Computer Systems Science & Engineering
DOI:10.32604/csse.2021.015593
Article

Tech Science Press

Pseudonym Mutable Based Privacy for 5G User Identity

Rashid A. Saeed[1], Mamoon M. Saeed[2,3], Rania A. Mokhtar[1], Hesham Alhumyani[1] and S. Abdel-Khalek[4,*]

[1]Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
[2]Department of Electrical Engineering, Faculty of Engineering, Alzaiem Alazhari University, Khartoum, 11111, Sudan
[3]Department of Communications and Electronics Engineering, Faculty of Engineering, University of Modern Sciences (UMS), Sana'a, 16784, Yemen
[4]Department of Mathematics, College of Sciences, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
*Corresponding Author: S. Abdel-Khalek. Email: abotalbquantum@gmail.com
Received: 29 November 2020; Accepted: 03 March 2021

Abstract: Privacy, identity preserving and integrity have become key problems for telecommunication standards. Significant privacy threats are expected in 5G networks considering the large number of devices that will be deployed. As Internet of Things (IoT) and long-term evolution for machine type (LTE-m) are growing very fast with massive data traffic the risk of privacy attacks will be greatly increase. For all the above issues standards' bodies should ensure users' identity and privacy in order to gain the trust of service providers and industries. Against such threats, 5G specifications require a rigid and robust privacy procedure. Many research studies have addressed user privacy in 5G networks. This paper proposes a method to enhance user identity privacy in 5G systems through a scheme to protect the international mobile subscriber identity (IMSI) using a mutable mobile subscriber identity (MMSI) that changes randomly and avoids the exchange of IMSIs. It maintains authentication and key agreement (AKA) structure compatibility with previous mobile generations and improves user equipment (UE) synchronization with home networks. The proposed algorithm adds no computation overhead to UE or the network except a small amount in the home subscriber server (HSS). The proposed pseudonym mutable uses the XOR function to send the MMSI from the HSS to the UE which is reducing the encryption overhead significantly. The proposed solution was verified by ProVerif.

Keywords: 5G; MMSI; IMSI; AKA; privacy; user identity

1 Introduction

Mobile communication has become vital in daily life and business. It is involved in many applications and has seen extensive research and development. Users rely on mobile systems to transmit both voice and data [1], especially with the advent of technologies such as the Internet of Things (IoT). These technologies are associated with many services, such as big data, cloud computing, and fog computing [2,3,4]. The 5G

standard has responded to this aggressive development with standards such as device-to-device (D2D), vehicle-to-everything (V2X), long-term evolution for machine type (LTE-m), extended coverage GSM (EC-GSM), and narrowband IoT (NB-IoT). Standards have been developed, such as LoRa, Sigfox, and Weightless, all based on the low-power wide-area network (LPWAN) [5].

Security, privacy, and integrity have become crucial issues for telecom standards and organizations. For all the above technologies, with massive data traffic, standards' bodies should ensure users' security and privacy in order to gain the trust of service providers and industries [6]. 4G employs mutual authentication between user entity (UE) and serving network (SN), whereas previous generations used authentication in the home network only [7,8]. In 4G, authentication is accomplished by an evolved packet system-authentication and key agreement (EPS-AKA) protocol, but user privacy is still considered weak. Mobile networks use the international mobile subscriber identity (IMSI) to identify the UE, but the permanent identity IMSI is sent in plaintext [9].

The Third Generation Partnership Project (3GPP) uses the cell radio network temporary identifier (C-RNTI), temporary mobile subscriber identifier (TMSI), and global user temporary identifier (GUTI) for a particular UE at various stages, but there still are situations in which the IMSI must be exchanged in plaintext [10,11], such as between a mobility management entity (MME) and authentication center (AuC) for a network attachment access request. This paper analyzes authentication in the 5G system with the same architecture as in the 4G system and proposes an authentication method that can hide the IMSI identification during message exchanges at all communication stages [12].

The remainder of this paper is organized as follows. Section 2 describes authentication in the 5G system. Sections 3 and 4 discuss related work and user privacy issues in the 5G system, respectively. Sections 5 and 6 provide the proposed solution and proof by ProVerif. We discuss our conclusions in Section 7.

2 Mobile Security and Privacy

Security in mobile communication has experienced many advancements, mostly focused on authentication and enhancement of the AKA protocol [13–15]. The authentication process in 4G is between three parties: the home subscriber server (HSS), MME, and UE, which contains the universal subscriber identity module (USIM) and mobile equipment (ME), as shown in Fig. 1.

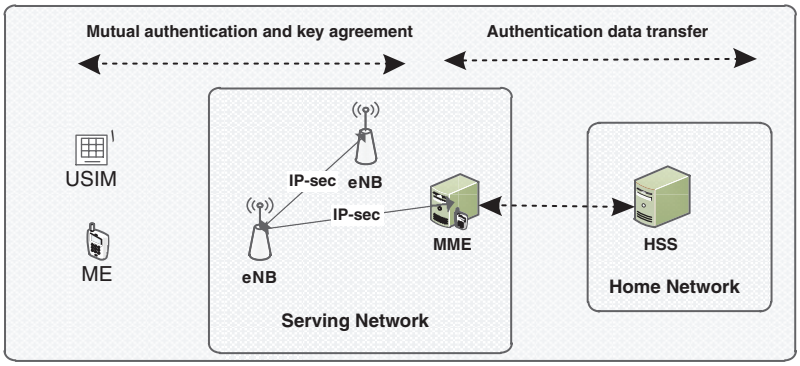

Figure 1: 4G security architecture

The UE sends an attached call to the service network, which involves its IMSI (in clear text) every time it needs to attach to the network. The MME sends the call, which includes IMSI, to the HSS in an authentication vector (AV); the HSS responds to the AV request by generating a changeable random challenge (RAND) (128 bits), and the sequence number SQN is calculated [16]. Next, over SQN, RAND,

and the authentication management field (AMF), the message authentication code (MAC) is computed using f_1. After that, using f_2, f_3, f_4, and f_5, the ciphering key (CK), integrity key (IK), anonymity key (AK), and expected response (XRES) are computed over RAND [17]. AK and AMF are produced by XORing the authentication token (AUTN), which contains the SQN with the MAC. Finally, the AV, which consists of CK, IK, XRES, AUTN, and RAND, is created by the HSS. The AV is sent to the MME, which forwards the AUTN and RAND within an authentication request to the UE and saves XRES, as shown in Fig. 2 [18,19].

