A Secure Efficient and Lightweight authentication protocol for 5G cellular networks: SEL-AKA

Ikram Gharsallah
University of Sfax
NTS'Com Research Unit
Tunisia, Sfax
ikramgharsallah1@gmail.com

Salima Smaoui
University of Sfax
NTS'Com Research Unit
Tunisia, Sfax
salima.smaoui@gmail.com

Faouzi Zarai
University of Sfax
NTS'Com Research Unit
Tunisia, Sfax
Faouzifbz@gmail.com

***Abstract*— The upcoming Fifth Generation of mobile cellular networks 5G is expected to support a set of many requirements and new use cases. The main two user requirements are amplified data-rates at high-speed mobility and a robust and strong network security. Thus, the Third Generation Partnership Project (3GPP) published its first 5G security specifications recently in June 2018 and has been revised in December 2018. Although the security has been improved when compared to previous generations, our analysis recognizes some unrealistic system assumptions that are decisive for security as well as a number protocol edge cases that make 5G systems vulnerable to several attacks. In this paper, we propose a Secure Efficient and Lightweight authentication and Key Agreement protocol SEL-AKA of 5G cellular network taken into account the different limitations relieved in 5G-AKA and without relying on a Global Public Key Infrastructure. Analysis results obtained using the SPAN tool have proved that authentication and privacy objectives are met.**

Keywords*— *security, 3GPP, 5G, authentication, AKA protocol, SPAN.

I. INTRODUCTION

Two thirds of the global's population, approximately 5 billion people, are now mobile subscribers [1]. They are connected to the mobile network via their USIM (Universal Subscriber Identity Module) cards and are protected by security mechanisms standardized by the 3rd Generation Partnership Project (3GPP) group. In December 2018, the 3GPP released and enhanced the final version v15.1.0 of Release 15 of the Technical Specification (TS) 33.501 defining the 5G security architecture and procedures for 5G system [2]. The section 6.1.3.2 has specified the new 5G-AKA (Authentication and Key Agreement) protocol which supposedly provides improved security guarantees such as introducing the concept of increased home control where the home network receives proof of UE (User Equipment) participation in a successful authentication.

The protocol model has four new essential roles [3] that are responsible for assuring the authentication process : UEs where each of them is individually identified by its SUbscription Permanent Identifier (SUPI) which performs the same role as the "IMSI (International Mobile Subscriber Identification Number)" in previous 4G standards. The SUPI is allocated in both the UE and the home network (UDM (Unified Data Management) / (ARPF (Authentication credential Repository and Processing Function)). In order to provide a privacy preserving identity, a SUCI "SUbscribption Concealed Identier" value is used to decrypt (de-conceal) the SUPI by using the SIDF "Subscriber Identity De-concealing Function", this functionality resides within the home network ARPF. Both the UE and APRF pre-shared a long-term secret key K. The SEAF (Security Anchor Function) which is within the Serving Network collocated in the AMF (Access and Mobility Management Function) (which has part of MME (Mobility Managment Equipement) functionality in LTE (Long Term Evolution)), it interacts with the AUSF (Authentication Server Function) and the UE in order to provide authentication. The third entity AUSF residing within the Home Network, acts like an authentication server (as a part of the HSS (Home Subscriber Server) in the EPC (Evolved Packet Core) system). The AUSF interacts with SEAF in order to authenticate user. However, the ARPF also resides within the Home Network collocated with the UDM in a secure location, such as a Hardware Security Module. It supports the storage of all AKA long-term credentials and can execute cryptographic algorithms and generate authentication vectors. The 5G-AKA procedure mainly consist of two phases: 1. Initiation of authentication and selection of authentication method and 2. Authentication procedure for 5G AKA. A full explanation of the authentication process can be found in [2].

The remainder of the paper is structured as follows. First, the different 5G-AKA weaknesses and limitations are reviewed (section II). Next, a novel SEL-AKA authentication protocol for 5G attach procedure is detailed (section III). Afterwards, the proposed scheme is evaluated (section IV). Finally, some final remarks conclude the paper.

