A Generic Construction for Efficient and Secure AKA Protocol in 5G Network

Abstract—**The 3GPP has designed the authentication and key agreement (AKA) protocol for the 5G network to overcome the security deficiencies found in (Evolved Packet Service) EPS-AKA protocol of Long Term Evolution-Advanced (LTE-A) network. However, the existing 5G-AKA protocol is vulnerable to several attacks such as impersonation, man-in-the-middle, and denial of service attack. The identified protocol vulnerabilities would enable an adversary to impersonate the legitimate mobile user and the serving network. In addition, the communication entities incur high computational overhead. In this paper, we propose the generic construction for efficient and secure AKA protocol in the 5G network. For the correctness of the protocol, the formal verification is carried out using the AVISPA tool. In addition, the security analysis illustrates that the protocol fulfills all the security requirements and is secure against the known attacks. Moreover, the performance evaluation of the protocol shows less communication and computation overhead during the AKA process of 5G network.**

Index Terms—**5G, communication and computation overhead, security vulnerabilities, AVISPA.**

I. Introduction

With the evolution of the mobile communication technology from the first generation (1G) to fourth generation (4G), the 3GPP has recently designed the fifth generation (5G) technology to designate the new facilitator platform for IoT-based applications and services in the wireless telecommunication network [1], [2]. The Internet of Things (IoT) is the forthcoming mechanism where millions of devices are connected by the 5G network to manage numerous applications such as smart transportation system, smart healthcare monitoring system, intelligent tracking, and tracing system [3]. The 5G technology is introduced with several goals that enable 5G network with low latency, better network slicing, flexible non-3GPP access inter-networking, high data rate and good quality of services [4]. Therefore, the 5G network can provide the ubiquitous connectivity among the people as well as the devices in the IoT-based applications.

Recently, 3GPP has published various technical reports with necessary amendments regarding the authentication and key agreement (AKA) protocol of 5G network [1], [2], [5]. The design of 5G-AKA protocol is based on the Evolved Packet Service (EPS)-AKA protocol of the Long-Tem Evolution (LTE)/4G network [5]. The 5G-AKA protocol inherits certain security vulnerabilities from EPS-AKA protocol such as impersonation, MitM and DoS attack [6]. Therefore, it is required to revisit the 5G-AKA protocol for establishing information security during the authentication process.

A. Existing 5G-AKA protocol

The 5G-AKA protocol is proposed to resist the cellular network from the malicious security attacks by using the challenge-response scheme as shown in Fig. 1 [1], [7]. There are four communication entities in the protocol named as UE, Security Anchor Function (SEAF), Authentication Server Function (AUSF), Authentication Credential Repository and Processing Function (ARPF). The SEAF works within the serving network, AUSF resides in the home network, ARPF establishes in a secure location and works within the home network. The UE and ARPF share the secret symmetric key K.

The 5G-AKA protocol executes the authentication steps as follows (i) UE transfers the Subscription Permanent Identifier (SUPI)/ Subscription Concealed identifier (SUCI) (performs the similar role as the International Mobile Subscriber Identity (IMSI)) to the SEAF. In the protocol, the SUPI is never transmitted in the air. Hence, SUCI is used to achieve this. (ii) SEAF transfers the SUCI with $SEAF_{ID}$ to ARPF. The ARPF decrypts the SUCI by using Subscriber Identity De-concealing Function (SIDF) and verifies the $SEAF_{ID}$. Then, ARPF generates the AV_{ARPF} with K_{AUSF} and sends to the AUSF. (iii) AUSF stores the $XRES^*$ and computes the $HXRES^*$, K_{SEAF}. Then, it sends the AV_{AUSF} to the SEAF and the SEAF transfers the $r_{AUSF}, HXRES^*, AUTN_{AUSF}, ngKSI$ to the UE. (iv) UE verifies the $HXRES^*$, computes the K_{AMF}, RES^* and sends the RES^* to the SEAF. (v) SEAF computes the $HRES^*$, verifies with $HXRES^*$ and transfers the RES^* to AUSF. (vi) AUSF verifies the RES^* and transfers the authentication confirmation message to the SEAF. After the successful mutual authentication, SEAF computes the K_{AMF}.

B. Weakness of the existing 5G-AKA protocol

The 5G-AKA protocol accomplishes most of the security demands and achieves the privacy-preservation with key forward/backward secrecy (KFS/KBS). According to the security weakness found in technical report [1], the protocol is vulnerable to malicious security attacks such as

1) An adversary can impersonate the genuine UE and sends its own Universal Subscriber Identification Module (USIM), SUCI to ARPF. Also, there is a possibility that an adversary can be authenticated by the network because the ARPF doesn't verify the integrity of the request message transferred from UE through AUSF. In addition, the ARPF is not authenticated at the UE.