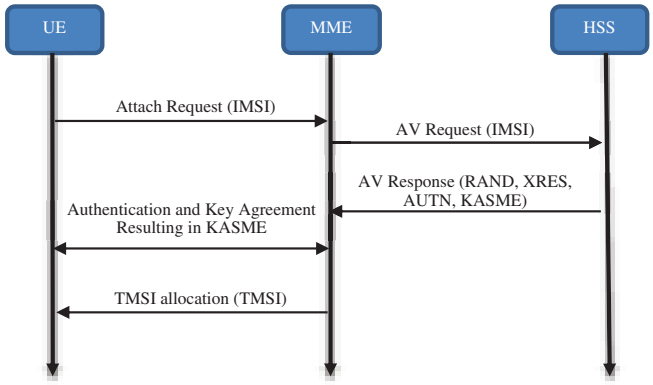

Figure 2: Authentication and Key agreement (AKA) in 4G

Authentication in the 5G system should provide a high degree of privacy because it will be used in medicine, communication, business, and IoT as well as to transmit voice and data, which will enable a high data rate with little latency. For these reasons [20], along with widespread applications and high data rates, many studies focus on enhancing identity privacy by hiding the permanent identity IMSI. Many solutions have been suggested to improve the privacy of user identity in the 5G system. Some have assumed new 5G architecture and suggested the use of network function virtualization (NFV) and software-defined networking (SDN) [21], whereas others assume the architecture will be the same as in 4G and accordingly suggest new methods [21]. We discuss these solutions in Section 4.

3 Related Work

User privacy has been a concern through all previous generations of mobile systems, including GSM, UMTS, and LTE [22] in particular. Much work discusses 5G privacy and related issues. Primarily, the following three topics have been studied: (1) using a private key, a public key, or mutual group keys to encrypt the permanent identity; (2) the use of pseudonyms to hide the permanent identity; and (3) changing the AKA protocol and suggesting a design to hide the permanent identity [23]. A wide variety of research uses shared group keys, a private key, or a public key of the SN to hide the permanent identity. A procedure built on identity-based encryption, namely privacy enhanced fast mutual authentication (PEFMA), has been used to encrypt the IMSI [24]. In this procedure, the server network need not join the UE by the HN, and the SN has public keys. The UE directs the permanent identity after encrypting it by the public key of the server network. PEFMA can run without communicating with the network, as the SN and UE have the public keys.

A mobility support system (MSS) [25] presented a fundamental key to hold a user's permanent identity in the 5G system with secrecy and with slight effect on the communication standard (the modification was transparent and compatible with the standard). Two crypto libraries, Nettle and Open SSL, were used to test

four Android-based strategies. An Android execution of one of the tests was evaluated, comprising the unequal method elliptic curve integrated encryption scheme (ECIES). The effect of the applied estimation of encrypting the IMSI in 5G networks was provided through the usage of ECIES (without MAC) [26]. The structures of 3GPP AKA were presented [27] to propose guaranteed privacy during the whole communication session for the session key. The USIM card and mobile device interface were not affected, allowing reuse of deployed USIMs. The authors concluded that it is possible to bind the assets of a defrayal of K and that achievement is conceivable with a slight effect on legacy 3GPP construction.

There was another study to encrypt the IMSI [28]. The paper identified three identifications, namely the IMSI, NC (network code), and CC (country code), that must be publicized and are vulnerable to attack. In this regard, the authors reevaluated and answered research questions about the privacy of the three identities. The paper did not address the vulnerability caused by routing requirements for data validation between the home network (HN) and visited network (VN), and the VN could also request other information from the home network that may lead to the compromise of IMSI privacy.

All of these solutions use numerous methods to encrypt the identity with either a private key or through public-key cryptography. However, the additional calculation may add overhead in terms of time and bandwidth [29]. Many researchers have used pseudonyms to hide the permanent identity in 5G. For instance, researchers [30] presented a novel scheme to defend the permanent identity by generating a pseudonym in the middle of the HN and UE. The pseudonym is generated locally at the HN, and the UE is prevented from performing available USIMs. Two stages are suggested. First is an initial attachment by the user equipment, when the SN or HN does not join any pseudonym with it. In this situation, the UE is allocated a TMSI by the SN and a pseudonym P by the HN. In the second stage, the UE is forced to detect the identification using P, where the UE does not exchange the TMSI with the SN with strong support for unlinkability.

New concepts have been proposed [31], such as using the 3GPP system to use and manage a locally randomized address for the UE WLAN MAC address, which replaces the general MAC address to avoid privacy risks. These methods tried to boost pseudonym usage in 5G systems. However, the methods have shortcomings. The administration of pseudonyms requires redundant backup with space and memory cost. The distribution of pen names to all user equipment from the system uses extra bandwidth. Finally, there are several new architectures and layouts in 5G systems. For example, a general idea was provided for security contests in SDN, NFV, and clouds [32]. It was believed that there must be shared engagements and trust replicas among members such as network operators, service providers, application designers, users, and manufacturers on information use and storage to maintain user privacy.

