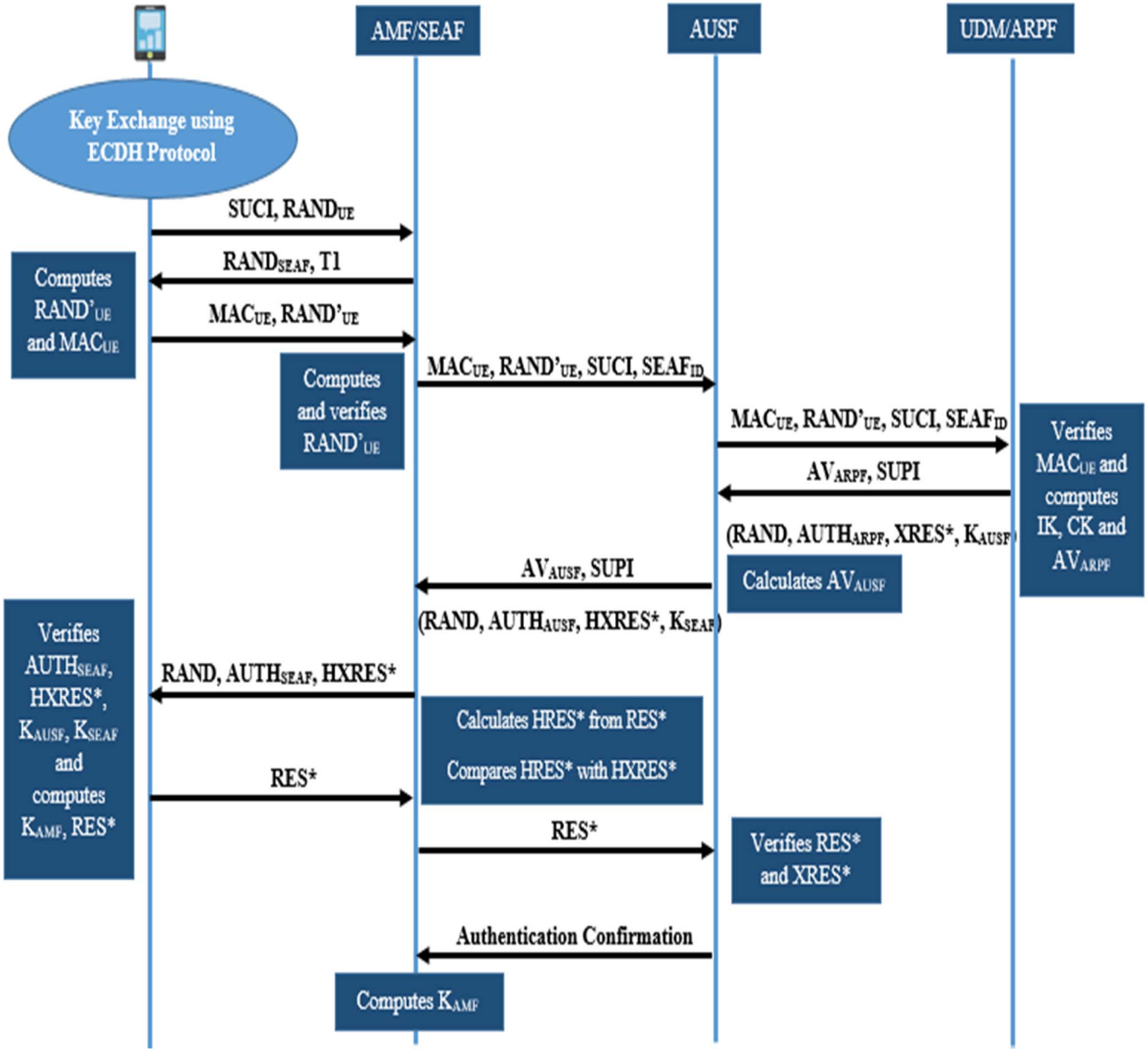

Fig. 3. Proposed Protocol

K_{AUSF} = KDF(CK, IK, $RAND_{ARPF}$, SUCI) (8)

AV_{ARPF} = (RAND, $AUTN_{ARPF}$, XRES*, K_{AUSF}) (9)

M6: AUSF→AMF/SEAF : Authentication Response

After receiving the previous message, the AUSF stores XRES* and K_{AUSF}, then it selects the $RAND_{AUSF}$. Further it computes HXRES*, $AUTH_{AUSF}$, K_{AUSF}, HXRES* which is the hash if XRES* and transmits all the parameters to the SEAF.