II. 5G-AKA WEAKNESSES

Although the security has been enhanced when compared to previous generations, some unrealistic system assumptions has been identified that are critical for security as well as a numeral protocol edge cases that make 5G systems susceptible to several attacks [5, 6]. Thus, the standard specifies requirements that are not enough to offer the expected security guarantees in the context of mobile communication telephony use cases. We mention them as follows:

- In order to provide privacy preservation and prevents against the disclosure of subscriber identity SUPI, 5G-AKA implements one of the Elliptic Curve Integrated Encryption Scheme (ECIES) profiles. However, this results in computation overhead and PKI problems. In addition, the IMSI catchers are avoiding only if the UE knows the public key of every single network operator and if the serving network imposes optional security features. Thereafter, it makes the scheme impractical to be implemented in mobile networks. Moreover, low-end MTC is not able to support ECIES and asymmetric encryption. The comparison with 4G LTE protocol model feats reveals that the 5G security specifications, as of Release 15, do not fully address the subscriber privacy and network availability concerns, where

one edge case can compromise the privacy, availability and security of 5G users and services [5].

- A vulnerability in the 5G-AKA protocol has been found in [4]. In which, an attacker in a roaming scenario and with no privileged network access can impersonate a legitimate user and gain access to the serving network of the honest user. The protocol weakness takes place in two separate phases. In first phase, the malicious actor B eavesdrops and records a legitimate SUCI "encrypted SUPI" of user A, after that, the attacker physically attacks and compromises an honest USIM in the same home network, and extracts the long term key KB in its possession. In second phase, he starts two sessions in parallel at the same time, one is with the attacker's own USIM and SUCI-B, and the other one is started by replaying the overheard SUCI of the legitimate user A. Thus, as a result, to the run sessions in parallel, the AUSF will be incapable to distinguish between the two messages containing the Authentication Vectors received from the ARPF, and it has to associate the mistaken response (and resultant keys) with the incorrect user. In case that this happen, the SEAF does not know which one of these two response messages is sent to user A or B as there is no reference or indication term to either SUPI-A or SUPI-B. As a result, the attacker will now be able to construct K_{SEAF} that the SEAF now believes is the anchor key for SUPI-A and not for SUPI-B which the attacker has compromised. A full explanation of the procedure attack can be found in [4].

- During 5G-AKA procedure, the UE authentication within the home network is only verified in step 10 after commiting ressources, time, bandwith and memory that are required to perform many transmitted messages. This specification can favour apparition of different attacks such as DoS attack.

- In case of authentication failure [11, 12], AKA protocol suffers from the linkability attack. This attack lets the adversary detect the presence of a victim Mobile Station in one of his monitored areas, an active attacker just needs to have previously captured one legitimate authentication request message containing the pair (AUTN, RAND) sent by the network to the UE. The adversary can now replay the captured authentication request each time he wants to check the location of the MS in a specific area. In fact, thanks to the different error messages (SYNC_FAIL, MAC_FAIL), the adversary can differentiate any mobile station from the one which the authentication request was firstly sent to according to the error message type. On reception of the replayed authentication token and authentication challenge (AUTN, RAND), the victim UE successfully verifies the MAC and sends a synchronisation failure message. Nevertheless, the MAC verification fails when performed by any other mobile station, and as a result, a MAC failure message is sent. In case the adversary receives a SYNC_FAIL message, he/she can determine the presence of the targeted UE in a certain area. This breaches the user location confidentiality and subscriber's untraceability.

- While the SEAF authenticates the UE, this later in 5G-AKA protocol has no guarantee on the legitimacy of its serving network.

- In order to prevent from replay attacks and providing freshness, the standard implements a counter SQN (Sequence Number). However, while this parameter is required to be synchronized between the subscriber and its HN, it may happen that they become out-of-sync, e.g., due to message loss.

- 5G Network does not take into consideration the design of appropriate Authentication, Authorization and Accouting AAA mechanisms for 5G: exp (fast communication as well as Internet of Things devices with low power capacity need fast AKA procedures) [13].
- 5G Network does not take into consideration the huge number of IoT devices which expects to reach almost 25 billion interconnected devices in 2020 and can cause subsequently DDOS (Distributed Denial of Service attacks) attacks and signaling traffic problem [14].