Issues related to LTE and WiMAX have been considered at the MAC level and the physical layer [33]. Improving security in 5G is advised through creating a flexible architecture that needs authorized trusted replicas. A reporting service protocol was suggested to take advantage of the architecture of 5G systems in the status of low dormancy, great-speediness contacts, or abridged price [34]. The privacy of participants and users faces the contradiction of internal and external challenges that force arrangements of small cells, D2D communications, or cloud access. A ProSe purpose and ProSe app server in the 5G evolved packet core (EPC) were presented to offer proximity-based application amenities for D2D operators and to handle the communication of D2D procedures [35]. The ProSe utility interrelates with the MME and HSS and cooperates with the ProSe app server on numerous structures, including the packing of user-specific preparations, administration of ProSe amenity recording, security, privacy fortification, annulment, and device detection.

Key agreement protocols and privacy-preserving authentication (PPAKA-IBS and PPAKA-HAMC) were proposed to assure protected and unknown communications of the D2D group [36] [37]. Their change stayed at the protocol level of devices, and a set of users of D2D mutually validated each other

by leaking their individual identification while exchanging their public D2D set session keys. A new structure was designed for 5G network security such that the scrutiny of individuality administration and malleable validation is delivered [38]. The AKA in 4G mobile systems was proved as a symmetric key. 5G needs validation between user equipment and service networks and with third parties such as service suppliers. The hybrid and flexible validation of user equipment could be practical in the methods of validation by the service supplier and the SN, service supplier only, and SN only.

A fast validation pattern in SDN is suggested to boost the benefits of SDN. 5G has been declared to be accepting novel-based multi-party ecosystems where many performers can cooperate in the renovation techniques [39]. 5G will also strongly rely on softwarization models such as slicing and SDN. As the prototypes of 5G networks rely on softwarization, it has been suggested that the standard should include a set of regulations to ensure the privacy of users. Another study [40] proposed accorporating SDN into 5G networks as a step to support operative validation handover and fortification of privacy using softwarization techniques. The notion of a trusted third party is suggested to work like a disseminated network between the supplier and customer [41–44]. The complete official archetype of a procedure from the AKA group is provided. The 3GPP philosophy for 5G security is to hide users' identification in clear cipher requests. 3GPP conducts a complete, systematic, and secure estimation of SDN-enabled 5G with respect to safety and privacy [45].

An automatic examination pinpoints the minimal safety essential to every security aim, and some threats do not occur, except under abnormal circumstances.

Most of the proposed methods aim to provide mutual entity authentication in 5G networks. Most have proposed a verification procedure with complete communal verification between the serving network and user equipment and modified the AKA protocol, message elements, SN and UE, and new components such as and SDN [46–49]. A main drawback of these methods is the need of network physical component adjustments that could lead the hardware to be changed, which adds cost.

3.1 User Identity Privacy Issues

User identity privacy is one of the main issues in mobile network security, where the user identity is mainly in IMSI. The IMSI is used to identify user equipment (UE) and may be vulnerable to attacks commonly known as IMSI catching [50]. For that, the 3GPP allocates a number of short-term identities such as GUTI, M temporary mobile subscriber identity (M-TMSI), and C-RNTI to UE for various network services. To enhance the privacy of user identity, instead of using the permanent IMSI, UE can use these temporary identities, initiate a request, and access network services [51].

Although this procedure is used to enhance user identity privacy, the user's permanent identity remains exposed to IMSI catchers. There are some circumstances in which UE sends IMSI in clear text [52], such as when: (1) the mobile management entity (MME) might not get the GUTI from the UE; (2) the UE starts the initial network association; (3) the UE performs a handover (HO) between MMEs in the case of loss of the GUTI message; and (4) the MME cannot recover the IMSI from the temporary identifiers sent by the UE [53].

Moreover, if the UE uses impermanent identifiers such as C-RNTI and TMSIs, it would not be sufficient to protect the permanent identity from attacks because the temporary identities remain useable for a long period of time in the same coverage cell and can be reused over dissimilar regions, which allows for passive assaults against the permanent identity [54]. In the 5G system, the privacy of a user's identity should be improved to help users safely exchange information with mutual authentication [46,47]. A robust identity administration mechanism is needed to prevent unauthorized access because the 5G network will work with different hardware components from several vendors.

In 4G, when the UE initiates the network association process, it sends identifiers in plaintext, where it will be vulnerable to privacy attack. Many proposals for the 5G network have been introduced to hide the permanent IMSI [55].

The 3GPP works to protect the user's identity for privacy by hiding the IMSI. The solutions are based on the procedures of the SN to assign a randomly generated, temporary identity for UE, such as GUTIs, TMSIs, and C-RNTI. The permanent identity is used only when a temporary identity has not yet been assigned or as an error retrieval mechanism [56]. The recovery mechanism is necessary to prevent UE lockout if mistakes occur, such as when the SN or UE misses the temporary identity. However, the UE returns to use the permanent identity when the SN requests it from the UE. This retrieval mechanism enables IMSI-catchers to get the IMSI from the UE [57]. Therefore, current ways to protect user identity privacy do not prevent an active attacker from catching the IMSI, and the requirement for these problems is to have a genuine system with short-term cache memory to avoid IMSI catching. Additionally, there is no fortification to eliminate passive attackers who are extant when permanent identity requirements are obtained [6,8,34].

3.2 Privacy Enhancing Scheme for 5G System: (PES-5G)

To enhance the privacy of user identity in the 5G system, it is required to have a way to completely hide the permanent identity IMSI by replacing it with the mutable mobile subscriber identity (MMSI), where only the HSS server can plan for the privacy for a specific UE. The UE will use the MMSI when demanded to present its IMSI. User identity privacy is well-maintained because no component knows the IMSI except the UE and the home subscriber server [58].