HXRES*=f6K(XRE*,$RAND_{AUSF}$,$RAND_{ARPF}$,RAND) (10)

$AUTN_{AUSF}$ = (RAND, $RAND_{ARPF}$, $RAND_{AUSF}$) (11)

K_{SEAF} = KDF(K_{AUSF}, $RAND_{AUSF}$, $RAND_{UE}$, $SEAF_{ID}$) (12)

AV_{AUSF} = (RAND, $AUTN_{AUSF}$,HXRES*,K_{SEAF}) (13)

M7: AMF/SEAF → UE : Authentication Request

After receiving the message from the AUSF, SEAF computes MAC_{SEAF} and transfers the parameters RAND, $AUTH_{SEAF}$ and HXRES to UE.

MAC_{SEAF}= $f2_{KSEAF}$ ($RAND_{SEAF}$, $SEAF_{ID}$, RAND, MAC_{ARPF}) (14)

$AUTH_{SEAF}$ = (MAC_{SEAF}, $RAND_{SEAF}$, $SEAF_{ID}$) (15)

M8: UE → AMF/SEAF : Authentication Response

First, UE checks the verification of MAC_{ARPF} and MAC_{SEAF} in order to ensure that UE authenticates the ARPF and SEAF entities respectively. After UE compares the received values HXRES*, XRES* , K_{AUSF}, K_{SEAF} and if these values are matched, UE authenticates the ARPF and AUSF. Also it calculates K_{AMF} and RES* that it will be sends to SEAF.

K_{AMF} = KDF(SUCI, K_{SEAF}) (16)

RES* = $f5_K$ ($RAND'_{UE}$, $RAND_{ARPF}$, RAND) (17)

M9: AMF/SEAF→ AUSF: Authentication Request

SEAF will be successfully authenticate in the UE if the value HXRES* is verified and after receiving the RES* by the AUSF, it will compare the value of the parameter with XRES*.

HRES* =$f6_K$(RES*, $RAND_{AUSF}$, $RAND_{ARPF}$, RAND) (18)

M10: AUSF → AMF/SEAF : Confirmation message

AUSF sends the authentication confirmation message contained the result and the SUPI to SEAF and this later computes the K_{AMF}.

After the verification of all the procedure we can consider the our procedure of authentication and key agreement is completed successfully

C. Key Hierarchy in our System 5G

After successful authentication, each user equipment and serving network shared a key K_{AMF} as an essential tool for the derivation of the following keys. The hierarchy of keys in the 5G system is shown in Fig. 4.

Key hierarchy is longer in 5G than in 4G because 5G introduces two intermediate keys, K_{AUSF} and K_{AMF}. K_{SEAF} is the anchor key in 5G, equivalent to K_{ASME} in 4G.

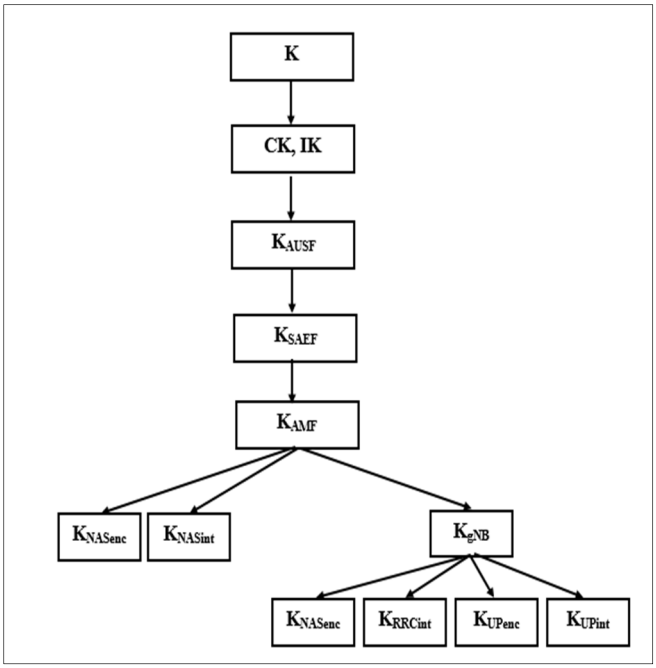

Fig. 4. Key Hierarchy in System 5G

IV. VALIDATION AND EVALUATION

This section evaluates the performances of our authentication protocol according to security analysis and the performance evaluation with other existing protocols.

A. Security Analysis

In this part, we analyze the security analysis and the formal verification to illustrate that our model can reach the security objectives and requirements.