- In the case of the UE's successful authentication, the SEAF will send 5G-AC (Authentication Confirmation) messages in 5G-AKA process. These messages are useful but not enough in protecting the system against some frauds like fraudulent Update Location request for subscribers (a link is needed between the authentication result and the location update procedure) [17].

Based on these weaknesses, some solutions based on group-based authentications schemes with an IoT gateway are proposed to reduce the number of complete execution of AKA procedure [15, 16]. However, these group-based AKA solutions have some limitations too. Some of these weaknesses are traditional AKA weaknesses, while some of them are precise to the group-based AKA nature of these approaches such as an attacker can pretend itself as a member of a group and then can attach and get access to the network. There exist also a few solutions such as [18, 12] that attempt to address the aforementioned security issues. However, each of these protocols is dedicated to one or two security issues merely.

III. PROTOCOL PROPOSITION

In order to overcome the different limitations listed above, we propose a new Secure Efficient and Lightweight Authentication and Key Agreement protocol for MTC devices in 5G cellular networks called SEL-AKA.

A. Assumptions

The SEL-AKA assumes the existence of the following assumptions:

- Each device has a permanent identity (SUPI), which identifies the device and should be installed by the supplier in order to allow it to register in a 3GPP network.

- Each device has a pre-shared secret key (K) with the UDM/ARPF.

- Secure communication channel between the Home network (UDM/ARPF) and the serving network (SEAF) has already been established (based on Diameter protocol [7]) and can offer security services to the transmitted data.

- Each device has a parameter called Ref pre-shared with the UDM/ARPF.

Our scheme is described using the notation summarized in Table I.

B. Authentication procedure

During the initial attachment of a device, an authentication procedure must be performed. The proposed protocol shown in Fig. 1 is as follows:

TABLE I. NOTATIONS USED AND THEIR DESCRIPTION.

Acronym	Description
K	(128 or 256 bits long), a pre-shared long-term key between the UE and the UDM/ARPF.
Ref	Reference parameter (64 bits)= index + Nauth
K_{AUSF}	Generated by the UDM/ARPF during an authentication and key agreement procedure and derived from K in case 5G-AKA is used. The ARPF then forward it to the AUSF.
K_{SEAF}	Called the anchor key generated by the AUSF from K_{AUSF} upon a successful primary authentication procedure in each serving network and it will never be transferred to any entity outside the SEAF. K_{SEAF} can be used by the UE and the serving network in order to protect the subsequent communication.
K_{AMF}	Generated by the SEAF and derived from K_{SEAF} after each authentication and key agreement procedure. Then, the SEAF sends it to the AMF.
SN-name	Name of the Serving Network= <5G, ':', SNid>
RAND	Random nonce generated by ARPF.
AUTN	Authentication Tokens generated by ARPF
MAC_x	Message Authentication Codes generated by x
r_x	Random nonce generated by x
$AUTH_{SEAF}$	Authentication Tokens generated by SEAF.
SUCI	Subscription Concealed Identifier, the concealed SUPI using the public key of the operator.
SUPI	SUPI Subscription Permanent Identifier, the permanent identity of a 5G subscriber, equivalent to the IMSI.
RES*	Authentication Response generated by UE.
XRES*	Expected Authentication Response generated by ARPF.
HRES*	Hash of RES* generated by SEAF.
HXRES*	Hash of XRES* generated by AUSF.
CK	Cipher Key.
IK	Integrity Key.
F1…F4	Used to compute the authentication parameters, are one-way keyed cryptographic functions completely unrelated with each other.
SHA256	Hash Function.

Step 1: UE→ SEAF: Attach Request (MAC_{UE}, M_{UE})

The UE calculates its authentication message M_{UE}= (SUCI //ref // r_{UE}), respectively, and generates its own $MAC_{UE}=f^1_K$ (SUCI//Ref //r_{UE}). Then, it sends its MAC_{UE} and M_{UE} to the SEAF.