In the authentication process, the HSS sends a fresh unpredictable MMSI (MFRESH) confidentiality to the UE. To implement this idea, changes in the features and usage of some basic authentication limitations, that is, SQN and RAND, are suggested. The XOR function is suggested to encrypt the RAND using the SQN token as a key, which is generated randomly at every run for the enhanced AKA protocol and using the challenge RAND to provide the UE with the sequence number SQNHE and the new MMSI. The RAND challenge, which is secure, includes the token SQNHE and is used to get the sequence number to the UE (SQNUE) [59]. The UE uses the RAND challenge to get the new SQNHE and new MMSI (MNEW) through a regular authentication procedure. The UE informs its MMSI of the new MMSI (MNEW) if the authentication process passes and identifies itself with its IMSI by using it the next time. To implement the suggested solution, an enhanced AKA protocol is suggested, as shown in Fig. 3.

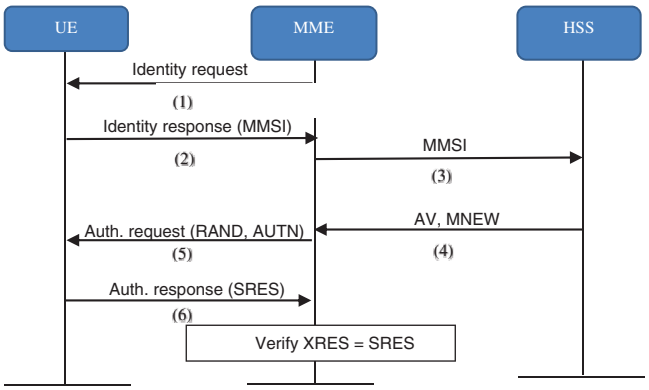

Figure 3: The enhanced AKA protocol

4 Enhanced AKA (EAKA) Protocol

In the initial attachment for each time the UE needs to connect to the network, the UE transmits an access request message to the serving network (MME), which consists of its MMSI each time the user equipment needs to connect to the network. The MME sends a validation data demand to the home network (HSS) with the incoming MMSI [53]. The HSS generates a new MMSI and supplies it to the MME, which forwards the MMSI to the UE. The EAKA protocol details are discussed below.

5 Enhanced HSS Algorithm

There are two MMSI values, M and MNEW, for each UE, which must be stored in the HSS to enhance the HSS algorithm. M supplies the MMSI presently in use, and MNEW supplies the freshly produced MMSI [60], which is assigned to the UE to use in the following stage to block its permanent identity. The home network (HSS) saves the extra values of M and MNEW in its database against the secret key K and IMSI for the UE, as shown in Tab. 1.

Table 1: The MMSI-Index and the HSS's database.

MMSI-Index		HSS-Database			
MMSI	MMSI-Status	IMSI	M	M_{NEW}	K
M_1	POSITIVE	$IMSI_1$	M_1	M_{NEW1}	K_1
M_2	NEGATIVE	$IMSI_2$	M_2	M_{NEW2}	K_2
:	:	:	:	:	:
M_i	NEGATIVE	$IMSI_i$	M_i	M_{NEWi}	K_i
:	:	:	:	:	:
:	:	:	:	:	:
M_b	POSITIVE	$IMSI_b$	M_b	M_{NEWb}	K_b

Tab. 1 is to be saved at the UE with the mapping IMSI at the HSS. It exclusively identifies the UE. The serving network (SN) also saves M and MNEW in its database for the UE within its area of service [61]. There is a group of base stations that contains b = 234 unique MMSI entrances, named MMSI-Index, which is saved in the HSS. This indicates that the home network (HSS) can continuously join the active MMSI.

Every MMSI entrance in the MMSI-index has a value named MMSI-status against it. An MMSI previously assigned to multiple UEs will have NEGATIVE in its MMSI-status to indicate that this MMSI is not ready to be used. An MMSI-status of POSITIVE against a specific MMSI in the MMSI-index signifies that the MMSI is available for use and is not used by any UE [62]. The function ENCODE is specified by an operator to encrypt MNEW and SQNHE using the key SQN in the HSS to produce the encrypted RAND. To implement the EAKA protocol requires some changes in the protocol HSS process, as shown in Algorithm 1.

The HSS should validate that an incoming MMSI is lawful and presently in use by several UEs by discovering the received MMSI in the database of the HSS before deciding whether to receive an MMSI-based validation demand. The demand is vetoed when no attachment is found. The home network (HSS) locates the secret key K and the corresponding UE's IMSI when a match is found [63]. The HSS allocates a used (fresh) MMSI; MFRESH is to be assigned to the UE, and information related to the UE

is updated at the HSS (i.e., the sequence number SQNHE). Second, the HSS validates that the received MMSI is the latest MMSI transmitted to the UE by checking that MMSI = MNEW. The sequence number is manipulated to some extent at the HSS. If the HSS confirms that the previous validation occasion was successful after getting MNEW from the UE, only then does the HSS update SQNHE (see Algorithm 1). This scheme has the following advantages:

Algorithm 1: Enhanced HSS and EAKA protocol

1. *If MMSI is not valid Then drop request and exit*
2. *Else*
3. *MMSI = M_{NEW} Then*
4. *Update MMSI-Index* → M_{FRESH}
5. *Update M* → *MMSI-Index*
6. *Update M_{NEW}* → *M*
7. *Update M_{FRESH}* → *M_{NEW}*
8. *Update SQN_{HE} + 1* → *QN_{HE}*
9. *{0, 1}^{48}* → *SQN*
10. *(SQN XOR (m = (M_{NEW}, SQN_{HE})))* → *RAND*
11. *f1(K,SQN, AMF,RAND)* → *MAC*
12. *f3(K,RAND)* → *CK*
13. *f4(K,RAND)* → *IK*
14. *f5(K,RAND)* → *AK*
15. *(SQN XOR AK,AMF,MAC)* → *AUTN*
16. *(AUTN, RAND, XRES, CK, IK)* → *AV*
17. *End If*
18. *Go to step (4)*

(1) There is no encryption, and it sends MMSI by excluding the XORing function.

(2) The HSS always stays in synchronization with the UE (USIM). After proper validation, SQNUE and SQNHE have the same value at any time, so AVs in transmission would not affect the synchronization because the standards of SQNUE and SQNHE stay in sync.