1) Formal Verification

This solution was checked by the security protocol verification tool, Automated Validation of Internet Security Protocols and Applications (AVISPA) [13], which indicated that it is a very secure level. The main advantage of this tool is the ability to use different verification techniques on the same protocol specification. The protocol designer interacts with the tool by specifying a security problem in the High Level Protocol Specification Language (HLPSL). The specification of the protocol is used as an input to the four different back-ends: On-the-fly Model-Checker (OFMC), CL-based Attack Searcher (CL-AtSe), SAT-based Model-Checker (SATMC) and Tree-Automata-based Protocol Analyzer (TA4SP). These back-ends perform the analysis and formatting of the output that contains the results.

The primary goal of our proposed scheme is to provide all security requirements between the UE equipment and the entities of serving network and home network. We need to verify that the proposed protocol can provide a successful mutual authentication between the UE, SEAF, AUSF and ARPF by using back-end servers.

After running this specification with OFMC and CLAtSe backends, we can conclude that the proposed solution can accomplish our goal and can resist those malicious attacks, such as replay attacks, secrecy attacks, and DoS attacks, MITM attacks… under the test of AVISPA. The outputs of the model checking results are shown in Figs. 5 and 6.

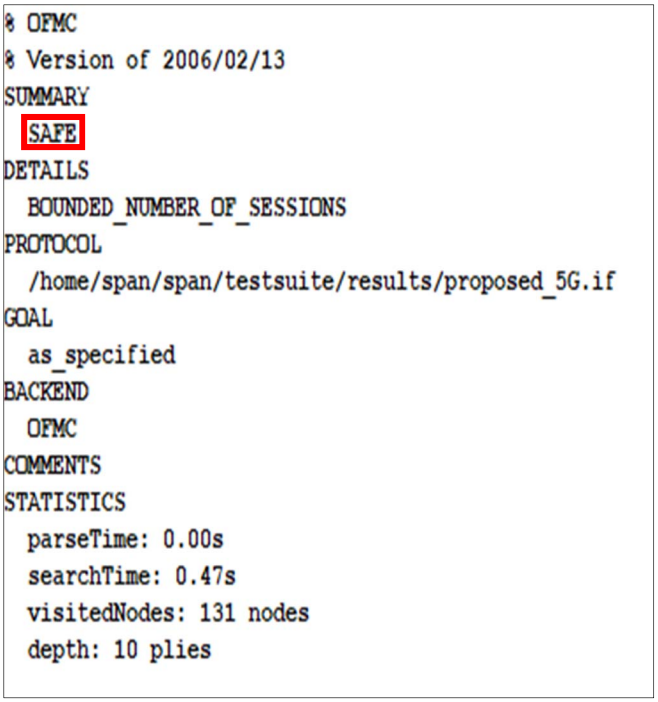

Fig. 5. Results Reported by the OFMC Back-End

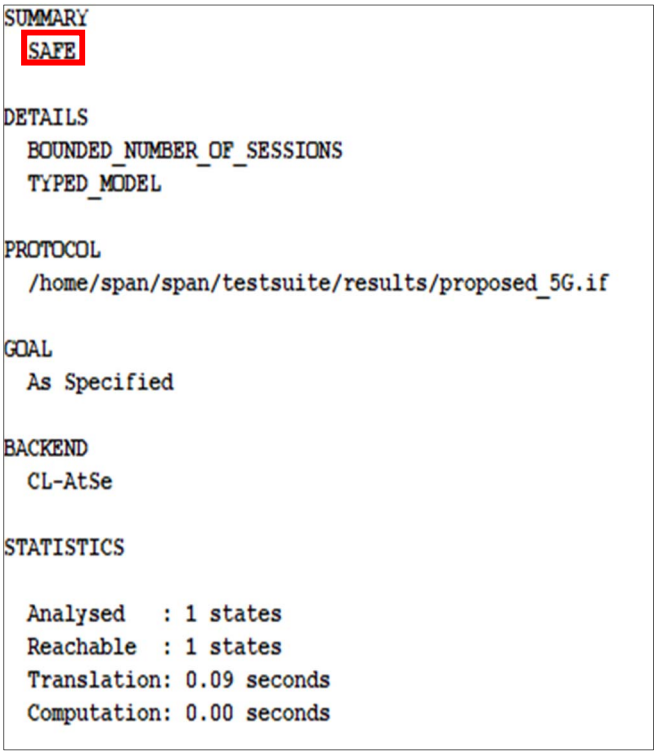

Fig. 6. Results Reported by the CL-AtSe Back-End

2) Mutual Authentication

In the proposed protocol, the communications between all entities UE, ARPF, SEAF, and AUSF performs and achieves the mutual authentication and key agreement and that using their own MAC. The UE authenticates the SEAF and ARPF after the verification of MAC_{UE} computes by UE and transmits to ARPF and also by checking the validation of the MAC_{ARPF} and MAC_{SEAF} and by verifying the received value of RES*. Then, the device authenticates the AUSF entity by generating and verifying the key K_{AUSF}.