Where: the SUCI is the concealed SUPI computed by the UE (as defined in Fig. 3). The SUPI consists of routing information parameters such as MCC (Mobile Country Code), MNC (Mobile Network Code) and MSIN (Mobile Subscription Identification Number). The MCC and MNC are not required to be transmitted confidentially, however, the MSIN parameter should be encrypted using the long-term secret key K. Subsequently, the Home network ARPF decrypts the encrypted part of SUCI by the same pre-shared key K to obtain the SUPI.

In addition, the purpose of the Ref parameter added by our proposition is twofold, first it references the shared secret key of the user and it indicates the number of authentication attempts related to this user. In fact (as shown in Fig. 2), Ref is a parameter (64 bits long) installed in both the ARPF and the UE and composed of two parts (left and right parts). The right part (56 bits) presents the pre-shared secret key index of the subscriber. However, the left part (8 bits) presents the number of authentication procedure already made and initialized to zero. Therefore, to de-conceal the encrypted SUPI, the ARPF extracts the 56 left bits part to discover the secret key index of the UE, thus, it determines the correspondent key, decrypts the SUCI and verifies then the MAC_{UE}.

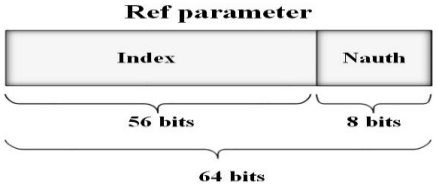

Fig. 2. Ref parameter.

Step 2: SEAF→ AUSF: Attach Request (M_{UE}, $MAC_{UE,}$ SN-name)

The SEAF shall include the Serving Network name (SN-name) in the Authentication Data Request together with the MAC_{UE} and M_{UE}. Then, sends it to the AUSF for further verification.

Step 3: AUSF→ UDM/ARPF: Authentication Data Request (M_{UE}, MAC_{UE}, SN-name)

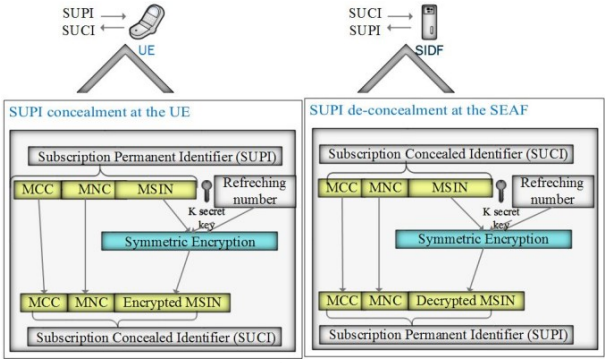

Fig. 3. Concealment/ De-concealment of SUPI.

Upon receiving "Authentication Data Request" message, the AUSF compares the SN-name received with the expected network name in order to check whether the requesting SEAF in the serving network is authorized to use the SN-name in the Authentication Data Request. If so, it stores the received SN-name temporarily.

Step 4: UDM/ARPF→AUSF: Authentication Data Response (5G HE AV, [SUPI])

Once the authentication request message has received, the UDM/ARPF needs to proceed as follows:

1) Extracts the index part from the Ref parameter to determine the correspondent shared key. Next, it verifies MAC_{UE} as well as the Nauth part from the Ref parameter. In fact, Nauth part must be incremented by one compared with the value stored in ARPF. If equality holds, the UE has authenticated with success. Thus, the Nauth must be updated by incrementing it by one.