(3) An attacker that directs several validation requests with an MMSI that was previously used by some UE cannot force the HSS to be out of sync. Likewise, a hacker who resends interrupted RAND and AUTN to the UE cannot force the UE to be out of sync.

(4) In a replay attack, if the hacker resends RAND and AUTN to the UE, it would be easily detected [64].

(5) It causes no authentication failure because synchronization failure does not occur. For the good functioning of this scheme, the MME must bring only one authentication vector from the HSS at a time [65].

The SQN is used as the input key for a function of encryption, namely ENCODE, to protect the confidentiality of the challenge RAND by the HSS. SQN, in addition to the random key, is also secured by a secured AK key. Because an unsystematic key SQN is created using a specific-operator function, attackers cannot obtain the SQN. By encrypting SQNHE and MNEW using the random key SQN, the RAND is produced to provide the UE with the MMSI [66].

5.1 Enhanced UE Algorithm

To enhance the UE algorithm, a unique MMSI value must be preserved in the smart card (USIM) of the user equipment that the UE must use when demanded to provide its permanent identity (IMSI). The service provider embeds an MMSI value, $MMSI_{FIRST}$, in the USIM before the first connection. The HSS database also stores $MMSI_{FIRST}$ in M_{NEW} for each USIM's IMSI and sets to NEGATIVE the status of the $MMSI_{FIRST}$ entered in the MMSI-Index. Throughout the first run of the EAKA protocol, $MMSI_{FIRST}$ is used only once. Service providers often set the function DECODE in their base stations (BSs) to decrypt RAND commands at the UE. Also, they use the random key (i.e., SQN attached with the AUTN message) to extract M_{NEW} and SQN_{HE}. When it receives AUTN and RAND, the UE validates AUTN and calculates the message of validation reaction, as shown in Algorithm 2.

Algorithm 2: Enhanced UE and EAKA protocol

1.	*If step (5) done*
2.	*f5(K,RAND) → Ak*
3.	*AK XOR AUTN(SQN XOR AK) → XSQN*
4.	*f1(K,XSQN,AUTN .AMF,RAND) → XMAC*
5.	*Verify XMAC = AUTN .MAC*
6.	*SQN XOR RAND → = (M_{NEW}, SQN_{HE})*
7.	*m .SQN_{HE} → SQN*
8.	*m .M_{NEW} → MMSI*
9.	*Verify XSQN = SQN_{UE} + 1*
10.	*Update XSQN → SQN_{UE}*
11.	*Update XMMSI → MSI*
12.	*f2(K,RAND) → SRES*
13.	*f3(K,RAND) → K*
14.	*f4(K,RAND) → K*
15.	*End if*
16.	*Go to step (6)*

5.2 Formal Verification

ProVerif software is used to automatically examine the safety of cryptographic protocols. It supports hash functions, asymmetric and symmetric encryption, and digital signatures. ProVerif can prove spread capability possessions, declarations, and observational and communication correspondence. These capabilities are valuable to the security and privacy domain, as they examine the verification and privacy procedures. Furthermore, the development of procedures such as verifiability, privacy, and traceability could also be considered. Analysis of protocol is performed with respect to an infinite number of instances and an infinite number of messages. There is also the capability of attack recovery. Whenever the procedure cannot be verified, ProVerif attempts to rebuild and implement suggestions that can fabricate the wanted events [67].

The main result of this paper is that EAKA imposes protected validation and identification and preserves the privacy of user identity (i.e., unlinkability and user anonymity). An outside observer (enemy) sees no difference in the outcomes of two implementations of the procedure that differ only in the user identities.

5.3 Key Features of EAKA

The privacy of user identity in the offered solution is discussed and considered against numerous potential assaults.

1) ***Protection of identity privacy***: EAKA protects the permanent identity IMSI from the disclosure problem by means of mutable temporary identifier MMSIs. The permanent identity IMSI is never used and is securely saved in the UE and HN forever, so no person and no component in the SN knows about it. The IMSI stays in the USIM, and the database of the HSS and is never used in any interacting procedure during the USIM's period.

2) ***Replay attack***: The user is defended from replay attack by using SQN in this EAKA. Assume that in the effective process of the enhanced AKA protocol, an adversary has interrupted an AV (RAND and AUTN) planned for a specific UE. The SQN stored in the UE is different from the SQN included in the RAND. In this case, the received SQN might be less than the SQN in the UE. The UE can easily detect that a replay attack occurred and tries to retransmit the authentication credentials to the UE.

3) ***Guessing user identity:*** It is not possible to presume the user identity because the total number of possible temporary identities MMSIs is $t = 2n$ where n is the number of bits of MMSI, and the probability that an attacker predicts a POSITIVE MMSI is $M = 1/t$. Because t is a large number, the possibility of correctly guessing a user's MMSI is clearly insignificant.

4) ***Anonymity of user:*** The individuality of the UE is a significant feature of user privacy. The suggested scheme gives a strong guarantee of preserving the identity of the UE. An assailant cannot distinguish the permanent identity of a specific user because it is found only in the database of the HSS and UMSI and is never used or transmitted. Therefore, no one in or out of the network knows about it. An attacker has no way to recognize the permanent identity MMSI assigned to a user because the HSS hides the MMSI before transferring it to the UE. Therefore, the MMSI to a specific UE remains unseen even if used to identify a user.

Also, there is no benefit to knowing the MMSI of an allocated fresh MMSI that is distinct from a previously used MMSI when the UE is effectively known by the HN. The new MMSI allocated to the UE is unsystematic and unconnected to the latest MMSI used by the UE. The attacker cannot discriminate the designated UE because the MMSIs are assigned to a specific user aspect as a random bit stream that cannot be linked to a certain user's equipment.