3) Resistance to Attacks

- ***Replay Attack***

The proposed protocol is resist to the replay attack and an intruder cannot computes the valid session keys and replays the same message, this is due to the generation of random numbers in each entity $RAND_{UE}$, $RAND_{SEAF}$, $RAND_{AUSF}$ and $RAND_{ARPF}$ and also the verification of the exchanges parameters XRES*, K_{AUSF} and AVs which allow the authentication of ARPF and AUSF by UE.

- ***DoS Attack***

Our solution can reduce the effects of DoS attack, by limiting the transmission of false massage requests to the entities in access and core network, for that each device generates it own message authentication code and verifies it in ARPF entity by computing $XMAC_{UE}$, then by the same way the UE authenticates the AUSF but this time by verifying XRES* and HXRES*.

- ***Man in the Middle Attack***

The shared keys K_{AUSF}, K_{SEAF}, K_{AMF} computed and verified in the communication between entities in 5G system overcome the problem of eavesdropping and avoided the compute of authentication messages by any adversary.

- ***Redirection Attack***

Our protocol is resist to redirection attack and an intruder cannot lunch this attack to obtain user information because the SUPI identity of UE is not transmitted over unsecured canal and the verification of the identity of $SEAF_{ID}$ realized by ARPF.

B. Performance Evaluation

In this part, we evaluate the performance of the proposed protocol in terms of communication overhead and computational overhead.

1) Communication Overhead

In order to evaluate the communication overhead of our proposed and other AKA protocols, based of each parameter passed in the message we compute the total number of bits in such messages transmitted between entities. The size of parameters in bit is shown in Table 2.

TABLE II. SIZE OF PARAMETERS

Parameters	Size (bits)
SUPI/SUCI/$SEAF_{ID}$	128
RAND/$RAND_{UE}$/RAND'$_{UE}$/$RAND_{SEAF}$/$RAND_{AUSF}$/ $RAND_{ARPF}$	128
CK/IK/AK/K	128
AUTN	Variable
AV/AV_{ARPF}/AV_{AUSF}	Variable
MAC/XMAC	64
KA_{SME} /K_{AUSF} /K_{SEAF} /K_{AMF}	256
RES/ XRES/RES*/XRES*/HRES*/HXRES*	64

In each AKA protocols, there are three phases, the first when the device establish the communication with the core network, the second when the home network send n Authentications Vectors (AVs) that will be stored in the serving network and the third phase is during the communication between the serving network and the UE, with n is the number of authentication requests (Table 3).

Number of bits in step 1 = ∑ messages (phase 1 + phase 2)

Number of bits in step 2 = ∑ messages (phase 3 * n)

Total number of transmitted bits = ∑ messages (phase 1 + phase 2) + ∑ messages (phase 3 * n)

2) Computation Overhead

We evaluate the computation overhead for our protocol, the standard protocol for 4G EPS-AKA and the existing 5G-AKA. In this context, we choose to implement using Crypto++ Library [14] the execution time values of such single operations were obtained by measurements running on a test platform with 2.1 GHz processor under Ubuntu. Table 4 illustrates the operations and their computation overheads.

In our proposed, to secure the first attach request we assume to use the ECDH protocol to secure the exchange of the key secret between entities and for encryption, we investigate the use of symmetric encryption operation AES-CTR [15] in order to take into consideration the nature of intelligent devices with low power capacity and energy constraints. Then for key derivation, generation, and hash function we use the HMAC-SHA256 and SHA-256 functions.