978-1-5386-8134-3/18/$31.00 ©2018 IEEE

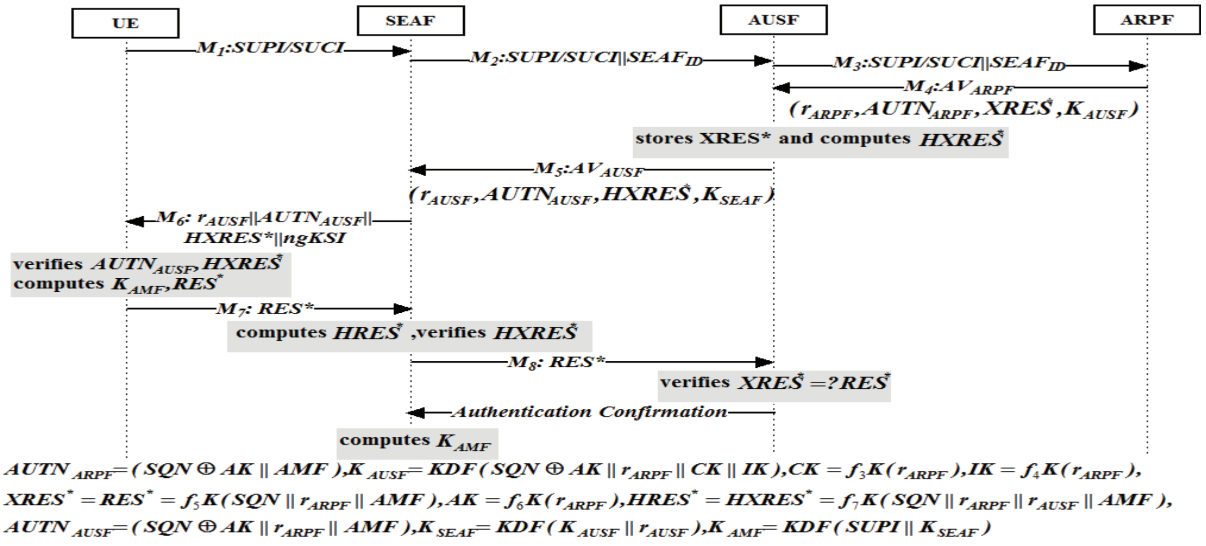

UE
SEAF
AUSF
ARPF
M_1:SUPI/SUCI
M_2:SUPI/SUCI||$SEAF_{ID}$
M_3:SUPI/SUCI||$SEAF_{ID}$
M_4:AV_{ARPF}
$(r_{ARPF}, AUTN_{ARPF}, XRES^*, K_{AUSF})$
stores XRES* and computes $HXRES^*$
M_5:AV_{AUSF}
$(r_{AUSF}, AUTN_{AUSF}, HXRES^*, K_{SEAF})$
M_6: r_{AUSF}||$AUTN_{AUSF}$||
HXRES*||ngKSI
verifies $AUTN_{AUSF}$, $HXRES^*$
computes K_{AMF}, RES^*
M_7: RES*
computes $HRES^*$,verifies $HXRES^*$
M_8: RES*
verifies $XRES^* =? RES^*$
Authentication Confirmation
computes K_{AMF}
$AUTN_{ARPF} = (SQN \oplus AK \| AMF), K_{AUSF} = KDF(SQN \oplus AK \| r_{ARPF} \| CK \| IK), CK = f_3K(r_{ARPF}), IK = f_4K(r_{ARPF}),$
$XRES^* = RES^* = f_5K(SQN \| r_{ARPF} \| AMF), AK = f_6K(r_{ARPF}), HRES^* = HXRES^* = f_7K(SQN \| r_{ARPF} \| r_{AUSF} \| AMF),$
$AUTN_{AUSF} = (SQN \oplus AK \| r_{ARPF} \| AMF), K_{SEAF} = KDF(K_{AUSF} \| r_{AUSF}), K_{AMF} = KDF(SUPI \| K_{SEAF})$

Fig. 1. The existing 5G-AKA protocol

Therefore, the protocol suffers from various security attacks such as MitM, impersonation, and DoS attack.

2) During the authentication process, the UE and ARPF establish the sequence number (SQN) between them. Therefore, the protocol suffers from the synchronization problem if an adversary makes the false registration.
3) The computational overhead at the ARPF, AUSF is very high as all the authentication vectors are computed by the ARPF, AUSF and transmitted to the SEAF. Hence, the protocol incurs high network overhead among the communication entities.