5) ***Untraceability of user***: Traceability of a user means the probability of knowing earlier identifying requirements and replies of the same user. The proposed solution removes the traceability of users and defends them from tracking attacks by presenting pseudonyms that are used instead of the permanent identifier (IMSI). The pseudonyms (MMSI) assigned to a user change whenever the user attaches to the HN and cannot be perceived or used in external attacks; therefore, the user's untraceability is preserved.

6) ***Unlinkability of the user***: It is impossible for an attacker to sniff the responses and identity because the MMSI identifier is used only one time by the UE. The MMSIs are randomly mutable and unrelated in the system (from the side of the observer); hence, unlinkability of the user is provided.

7) ***DoS attack***: It is impossible for denial of service (DoS) attackers to send many association requests that repeat the use of a real MMSI. A user only places a specified MMSI identifier once before it is replaced by the home local area network (HSS). The network does not accept obtaining several attach requirements parameterized with a similar MMSI. Therefore, attach requirements reached with similar MMSIs are thrown away by the service provider, and a DoS attack is impossible.

8) ***Synchronizing between HSS and UE***: The home network (HSS) uses the SQN just once when it obtains a fresh MMSI (M_{NEW}). It is privately transferred to the UE and stays hidden from the attacker and is not used by the UE; therefore, the attacker cannot disturb the effectiveness of HSS

synchronization. Likewise, the UE cannot be forced to be out of synchronization by a hacker who retransmits interrupted RAND and AUTN to the UE.

6 Conclusion

The need to ensure security and privacy for users on the Internet is an important issue. Most attacks can exploit privacy bugs. IMSI is a critical entity in the network that an attacker can utilize to prohibit network usage or exploit network resources. As the IoT is growing fast and will be deployed with 5G, massive data traffic will need to be exchanged, and the risk of privacy attacks will be greatly increase. In such a network environment, protecting the privacy of the IMSI is considered a vital issue. We presented an enhancement solution for user identity privacy in a 5G network by EAKA, which proposes MMSI for user identification in lieu of IMSI. The EAKA protocol hides the user identity by changing the MMSI in every network attachment without using the permanent IMSI, even at the first attachment. The proposed solution adds no computation overhead to UE or the network except a small amount in the HSS. The proposed solution uses the XOR function to send the MMSI from the HSS to the UE to reduce the encryption overhead. The proposed solution was verified by ProVerif.

Funding Statement: This Research was supported by Taif University Researchers Supporting Project Number (TURSP-2020/216), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Shih, J. Chou and J. Lin, "Wuong: Secure run-time environment and data-driven IoT applications for smart cities and smart buildings," *Journal of Internet Services and Information Security*, vol. 8, no. 2, pp. 1–17, 2018.

[2] D. Arnha, R. Dahab, J. López and L. Olivera, "Efficient implementation of elliptic curve cryptography in wireless sensors," *Adv Math. Communication*, vol. 4, no. 2, pp. 169–187, 2010.

[3] Z. Liu, E. Wenger and J. Großscädl, "MoTE-ECC: Energy-scalable elliptic curve cryptography for wireless sensor networks," in *Proc. Int. Conf. Appl. Cryptography Network Security (ACNS), Lecture Notes in Computer Science*, Cham, Switzerland: Springer, 8479, pp. 361–379, 2014.

[4] U. Gulen and S. Baktr, "Elliptic-curve cryptography for wireless sensor network nodes without hardware multiplier support," *Security and Communication Networks*, vol. 9, no. 18, pp. 4992–5002, 2016.

[5] M. Burrows, M. Abadi and R. Needham, "A logic of authentication," *ACM Trans. Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.

[6] H. Choudhury, "Enhanced anonymity: Customized for roaming and non-roaming IoT-devices in 5g mobile network, " in *Third ISEA Conf. on Security and Privacy (ISEA-ISAP)*, Guwahati, India, 2020.

[7] I. Gharalah, S. Smaui and F. Zarai1, "An efficient authentication and key agreement protocol for a group of vehicles devices in 5G cellular networks," *IET Information Security*, vol. 14, no. 11, 2018.

[8] Q. Jiang, N. Zhang, J. Ni, J. Ma and X. Ma, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. –9390 – 9401, 2020.

[9] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 9, no. 1, pp. 223–244, 2016.

[10] J. Gomez, D. Carrillo, R. Perez and A. Skarmta, "Secure authentication and credential establishment in narrowband IoT and 5G," *Sensors*, vol. 20, no. 3, pp. 882–,901, 2020.

[11] R. Lu, L. Zhang, NI. J. and Y. Fang, "5G Vehicle-to Everything Services: Gearing Up for Security and Privacy," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 373–389, 2020.

[12] S. Thiel and I. Larsen-Ledet, "The role of pseudonymity in mobile e-participation," in *Proceedings of the 52nd Hawaii Int. Conf. on System Sciences*, Grand Wailea, Maui, 2019.

[13] L. Jiang, X. Chang, J. Bai, J. Misic and V. Misic, "Dependability analysis of 5G-AKA authentication service from server and user perspectives digital object identifier," *IEEE Access*, vol. 8, pp. 89562–89574, 2020.

[14] P. K. Agyapong, M. Iwura, D. Stahle and A. Benbur, "Design considerations for a 5G network architecture," *IEEE Communications Magazine*, vol. 52, no. 11, pp. 65–75, 2014.

[15] M. B. Hassan, E. S. Ali, R. A. Mokhtar, A. R. Saeed and B. S. Chaudhari, "NB-IoT: Concepts, applications, and deployment challenges, " in *LPWAN Technologies for IoT and M2M Applications*, B. S. Chaudhari, *Chapter 6.* , Amsterdam, Netherlands: Marco Zennaro, Elsevier, 2020.

[16] Z. E. Ahmed, A. R. Saeed, S. N. Ghopade and A. Mukherjee, "Energy optimization in LPWANs by using heuristic techniques, " in *LPWAN Technologies for IoT and M2M Applications*, B. S. Chaudhari, *Chapter 11.* , Amsterdam, Netherlands: Marco Zennaro, Elsevier, March 2020.