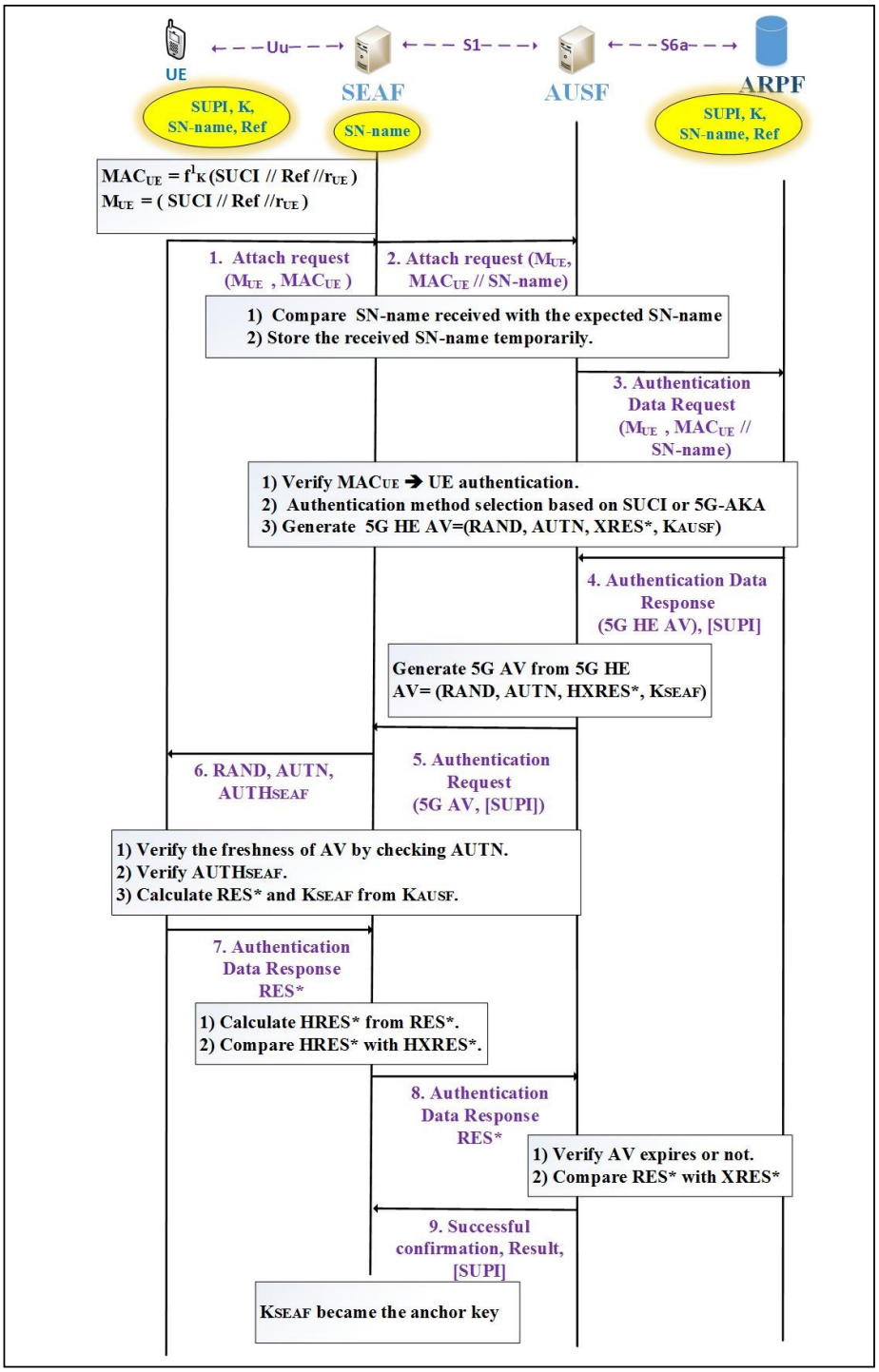

Fig. 1. Proposed scheme procedure SEL-AKA.

2) The SIDF de-conceals SUCI to SUPI based on the key K.

3) Based on the SUPI and the subscription data, the UDM/ARPF shall choose a method selection.

4) Generates a random number RAND. Then, it computes MAC_{ARPF}= f^{1}_{K} (ID_{ARPF}, $r_{UE,}$ RAND), an authentication token AUTN= (RAND, MAC_{ARPF}).

5) Calculates XRES* the expected result as XRES*= f^{4} (ID_{SEAF}, RAND, SUCI, K) and derives K_{AUSF} as defined in [1]. Then it sends the 5G HE AV (Home Environment Authentication Vector) = (RAND, AUTN, XRES*, K_{AUSF}) together with the SUPI to the AUSF in an Authentication Data Response.