Therefore, it is required to construct an efficient and secure AKA protocol for IoT-based applications in the 5G network. Also, there is a possibility that the IoT devices may increase the bandwidth consumption by transferring forged requests over the communication channel. This problem will emerge when the victim device can't authenticate the legitimate device connected to the network.

C. Core Contribution

To avoid the above-mentioned issues, we propose a generic construction for efficient and secure AKA protocol in the 5G network. The core contributions are as follows:

1) The proposed protocol adopts the basic framework of the 5G network and fulfills all the security demands of the IoT-based applications.
2) The protocol establishes the mutual authentication between UE and ARPF. The ARPF verifies the integrity of the authentication message transferring from UE. Also, the protocol ensures the freshness of the keys.
3) The protocol mitigates the bandwidth consumption among ARPF, AUSF, SEAF, and solves the synchronization problem occurs in the existing 5G-AKA protocol.
4) The formal verification of the protocol is executed using Automated Validation of Internet Security Protocol Application (AVISPA) tool. Moreover, the security analysis illustrates that the protocol accomplishes all the security properties and avoids the known attacks.
5) The performance evaluation of the protocol shows significant improvement in terms of communication and computation overhead.

The remaining sections of the paper are organized as follows. Section II discusses the related works. The proposed protocol for the 5G network is demonstrated in section III. Section IV shows the formal verification and the security analysis of the protocol. The performance evaluation of the protocol with respect to existing AKA protocol is shown in section V. Finally, section VI concludes the paper.

II. Related Work

Currently, 3GPP is specifying the security demands and requirements of 5G-AKA protocol to overcome the issues of EPS-AKA in LTE-A network. However, there is no such security improved/efficient AKA protocol has been proposed in 5G network. Although, researchers have proposed various AKA protocols to improve the efficiency and performance of the LTE-A networks [6], [8]–[14]. The privacy-preservation and security against various attacks are the major concerns of the LTE-A network. To improve the performance of EPS-AKA protocol, Purkhiabani's et al. [8] proposed the AKA protocol that resists from the redirection attack but, suffers from the identity catching and MitM attack. Further, Prasad et al. [9] proposed the digital signature based AKA protocol that incurs less computation overhead. But, the protocol needs the trust relationship among the communication entities from the trusted third party. Hence, the protocol is vulnerable to various known attacks. Hamandi et al. [10] proposed the hybrid key cryptosystem based privacy-preserving AKA protocol. The protocol improves the security of the communication entities but suffers from the synchronization problem and high computation overhead. Ramadan et al. [11] proposed the AKA protocol to avoid the problem of false base station attack and identity catching attack. However, the protocol incurs high network overhead due to public key cryptosystem. To preserve the privacy, Degefa et al. [12] proposed the performance and security-enhanced AKA protocol. However, the protocol suffers from high computation overhead during the authentication process. Different from above LTE/LTE-A network protocols, our main objective is to construct an efficient and secure AKA protocol for 5G networks. The proposed AKA protocol obtains all the security demands such as data integrity, establishes the mutual authentication among the communication entities and resists from all the identified attacks. Moreover, the protocol minimizes the overheads from the network during the key operations.

III. Proposed Protocol

To overcome the security vulnerabilities from the existing 5G-AKA protocol, we propose the generic construction for efficient and secure AKA protocol in 5G networks. The protocol maintains the mutual authentication among the communication entities and avoids the replay, impersonation, man-in-the-middle, and DoS attack. The protocol strictly follows the system architecture of the 5G network. In addition, the cryptographic functions such as f_1 to f_7 [15] and used notations in the protocol are shown in Table I.

TABLE I
PROTOCOL NOTATIONS AND THEIR DEFINITION

Notation	Definition
$r_x, r^{'}_x$	Random number computed by x
t_1	Time-stamp
$MAC_x/XMAC_x$	Message Authentication Code calculated by x
$SEAF_{ID}$	Identity of SEAF
D_{key}	Delegation key
CK_x /IK_x	Cipher/Integrity key generated by x
AMF	Authentication management field
$K_{AUSF}/K_{SEAF}/K_{AMF}$	Keys generated by ARPF, AUSF, SEAF
$XRES^*/HXRES^*$	Expected response value
$RES^*/HRES^*$	Authentication response value
AV_x	Authentication vector computed by $ARPF/ASPF$
$AUTN_x$	Authentication token computed by $ARPF/ASPF$
f_1	Random value generated function
f_2	Message authentication function
f_3, f_4	Key Generation function
f_5, f_7	Response value generated function
f_6	Delegation key generated function