[17] H. Ghahazi, A. El-Mougy and H. Motah, "Enhancing the privacy of LTE-based public safety networks, " in *13th Annual IEEE Workshop on Wireless Local Networks*. Edmonton, Canada, 2014.

[18] G. Koher, J. Jaff and B. Jun, "'Differential power analysis, " in *Advances in Cryptology*. Berlin, Germany: Springer, pp.388–397, 1999.

[19] F. van den Broek, R. Verdult and J. de Ruiter Defeating, "Defeating IMSI catchers," in *22nd ACM SIGSAC Conf. on Computer and Communications Security*, New York, USA, pp. 340–351, 2015.

[20] M. Saeed, A. Saeed. and E. Saeid, "Preserving privacy of paging procedure in 5G using identity-division multiplexing, " in *IEEE First Int. Conf. of Intelligent Computing and Engineering (ICOICE)*. Hadhramoot, Yemen, 2019.

[21] M. A. Elmubark, A. R. Saeed, M. A. Elshaikh and R. A. Mokhtar, "Fast and secure generating and exchanging a symmetric key with different key size in TVWS, " in *Int. Conf. on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE)*. Khartoum, Sudan, 114– 117, 2015.

[22] M. M. Saeed, A. R. Saeed and E. Saeid, "Survey of privacy of user identity in 5G: Challenges and proposed solutions," *Saba Journal of Information Technology and Networking (SJITN)*, vol. 7, no. 1, pp. 1–24, 2019.

[23] Y. Park and Y. Park, "Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 12, pp. p.–2123, 2016.

[24] A. Inn., R. Hassan, A. H. Aman and L. Lattif, "5G technology in internet of everything (IoE) application using light fidelity (Li-Fi) indoor communication," in *1st Int. Conf. on Informatics, Engineering, Science and Technology (INCITEST)*, Bandung, Indonesia2019.

[25] Z. Ali, S. Khaf, Z. H. Abbas, G. Abbas and L. Jiao, "A comprehensive utility function for resource allocation in mobile edge computing, CMC-Computers," *Materials & Continua*, vol. 66, no. 2, pp. 1461–1477, 2021.

[26] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Trans. Industry Electron*, vol. 63, no. 11, pp. 7124–7132, 2016.

[27] A. Arando, D. Basin, Y. Bochut, P. C. Hem and O. Kourenko, *The AVISPA tool for the automated validation of Internet security protocols and applications, Computer Aided Verification*. Berlin, Germany: Springer, 281–285, 2005.

[28] R. Hassan, S. Pepic, M. Sarevic, K. Ahmad and M. Tasic, "A novel approach to data encryption based on matrix computations, CMC-Computers," *Materials & Continua*, vol. 66, no. 2, pp. 1139–1153, 2020.

[29] M. Khan and V. Nemi, "Privacy enhanced fast mutual authentication in 5G network using identity-based encryption," *Journal of ICT Standadization 5*, vol. 1, no. 1, pp. 69–90, 2017.

[30] P. Zhang, M. Duresi and A. Durresi, "Mobile privacy protection enhanced with multi-access edge computing, " in *IEEE 32nd Int. Conf. on Advanced Information Networking and Applications (AINA)*. Cracow, Poland, 2018.

[31] R. Mokhtar and A. R. Saeed, "Conservation of mobile data and usability constraints, " in *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies*, Z. Junaid, M. Athar, eds. IGI Global, USA, pp. 40–55, 2011.

[32] S. Doss, J. Paranthaman, S. Gopalakrishnan and A. kila, "kila Memetic optimization with cryptographic encryption for secure medical data transmission in IoT-based distributed systems, CMC-Computers," *Materials & Continua*, vol. 66, no. 2, pp. 1577–1594, 2021.

[33] 3GPP TS 23.401, "General packet radio service (GPRS) enhancements for evolved universal terrestrial radio access network (E-UTRAN) access," *IEEE Standard*, vol. 15.4.0, 2016.

[34] R. Arul, G. Raja, A. Almagabi, M. Alkheiri, C. Hussain *et al.,* "A Quantum-safe key hierarchy and dynamic security association for LTE/SAE in 5G scenario," *IEEE Trans. on Industrial Informatics*, vol. 16, no. 1, pp. 681–690, 2020.

[35] I. Gharsalah, S. Smaui and F. Zarai, "A Secure efficient and lightweight authentication protocol for 5G cellular networks: SEL-AKA," in *15th Int. Wireless Communications & Mobile Computing Conf. (IWCMC)*, Tangier, Morocco, 2019.

[36] I. P. Chang, T. F. Lee, T. H. Lin and C. M. Liu, "Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks," *Sensors*, vol. 15, no. 12, pp. 29841–29854, 2015.

[37] K. Norrman, M. Naslund and E. Dubrov, "Protecting IMSI and user privacy in 5g networks," in *9th Int. Conf. on Mobile Multimedia Communications (MobiMedia)*, Brussels, Belgium, pp. 159–166, 2018.

[38] M. Choudhary, D. Das and M. Choudhary, "Privacy protection and mitigation of unauthorized tracking in 3GPP-WiFi interworking networks, " in *IEEE Wireless Communications and Networking Conf. (WCNC)*. Barcelona, Spain, 2018.

[39] M. M. Saeed, R. A. Saeed and E. Saeid, "Survey of privacy of user identity in 5G: Challenges and proposed solutions," *Saba Journal of information Technology and Networking (SJITN)*, vol. 7, no. 1, pp. 1–24, 2019.

[40] D. Wang, D. He, P. Wang and C. H. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," *IEEE Trans. Dependable Secure Computer*, vol. 12, no. 4, pp. 428–442, 2015.

[41] E. Cobo, J. Nakai, M. Näslu and K. Norrm, "Subscription identifier privacy in 5G systems, " in *IEEE Int. Conf. on Selected Topics in Mobile and Wireless Networking (MoWNeT)*. Avignon, France, 2017.