Step 5: AUSF➔SEAF: Authentication Data Response (5G AV, [SUPI])

On receiving the message from the UDM/ARPF, the AUSF stores XRES* temporarily until it expires and stores the K_{AUSF}. After that, it generates 5G AV from 5G HE AV= (RAND, AUTN, HXRES*, K_{SEAF}), where: the expected result HXRES* is the hash of XRES* computed as: HXRES*= SHA256 (RAND, XRES*) and the K_{SEAF} is derived from K_{AUSF} as follows: K_{SEAF}= KeySeed (K, RAND, r_{UE}, SN-name). Then it sends it with the SUPI to the SEAF.

Step 6: SEAF→ UE: Authentication Request (RAND, AUTN, $AUTH_{SEAF}$)

Upon receiving the message from the AUSF, SEAF computes MAC_{SEAF} as follows $MAC_{SEAF}= f^2_{KSEAF}$ (r_{SEAF}, ID_{SEAF}, RAND, MAC_{ARPF}), $AUTH_{SEAF}$= (MAC_{SEAF}, r_{SEAF}, ID_{SEAF}) and transmits it together with RAND, AUTN parameters to the UE.

Step 7: UE→ SEAF: Authentication Data Response (RES^*)

At receipt of the RAND, AUTN and $AUTH_{SEAF}$, the UE will perform the following operations:

1) Verifies the freshness of 5G AV by checking AUTN and MAC_{ARPF}. In case of MAC'_{ARPF} and MAC_{ARPF} matches, the UE authenticates the ARPF. Otherwise, the UE sends a synchronisation failure or a MAC failure message.

2) The UE computes MAC'_{SEAF} and compares it with MAC'_{SEAF}. If equality holds, the SEAF is validated by the UE. Otherwise, it rejects the authentication process.

3) Next, the USIM calculates a response value RES and returns RES, CK and IK to the UE. This later computes RES* from RES and sends it to the SEAF for mutual authentication of UE with SEAF in the Authentication Data Response.

Step 8: SEAF→ AUSF: Authentication Data Request (RES*, [SUPI])

The SEAF must calculate HRES* from RES* as: HRES*= SHA256 (RAND, XES*) and compares it with HXRES* received in the 5G AV. In case the values are equals, the authentication has considered as successful. Thus, the SEAF authenticates the UE, and sends the RES* in a message containing the SUPI and the SN name.

Step 9: AUSF→ SEAF: Confirmation message (Result, [SUPI])

For mutual authentication with the UE, the SEAF receives RES* and verifies if RES* matches with XRES*. If equality holds and AV does not expire. SEAF transmits a successful authentication message to the SEAF in a confirmation message contained the result and the SUPI. Thus, it considers the authentication and key agreement to be successfully completed.

After successful authentication, the UE and the SEAF shares a K_{SEAF} key as essential material and an anchor key.

IV. VALIDATION

A. Analytic analysis

In order to solve the 5G-AKA protocol problems, our proposal SEL-AKA must guarantee the following security and quality of service aspects:

Mutual authentication between each entity: The proposed protocol achieves the mutual authentication between each UE, the SEAF and ARPF by generating Message Authentication Code. In our scheme, the ARPF authenticates the UE by verifying the MAC_{UE}. In addition, each device authenticates the SEAF and ARPF by verifying the received MAC_{SEAF} and MAC_{ARPF} respectively. Moreover, each UE generates RES*. Then, it is authenticated at SEAF by verifying the received RES*. Hence, the communication entities perform the mutual authentication and key agreement.

Resistance against DOS attacks: During the authentication procedure, the UE authentication is moving to step 3 instead of step 10 such as in 5G AKA. Thus, SEL-AKA avoids resources consummations and energy if the authentication messages were from an attacker and then continues the procedure only with the authenticated UEs. Consequently, our scheme permits to minimize the DOS attacks.

Defend against the replay attack: The Ref parameter and especially the Nauth part is used in our protocol to prevent from replay attacks of authentication messages. In fact, if the UE is authenticated, the Nauth is incremented. Consequently, an intruder cannot replay the same message.