The proposed protocol establishes the mutual authentication and key agreement between UE and ARPF, UE and SEAF/AUSF. Also, the diameter protocol is already maintained between the AUSF and ARPF that provides robustness to the transmitted data. In addition, the protocol allows the ARPF to authenticate the AUSF/SEAF for the successive authentications of the UE. Once the UE is authenticated at ARPF successfully, ARPF transfers the D_{key} to the AUSF/SEAF for further authentications. Hence, it minimizes the network traffic among ARPF, AUSF, SEAF and reduces the bandwidth consumption. The Fig. 2 shows the pictorial presentation of the protocol and step-wise explanation is as follows:

- Step-1: To build the connection for authentication, the UE transmits the SUCI and r_{UE} to the SEAF.
- Step-2: After receiving the SUCI and r_{UE}, SEAF sends the random number $r_{SEAF}||t_1$ to the UE for verifying whether the UE is operating or not. After transmitting r_{SEAF}, the SEAF waits for the response till the expiration of t_1. If the UE doesn't obtain any information, it will transmit the message again.
- Step-3: If UE is operating, it will compute the $r^{'}_{UE} = f_1(r_{UE}||r_{SEAF})$ and $MAC_{UE} = f_{2_{D_{key}}}(r^{'}_{UE}||SUCI||SEAF_{ID})$, where $D_{key} = f_{6_K}(r^{'}_{UE})$. Then, UE transmits the $r^{'}_{UE}, MAC_{UE}$ to the SEAF.
- Step-4: Then SEAF verifies the $r^{'}_{UE}$. If it matches, SEAF transfers the $SUCI, r^{'}_{UE}, MAC_{UE}, SEAF_{ID}$ to the ARPF through AUSF.
- Step-5: The ARPF generates the D_{key} and $XMAC_{UE} = f_{2_{D_{key}}}(r^{'}_{UE}||SUCI||SEAF_{ID})$ and compares with received MAC_{UE}. The UE is authenticated if these values are matched. Then, ARPF verifies the $SEAF_{ID}$ and matches with the UE's $SEAF_{ID}$. If it matches, ARPF authenticates the $SEAF_{ID}$. Further, ARPF selects the r_{ARPF} and computes the $CK = f_{3_K}(r_{ARPF})$, $IK = f_{4_K}(r_{ARPF})$, $XRES^* = f_{5_{D_{key}}}(r^{'}_{UE}||r_{ARPF}||AMF)$, $AUTN_{ARPF} = (AMF||r_{ARPF}||D_{key})$, $K_{AUSF} = KDF(CK||IK||r_{ARPF}||SUCI)$. Then, ARPF transfers the $AV_{ARPF} = (AUTN_{ARPF}, XRES^*, K_{AUSF})$ to the AUSF.
- Step-6: The AUSF stores the $XRES^*, K_{AUSF}$ and selects the r_{AUSF}. It computes the $HXRES^* = f_{7_{D_{key}}}(XRES^*||r_{AUSF}||r_{ARPF}||AMF)$, $AUTN_{AUSF} = (AMF||r_{ARPF}||r_{AUSF})$ and $K_{SEAF} = KDF(K_{AUSF}||r_{AUSF}||SUCI)$. Finally, AUSF transfers the $AV_{AUSF} = (AUTN_{AUSF}, HXRES^*, K_{SEAF})$ to the SEAF.
- Step-7: The SEAF transfers the $HXRES^*, AUTN_{AUSF}, ngKSI$ to the UE and UE computes the $HXRES^*, XRES^*, K_{AUSF}, K_{SEAF}$. Also, UE computes the $K_{AMF} = KDF(SUCI||K_{SEAF})$. Then, it compares the computed values with the received ones and if these values are matched, UE authenticates the ARPF and AUSF. In addition, UE generates the $RES^* = f_{5_{D_{key}}}(r^{'}_{UE}||r_{ARPF}||AMF)$ and transmits to the SEAF.
- Step-8: Then, SEAF computes the $HRES^* = f_{7_{D_{key}}}(RES^*||r_{AUSF}||r_{ARPF}||AMF)$ and compares with $HXRES^*$. If they match, SEAF will consider the successful authentication of the UE. Further, SEAF transfers the RES^* to the AUSF.
- Step-9: The AUSF receives the RES^* and compares with $XRES^*$. The AUSF transfers the authentication