We demonstrate the computation overhead in Fig. 7. It is observed that our protocol, compared to EPS-AKA, gives greater delay this is due to the fact that our solution use more operations that offers better security and enhance the system security and privacy protection. In addition our proposed is much faster than the 5G-AKA protocol, the reason is that the choice of lightweight operations to make the mutual authentication

TABLE III. COMMUNICATION OVERHEAD

AKA Protocols	Communication Overhead
EPS-AKA	276 + 1088n
5G-AKA	2787 + 2147n
Proposed-AKA	2240 + 1024n

TABLE IV. COMPUTATION OVERHEAD OF SINGLE OPERATION

Operations	Time (us)
ECDH	1290
ECIES/EN	2580
ECIES/DE	1750
Hash (SHA-256)	3.8
HMAC-SHA256	67
AES-CTR	0.47

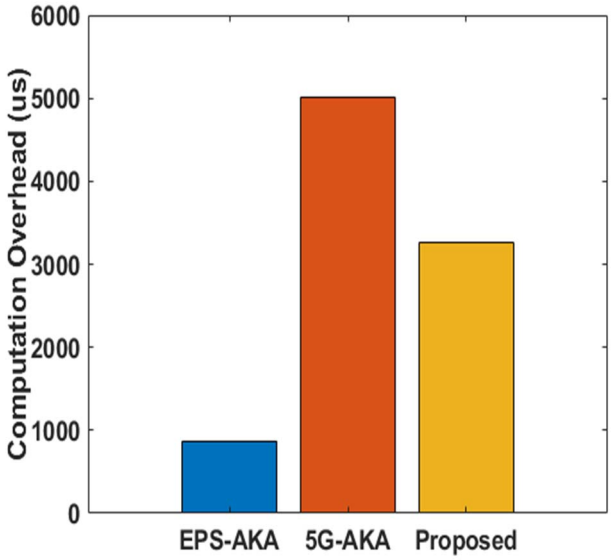

Fig. 7. Computation Overhead

V. CONCLUSION

In this article, we have proposed an improved authentication and key agreement protocol for 5G network based privacy preservation. The main goal of our protocol is to surmount the different weakness existing in 5G-AKA standard protocol. The formal verification using AVISPA tool showed that the solution achieves the total security requirements and resists against several attacks. In addition, we have evaluated the performance of EPS-AKA, 5G-AKA and our proposal in terms of communication overhead and computation delay, the results illustrate that our protocol is performant that the other existing.

REFERENCES

[1] M. Ouaissa, M. Ouaissa, and A. Rhattoy, "An Efficient and Secure Authentication and Key Agreement Protocol of LTE Mobile Network for an IoT System," International Journal of Intelligent Engineering and Systems (IJIES), vol. 12, no. 4, 2019, pp. 212-222.

[2] M. Ouaissa, A. Rhattoy, and M. Lahmer, "New Method to Control Congestion for Machine to Machine Applications in Long Term Evolution System," International Journal on Communications Antenna and Propagation (I.Re.C.A.P.), vol. 8, no. 4, 2018, pp. 355-363.

[3] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," Physical Communication, vol. 18, 2016, pp. 64-84.

[4] M. Ouaissa and A. Rhattoy, "A new scheme of group-based AKA for machine type communication over LTE networks," Int J Electric Comput Eng (IJECE), vol. 8, no. 2, 2018, pp. 1169–1181.

[5] X. Zhang, A. Kunz, and S. Schroder, "Overview of 5G security in 3GPP," IEEE Conference on Standards for Communications and Networking (CSCN), pp. 181–186, 2017.

[6] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," IEEE Access, vol. 3, 2015, pp. 1206-1232.

[7] M. Ouaissa, A. Rhattoy, and I. Chana, "New security level of authentication and key agreement protocol for the IoT on LTE mobile networks," 6th international conference on wireless networks and mobile communications (WINCOM), pp 1–6, 2018.

[8] 3rd Generation Partnership Project (3GPP) TR 33.899 V1.3.0 "Study on the security aspects of the next generation system. Draft", Aug. 2017.

[9] 3rd Generation Partnership Project (3GPP) TS 33.501, "Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system",V.16.2.0, March 2020.

[10] M. Dehnel-Wild and C.Cremers, "Security vulnerability in 5G-AKA draft", February, 2018

[11] V. Gayoso Martínez, L. Hernández Encinas, and A. Queiruga Dios, "Security and practical considerations when implementing the Elliptic Curve Integrated Encryption Scheme," Cryptologia, vol. 39, no 3, 2015, pp. 244-269.

[12] A. P. Fournaris, I. Zafeirakis, C. Koulamas, N. Sklavos, and O. Koufopavlou, "Designing efficient elliptic curve Diffie-Hellman accelerators for embedded systems," IEEE International Symposium on Circuits and Systems (ISCAS), pp. 2025-2028, 2015.

[13] AVISPA Project: http://www.avispa-project.org/

[14] Crypto++ Library: http://www.cryptopp.com/

[15] S. Heron, "Advanced encryption standard (AES)," Network Security, no. 12, 2009, pp. 8-12.