Data integrity: To ensure integrity of messages, a Message Authentication Code calculated by the different entities UE, the SEAF and the ARPF is inserted.

Latency reduction: The time reserved for concealment and de-concealment procedure used in our scheme is reduced compared with those reserved in the 5G-AKA standard, since it is based on the symmetric encryption instead of the asymmetric one.

B. Automated formal security analysis of the proposed scheme:

In this section, we examine various security properties of the proposed scheme by a formal verification tool known as Automated Validation of Internet Security Protocols and Applications (AVISPA) [8] and its Security Protocol ANimator (SPAN) [9].

The mutual authentication between the users equipment and the network, as well as the confidentiality of the generated keys represent the two security properties of our SEL-AKA protocol that must be specified and verified with SPAN.

- Mutual authentication

The first mutual authentication to check is between the UE and the ARPF. Witness and request events are done to control authentication. Hence, we modeled this goal with HLPSL as shown below:

```
role UE (UE, SEAF, ARPF:agent,……)
played_by UE
transition:
.
.
/\witness(UE,ARPF,auth_1,MAC(SUCI.rUE.K.Ref))
/\request(UE,ARPF,auth_2,MAC(IDARPF,rARPF,K))

roleARPF(UE,SEAF,AUSF, ARPF:agent,……)
)
played_by ARPF
transition:.
.
/\request(ARPF,UE,auth_1,MAC(SUCI.rUE.K.Ref))
/\witness(ARPF,UE,auth_2,MAC(IDARPF,rARPF,k))
```

This specification at the basic role level must be followed by a specification at the goal section level as follows:

authentication_on auth_1
authentication_on auth_2

In other words, to ensure their authenticity, the UE requests from the ARPF a verification of the Message Authentication Code MAC_{UE} generated and identified by auth_1. And conversely, to guarantee its authenticity, the ARPF requests from UE a verification of the MAC_{ARPF} identified by auth_2.

The second mutual authentication to check is between the UE and the SEAF. The same procedure is adopted then.

- Confidentiality of keys

The anchor key K_{SEAF} key derived from K_{AUSF} key must be known only by the SEAF and the UE. Moreover, K_{AUSF} key which is also derived from CK and IK keys must be known only by the ARPF and the UE. These objectives are modeled in HLPSL as follows:

- secret (CK, sec_1, {SEAF, UE}): The key CK derived from the key K_{SEAF} must be known only by the SEAF and the UE. This verification is identified by sec_1.

- secret (IK, sec_2, {SEAF, UE}): The key IK derived from the key K_{SEAF} must be known only by the SEAF and the UE. This check is identified by sec_2.

These two checks are identified by sec_1 and sec_2 which must be defined as an ID protocol in the environment role. These basic role level specifications must be followed by a specification at the goal section level as follows:

Secrecy of sec_1
Secrecy of sec_2

Finally, we run the Security Protocol ANimator for AVISPA (SPAN) [9] in On-the-fly Model-Checker (OFMC) and Constraint-Logic-based Attack Searcher (CL-ATSE) back ends to check if our proposed scheme can achieve the above security goals even under various attacks. Fig. 4 shows the outputs of OFMC and CL-ATSE respectively.

In fact, we can conclude that our proposed scheme ensures mutual authentication between network entities and secure session key establishment. Therefore, the defined security goals are successfully reached.

V. CONCLUSION

We have proposed a secure efficient and lightweight authentication and key agreement protocol in order to overcome the different weaknesses deceled in the standard 5G-AKA. Software verification using SPAN has shown that proposed scheme is secure against several attacks such as authentication and confidentiality. In addition, it provides data integrity and latency reduction. Thus, it is more robust than 5G-AKA recently standardized.

As future work, we will discuss the authentication of group of MTCs devices simultaneously in 5G networks. Furthermore, as another perspective, we have the intention to adapt our proposed scheme SEL-AKA in vehicular cellular networks in 5G in order to support V2X (Vehicle To Everything) services.