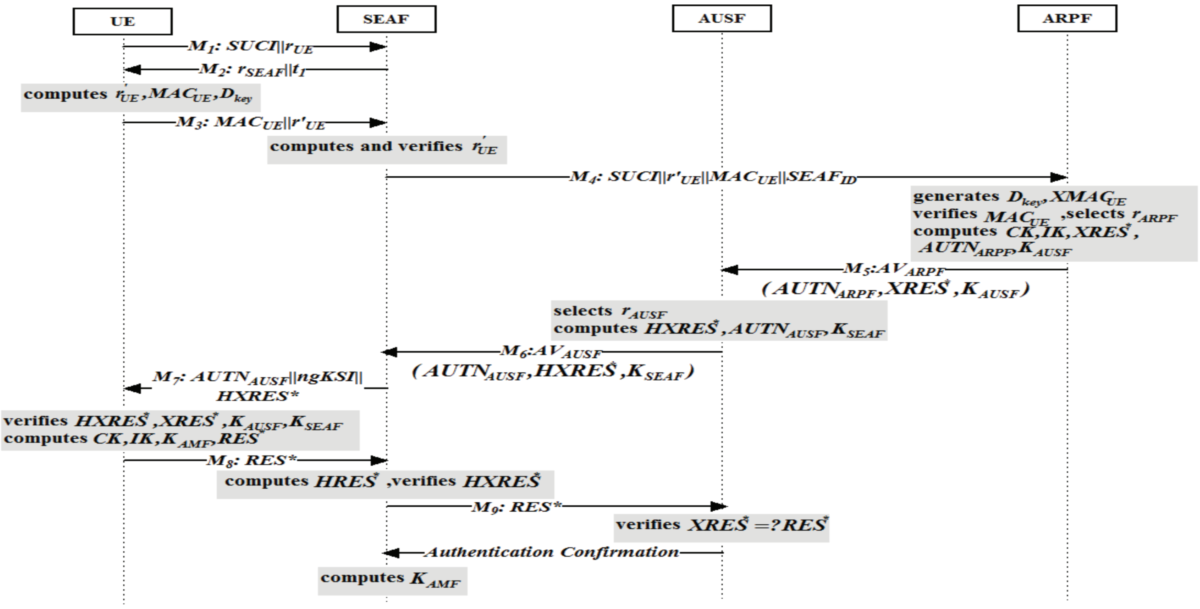

UE
SEAF
AUSF
ARPF
M_1: $SUCI||r_{UE}$
M_2: $r_{SEAF}||t_1$
computes r'_{UE}, MAC_{UE}, D_{key}
M_3: $MAC_{UE}||r'_{UE}$
computes and verifies r'_{UE}
M_4: $SUCI||r'_{UE}||MAC_{UE}||SEAF_{ID}$
generates D_{key}, $XMAC_{UE}$
verifies MAC_{UE} ,selects r_{ARPF}
computes $CK, IK, XRES^*$,
$AUTN_{ARPF}$, K_{AUSF}
M_5:AV_{ARPF}
$(AUTN_{ARPF}, XRES^*, K_{AUSF})$
selects r_{AUSF}
computes $HXRES^*$, $AUTN_{AUSF}$, K_{SEAF}
M_6:AV_{AUSF}
$(AUTN_{AUSF}, HXRES^*, K_{SEAF})$
M_7: $AUTN_{AUSF}||ngKSI||$
$HXRES*$
verifies $HXRES^*$,$XRES^*$,K_{AUSF}, K_{SEAF}
computes CK, IK, K_{AMF}, RES^*
M_8: $RES*$
computes $HRES^*$,verifies $HXRES^*$
M_9: $RES*$
verifies $XRES^* =?RES^*$
Authentication Confirmation
computes K_{AMF}

Fig. 2. The proposed 5G-AKA protocol

confirmation message to SEAF if the comparison is valid. After this, the SEAF computes the K_{AMF}.

IV. Simulation and Security Analysis

A. Simulation using AVISPA tool

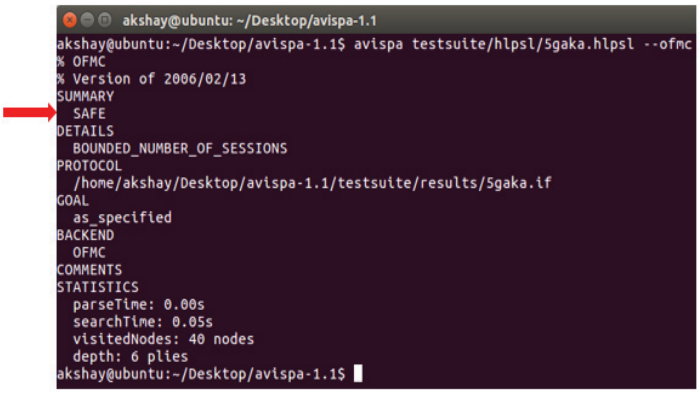
The simulation of the proposed protocol is carried out using the AVISPA tool. The simulation result proves the correctness of the protocol and validates the message confidentiality, integrity, and key secrecy. AVISPA supports various verification models such as OFMC (On-the-Fly-Model-checker), and Cl-AtSe (Constraint Logic-Based Attack Searcher) [16]. The main goals of the protocol are to establish mutual authentication and obtain the secrecy of symmetric keys between the communication entities.