[42] J. Arko, K. Norrm, M. Näslu and B. Sahin, "Ericsson research, a USIM compatible 5G AKA protocol with perfect forward secrecy, " in *IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom)*. Helsinki, Finland, 2015.

[43] M. Khan, V. Niemi and P. Ginzborg, "IMSI-based routing a*nd* identity privacy in 5G, 22nd Conf, " in *Open Innovation Association FRUCT*. Jyvaskyla, Finland, 338–343, 2018.

[44] G. Arfaoui, J. Manuel, S. Vichez and P. Wary, "Security and resilience in 5G: Current challenges and future directions," in *IEEE Int. Conf. on Big Data Science and Engineering (Trustcom/BigDataSE)*, Sydney, Australia, 2017.

[45] X. Duan and X, "Wang Authentication handover and privacy protection in 5G HetNets using software-defined networking," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 28–35, 2015.

[46] L. Søresen, S. Khajuria and K. Skouby, "5G visions of user privacy," in *IEEE 81st Vehicular Technology Conf. (VTC Spring)*, Glasgow, Scotland, 2015.

[47] D. Basin, J. Dreie, L. Hirschi, S. Radirović, R. Sasse *et al.,* "A formal analysis of 5G authentication," *ACM SIGSAC Conf. on Computer and Communications Security*, Toronto, Canada, 2018.

[48] E. Yang1, P. Joshi and C. Seo, "Improving the detection rate of rarely appearing intrusions in network-based intrusion detection systems," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1647–1663, 2021.

[49] N. Mohammad and A. Reza, "A multi-factor user authentication and key agreement protocol based on bilinear pairing for the internet of things Wireless," *Personal Communications (WPC)*, vol. 111, no. 1, pp. 463–494, 2020.

[50] S. Shin and T. Kwon, "Two-factor authenticated key agreement supporting unlinkability in 5G-integrated wireless sensor networks," *IEEE Access*, vol. 6, pp. 11229–11241, 2018.

[51] A. Maurya and V. N. Sastry, "Fuzzy extractor and elliptic curve based efficient user authentication protocol for wireless sensor networks and internet of things," *Information-an Int. Interdisciplinary Journal*, vol. 8, no. 4, pp. p.–136, 2017.

[52] R. A. Mokhtar, S. Khatun, A. Borhaddin, A. Ramli and A. R., "Saeed Authentication and user presence monitoring technique for mobile computers using JSR82," *Proc. of Brunei Int. Conf. on Engineering and Technology*, vol. 2, pp. 133–136, 2005.

[53] S. Rajamanickam, S. Volala, R. Amin and N. Ramas, "Insider attack protection: Lightweight password-based authentication techniques using ECC," *IEEE Systems Journal*, vol. 14, no. 2, pp. –1972 – 1983, 2019.

[54] S. Baskaran, G. Raja1, A. Bashir and M. Murata, "QoS-aware frequency-based 4g-relative authentication model for next generation LTE and its dependent public safety networks," *IEEE Access*, vol. 5, pp. 21977–21991, 2017.

[55] A. K. Mauya, V. N. Satry and S. K. Udata, "Cryptanalysis and improvement of ECC-based security enhanced user authentication protocol for wireless sensor networks," *Security in Computing and Communications: Springer*, vol. 536, pp. 134–145, 2015.

[56] I. Ahmad, T. Kumar, M. Liyanage, J. Okwu and M. Ylian, "Overview of 5G security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[57] K. Gagnja, "Secure communication scheme for wireless sensor net-works to maintain anonymity," in *Proc. Int. Conf. Computer, Network Communication (ICNC)*, California, USA, pp. 1142–1147, 2015.

[58] H. Choudhury, B. Roych and D. K. Saikia, "Enhancing user identity privacy in LTE, " in *IEEE 11th Int. Conf. on Security and Privacy in Computing and Communications (TrustCom)*. Liverpool, UK, 949–957, 2012.

[59] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan and L. Leng, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," *Computer Networks*, vol. 101, no. 4, pp. 42–62, 2016.

[60] M. Arapi, L. Mancini, E. Ritter, M. Ryan and N. Golde, "New privacy issues in mobile telephony: Fix and verification, " in *ACM Conf. on Computer and Communications Security.* Carolina, USA, 205–216, 2012.

[61] G. Choudhary, J. Kim and V. Sharma, "Security of 5G-mobile back-haul networks: A survey, wireless mobile network, ubiquitous computer," *Dependable Appl.*, vol. 9, no. 4, pp. 41–70, 2018.

[62] D. He, J. Bu, S. Zhu, S. Chan and C. Chen, "Distributed access control with privacy support in wireless sensor networks," *IEEE Transactions on Wireless Communication*, vol. 10, no. 10, pp. 3472–3481, 2011.

[63] Q. Jiang, J. Ma, X. Lu and Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," *Peer-to-Peer Networking and Appl.*, vol. 8, no. 6, pp. 1070–1081, 2015.

[64] J. Cheng, R. M. Xu, X. Y. Tang, V. S. Sheng, C. T. Cai *et al.,* "An abnormal network flow feature sequence prediction approach for DDoS attacks detection in big data environment," *Computer Materials & Continua*, vol. 55, no. 1, pp. 95–119, 2018.

[65] Q. Zhu, R. Wang, Q. Chen, Y. Liu and W. Qin, "IoT gateway: Bridging-wireless sensor networks in to internet o things," in *Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Computer*, Hong Kong, China, pp. 347–352, 2010.

[66] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde *et al.,* "New privacy issues in mobile telephony: Fix and verification, " in *19th ACM Conf. on Computer and Communications Security.* North Carolina, 2012.

[67] M. S. A. Khan and J. C. Mitchell, "Another look at privacy threats in 3g mobile telephony, " in *19th Australasian Conf.* Wollongong, China, 2014.