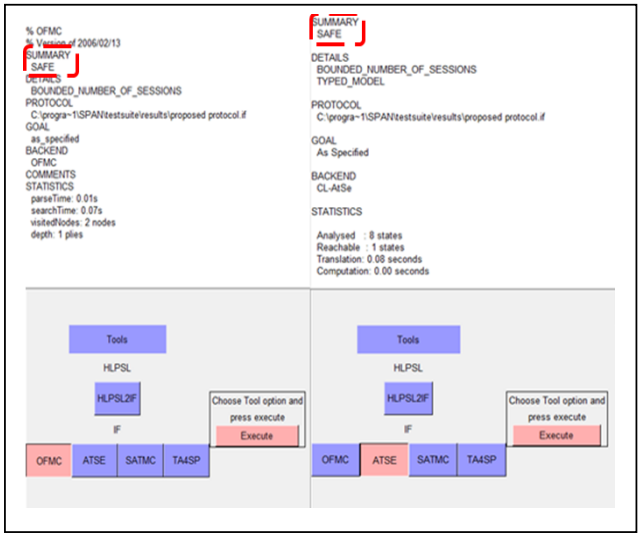

Fig. 4. Formal verification results under the test of AVISPA and SPAN using OFMC and CL-ATSE back-ends.

REFERENCES

[1] GSMA. 2017. Global Mobile Trends 2017. https://www.gsma.com/globalmobiletrends/. Accessed: 2018-05-06.

[2] 3GPP TS 33.501, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 15)", December, 2018.

[3] 3GPP. Security Architecture and Procedures for 5G System. TS 33.501 V0.3.0, 3rd Generation Partnership Project (3GPP), Aug. 2017.

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

[5] D. Basin, J. Dreier, L.Hirschi, S. Radomirović, R. Sasse and V. Stettler, "A Formal Analysis of 5G Authentication", unpublished, arXiv:1806.10360v2 [cs.CR], 16, Aug, 2018.

[6] R. Jover and V. Marojevic, "Security and Protocol Exploit Analysis of the 5G Specifications", unpublished, arXiv:1809.06925v2 [cs.CR] 20, Sep, 2018.

[7] V. Fajardo , J. Arkko , J. Loughney and G. Zorn , " Diameter Base Protocol", Technical Report, Internet Engineering Task Force (IETF), 2012 .

[8] AVISPA v1.1 User Manual, June, 2006.

[9] Y. Glouche, T. Genet, O. Heen, and O. Courtay,"A Security Protocol Animator Tool for AVISPA", ARTIST2 Workshop on Security Specification and Verification of Embedded Systems, Pisa, May, 2006.

[10] A. Prasad, S. Arumugam, Sh. B and A. Zugenmaier, "3GPP 5G Security", Journal of ICT Standardization, pp: 137-158, May 2018.G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. ondon, vol. A247, pp. 529–551, April 1955.

[11] M. Arapinis etc., "New Privacy Issues in Mobile Telephony: Fix and Verification". CCS'12, pp. 16–18, Raleigh, North Carolina, USA. October, 2012.

[12] F. Liu, J. Peng and M. Zuo, "Toward a secure access to 5G network", 17th IEEE International Conference On Trust, Security And Privacy Computing And Communications, 2018.

[13] P. Schneider and G. Horn, "Towards 5G security," Trustcom/BigDataSE/ISPA, vol. 1, pp. 1165–1170, 2015.

[14] 5G Ensure Project, "Deliverable D2.4 Security Architecture (draft)," 2016.

[15] J. Li, M. Wen and T. Zhang, Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A Networks, IEEE Internet of Things Journal, vol.99, pp.1-9, 2015.

[16] W.-T. Su, W.-M. Wong, and W.-C. Chen, "A survey of performance improvement by group-based authentication in iot," International Conference Applied System Innovation (ICASI), pp. 1–4, 2016.

[17] 3GPP, "Security Architecture and Procedures for 5G System," TS 33.501, Tech. Spec. 0.3.0, 201.

[18] A. Koutsos, "The 5G-AKA Authentication Protocol Privacy (Technical Report)", arXiv:1811.06922v1 [cs.CR], November, 2018.