1) Goals of the Proposed Protocol: The goals of the proposed 5G-AKA protocol are shown in Fig. 3. For secrecy of the protocol from malicious attacks, the goals are declared to show which values are secret among the participants. To verify our protocol, we verify two secrecy and four strong authentications.

```
goal
secrecy_of sec_k, sec_dkey
authentication_on ue_seaf
authentication_on seaf_ausf
authentication_on ue_ausf
authentication_on ue_arpf
end goal
```

Fig. 3. Goals of the proposed 5G-AKA protocol

In the proposed protocol, there are four participants such as UE, SEAF, AUSF, and ARPF. The protocol is coded in High-Level Protocol Specifications Language (HLPSL) to verify its security properties. We verify the protocol using OFMC and the results are presented in Fig. 4. The SAFE keyword in Fig. 4 shows that the protocol obtains the identified goals and resists all the malicious attacks.



```
akshay@ubuntu:~/Desktop/avispa-1.1$ avispa testsuite/hlpsl/5gaka.hlpsl --ofmc
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/akshay/Desktop/avispa-1.1/testsuite/results/5gaka.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.05s
  visitedNodes: 40 nodes
  depth: 6 plies
akshay@ubuntu:~/Desktop/avispa-1.1$
```

Fig. 4. Result of OFMC back-end

B. Security Analysis

In this section, we analyze the security of the proposed protocol in terms of various security parameters, and resistance against malicious attacks.

1) ***Mutual authentication:*** In the proposed protocol, UE, ARPF, SEAF, and AUSF maintain the mutual authentication with the key agreement. Firstly, UE computes the MAC_{UE} and transfers to the ARPF. ARPF computes the $XMAC_{UE}$ and matches with MAC_{UE}. If it verifies, ARPF authenticates the UE. Further, ARPF and AUSF transfer the $XRES^*$ and $HXRES^*$ to UE respectively. UE computes these values and generates K_{AUSF} and K_{SEAF}. If these values are matched,

TABLE II
COMPARATIVE ANALYSIS OF THE AKA PROTOCOLS

	Security Parameters, Communication and Computation Overhead									
AKA Protocols	SP_1	SP_2	SP_3	SP_4	SP_5	SP_6	SP_7	$\boldsymbol{CO_{Msg}}^{\boldsymbol{w}}$ (in bits)	$\boldsymbol{CO_{UE}}^{\boldsymbol{x}}$	$\boldsymbol{CO_{Network}}^{\boldsymbol{y}}$
5G-AKA [1]	Yes	Yes	Yes	No	No	Yes	No	2787 + 2147n	7n	8n
EPS-AKA [6]	Yes	No	No	No	No	Yes	No	384 + 1219n	5n	8n
Purkhiabani's-AKA [8]	Yes	No	No	No	No	Yes	No	1027 + 1091n	12n	11n
Hamandi's-AKA [10]	Yes	No	Yes	No	No	Yes	No	384 + 1312n	8n	11n
Proposed-AKA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	2835 + 499n	9n	2n +8

SP_1: Establish mutual authentication; SP_2: Maintains the KFS/KBS; SP_3: Resistance from redirection attack; SP_4: Resistance from impersonation attack; SP_5: Resistance from DoS attack; SP_6: Resistance from replay attack; SP_7: Resistance from MitM attack; n is number of authentication messages; w: Communication overhead of total messages during authentication; x: Number of cryptographic functions for computation cost at UE; y: Number of cryptographic functions for computation cost at network (SEAF, AUSF, ARPF).

UE authenticates the AUSF and ARPF. Moreover, UE sends the RES^* to the SEAF and computes K_{AMF}. Then, SEAF computes the $HRES^*$ and verifies with $HXRES^*$. If it agrees, SEAF authenticates the UE and sends the RES^* to AUSF. AUSF verifies the $RES^* = ?XRES^*$ and transfers the authentication confirmation to the SEAF. Therefore, the protocol maintains the mutual authentication and key agreement.

2) ***KFS/KBS:*** In the protocol, the ARPF, and AUSF computes the K_{AUSF} and K_{SEAF} for each new authentication request. Also, UE and SEAF compute the K_{AMF} securely at each distinct connection. Therefore, it is not possible for an adversary to derive any information through several request messages. In addition, an adversary can't use these keys in the preceding/following sessions as the communication entities generate the new keys in each session.
3) ***Redirection attack:*** An adversary places a false base-station to achieve the user information in the proposed protocol. It is impossible for him/her to launch the redirection attack on the communication network if he/she fails to obtain the user information. An adversary will never achieve the UE's identity as SUPI is never transmitted over the communication channel. In addition, the $SEAF_{ID}$ is implanted into MAC_{UE} and sends to the ARPF. The ARPF compares the implanted $SEAF_{ID}$ with the received one. The request message fails if HSS declines to verify the $SEAF_{ID}$. Therefore, the protocol resists from the redirection attack.
4) ***Impersonation attack:*** For instance, an adversary generates the MAC_{UE} by masquerading the MS and transfers to the ARPF. Also, the ARPF generates the $XMAC_{UE}$ and compares with MAC_{UE}. If the authentication fails, a false UE is identified by the ARPF. In addition, the false UE will never compute the $HXRES^*, XRES^*, K_{AUSF}$, K_{SEAF} and communication entities remains secure throughout the authentication process. Therefore, an adversary can never execute the impersonation attack in the network.
5) ***DoS attack:*** To execute the DoS attack, an adversary can impersonate as the genuine UE and transfers the false message requests to access the network. In the protocol, UE generates the MAC_{UE} and sends to the ARPF. The ARPF computes the $XMAC_{UE}$ and verifies it with received one. If the authentication declines, ARPF recognizes the false UE and transfers the authentication failure message to the UE. Similarly, UE authenticates the ARPF and AUSF by verifying the $HXRES^*, XRES^*$. If the verification doesn't succeed, an authentication failure message is sent to the AUSF and ARPF. Hence, the communication entities avoid the DoS attack from the protocol.
6) ***Replay attack:*** In the protocol, the UE computes the MAC_{UE} by using $r^{'}_{UE}$ and sends to the ARPF. Also, ARPF uses its random number r_{ARPF} and generates the K_{AUSF}, $XRES^*$. Then, it sends the AVs to the AUSF and AUSF uses its random number r_{AUSF}. UE authenticates the ARPF and AUSF by verifying $XRES^*$ and $HXRES^*$ respectively. At each connection request, an unique and distinct r_{ARPF}, r_{AUSF}, r_{SEAF} are used in the authentication process of the protocol. Therefore, an adversary can never compute the valid session keys to launch the replay attack in the protocol.
7) ***MitM attack:*** The communication entities of the protocol maintains the shared session keys throughout the authentication process. Suppose, if an adversary captures D_{key}, but he/she can't achieve verification from ARPF by computing $XMAC_{UE}$. In addition, the K_{AUSF}, K_{SEAF}, K_{AMF} is computed between communication entities to overcome the eavesdropping of transmitted messages. Hence, it is merely impossible for him/her to compute the legitimate authentication messages.

The comparative analysis of the AKA protocols on the basis of security parameters is presented in Table II. It is observed that the existing protocols fail to avoid various known attacks as an adversary may masquerade the UE and transfers the malicious requests to the ARPF. However, the proposed protocol defeats all the known attacks from the communication network and realizes the mutual authentication. Hence, the proposed AKA protocol is comparatively better than the existing one.

V. Performance Evaluation

In this section, the performance of the existing and proposed AKA protocols is evaluated in terms of communication and computation overhead.

TABLE III
SYMBOLS/PARAMETERS AND THEIR SIZES (IN BITS)

Symbol/Parameters	Size (in bits)
PID/TID/IMSI/SUPI/SUCI/$SEAF_{ID}$	128
r_{UE}/r_{ARPF}/r_{AUSF}/r_{SEAF}/RAND/$r^{'}$	128
SN_{ID}/CK/IK/DK/AK/D_{key}	128
SQN / XSQN/AMF	48
AUTN	Variable
AV/GAV/DAV/AV_{ARPF}/AV_{AUSF}	Variable
MAC/XMAC	64
K_{ASME} /K_{AUSF}/K_{SEAF}/K_{AMF}	256
KSI_{ASME}/$ngKSI$	3
TS/t_1/t_2	64
RES/ XRES/RES^*/$XRES^*$/$HRES^*$/$HXRES^*$	64

A. Communication Overhead

To achieve the mutual authentication and key agreement in existing and proposed 5G-AKA protocol, various messages are transmitted among the communication entities. In order to evaluate the communication overhead, we compute the transmitted message size. The total number of bits in the messages transmitted by the AKA protocols are shown in Table II. The protocols are assumed to be of standard sizes with respect to numerous parameters as shown in the Table III [15]. For the proposed 5G-AKA protocol, the computation overhead is as follows:

M_1= 256; M_2= 192; M_3= 192; M_4= 448; M_5= 624; M_6= 624; M_7= 371; M_8= 64; M_9= 64.

Hence, total Communication overhead = 2835 + 499n bits, where n is number of messages. In the existing 5G-AKA protocol, the ARPF and AUSF send n AVs to the SEAF after the UE's authentication. The SEAF needs another authentication when these AVs are expired. The transmission of AVs suffers from high communication cost. However, the proposed 5G-AKA protocol uses the D_{key} during the authentication process. Therefore, the communication overhead of the proposed protocol is less compared to the existing protocol.

B. Computation Overhead

In this section, the computation overhead is shown for the proposed and existing 5G-AKA protocol in terms of the number of cryptographic functions at the communication entities. Table I shows various functions which are used to compute the authentication parameters during the key operations. All the cryptographic functions are considered the unit value to maintain the consistency while evaluating the computation overhead. Table II shows the comparative review of the computation overhead incurs in the AKA protocols. It is observed that the computation overhead of the proposed protocol is better compared to the existing protocols as it uses less cryptographic functions during the authentication process.

VI. Conclusion

In this paper, we have investigated the security weakness of existing 5G-AKA protocol and proposed an efficient and secure AKA protocol in the 5G network. The proposed AKA protocol is simulated using the AVISPA tool and achieves all the security goals. The security analysis represents that the protocol overcomes the malicious attacks such as impersonation, MitM, DoS from the authentication network. We have evaluated the performance of the proposed 5G-AKA protocol and compared it with the existing one. The results illustrate that the protocol generates less overhead and shows improvement in bandwidth utilization for the communication entities. Hence, it is anticipated that the proposed protocol will enhance the security and performance of the 5G network.

References

[1] 3rd Generation Partnership Project (3GPP) TS 33.501, "Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system",V.15.0.0, March 2018.

[2] 3rd Generation Partnership Project (3GPP) TS 33.501, "Technical Specification Group Services and System Aspects (SA3): Security Architecture and Procedures for 5G System", V.0.7.0, December 2017.

[3] M.A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes", Journal of Network and Computer Applications, vol. 101, pp. 55–82, January 2018.

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

[5] 3rd Generation Partnership Project (3GPP) TS 33.401, "Technical Specification Group Services and System Aspects (SA3): 3GPP System Architecture Evolution (SAE)", V.15.2.0, January 2018.

[6] M. Abdeljebbar, and R. Elkouch, "Security analysis of LTE/SAE networks over E-UTRAN", IEEE International Conference on Information Technology for Organizations Development, pp. 1–5, May 2016.

[7] 5G PPP Architecture Working Group, "View on 5G Architecture", V.2.0.0, July 2017.

[8] M. Purkhiabani, and A. Salahi, "Enhanced authentication and key agreement procedure of next generation 3GPP mobile networks", International Journal of Information and Electronics Engineering, vol. 2, no. 1, pp. 557–563, September 2011.

[9] M. Prasad, and R. Manoharan, "A robust secure DS-AKA with mutual authentication for LTE-A,", Applied Mathematical Sciences, vol. 9, no. 47, pp. 2337–2349, January 2015.

[10] K. Hamandi, K. Abdo, J.B. Elhajj, I.H. Kayssi, and A. Chehab "A privacy-enhanced computationally-efficient and comprehensive LTE-AKA,", Computer Communications, vol. 98, pp. 20–30, January 2017.

[11] M. Ramadan, F. Li, C. Xu, A. Mohamed, H. Abdalla, and A. Ali "User-to-user mutual authentication and key agreement scheme for LTE cellular system,", International Journal Network Security, vol. 18, no. 4, pp. 769–781, January 2016.

[12] F.B. Degefa, B. Lee, D. Kim, J. Choi, and Y. Won "Performance and security enhanced authentication and key agreement protocol for SAE/LTE network,", Computer Networks, vol. 94, no. C, pp. 145–163, January 2016.

[13] S. Gupta, B. L. Parne, and N. S. Chaudhari "DGBES: Dynamic Group Based Efficient and Secure Authentication and Key Agreement Protocol for MTC in LTE/LTE-A networks,", Wireless Personal Communications, vol. 98, no. 3, pp. 2867–2899, February 2018.

[14] B.L. Parne, S. Gupta, and N. S. Chaudhari "SEGB: Security Enhanced Group Based AKA Protocol for M2M Communication in an IoT Enabled LTE/LTE-A Network,", IEEE Access, vol. 6, pp. 3668–3684, January 2018.

[15] N. Saxena, J. Thomas, and N.S. Chaudhari "ES-AKA: An Efficient and Secure Authentication and Key Agreement Protocol for UMTS Networks,", Wireless Personal Communications, vol. 84, no. 3, pp. 1981–2012, April 2015.

[16] AVISPA, "Avispa automated validation of Internet security protocols," 2003 [Online]. Available: http://www.avispa-project.org.